5.4.5 Taller de Seguridad Web

1. Datos Generales de la asignatura

Nombre de la asignatura:	**Taller de Seguridad Web**
Clave de la asignatura:	**TDB-1405**
Créditos (Ht-Hp_ créditos):	**1-4-5**
Carrera:	**Ingeniería en Tecnologías de la Información y Comunicaciones**

2. Presentación

Caracterización de la asignatura
La asignatura aporta al perfil del Ingeniero en Tecnologías de la Información y Comunicaciones,los conocimientos, habilidades, y metodologías para implementar sistemas de seguridad bajo políticas internas de las organizaciones yestándares aceptados, que permitan plantear soluciones y protección de datos en el desarrollo de aplicaciones web haciendo uso de herramientas de software y hardware adecuadas.
Intención didáctica
El programa de la asignatura de Taller de Seguridad Web se organiza en cinco temas, en los cuales se incluyen aspectos con un enfoque principalmente práctico, sin perder de vista el marco conceptual. El primer tema,Seguridad de Cómputo, le permitirá al estudiante conceptualizar aspectos fundamentales de seguridad de cómputo, abordando políticas y procedimientos de seguridad, así como mecanismos de

encriptación.

En el segundo tema, Protocolos SSL y TLS, se aborda la seguridad en la capa de transporte, tratando principalmente los protocolos de tunelización SSL/TLS, ubicándolos adecuadamente dentro del modelo de protocolos TCP/IP. Además el estudiante aplicará el concepto de Infraestructura de Clave Pública (PKI) y sus componentes, con el fin de mostrar su utilidad en la generación de certificados digitales.

El tercer tema, Seguridad de Servidores, tiene como intención el estudio de la seguridad del lado del servidor, incluyendo temas que ilustran la operación de servidores con servicios configurados de forma segura. También se incluyen conceptos de seguridad perimetral como el uso de cortafuegos, sistemas de detección de intrusos y canales seguros con VPNs. Un complemento interesante al tema de la seguridad del lado del servidor, es el referido a las técnicas de análisis forense, como un mecanismo útil en la obtención de información que permita deducir las causas de posibles de ataques o desastres en servidores.

En el cuarto tema, Seguridad Web, se presenta al estudiante distintos frameworks de desarrollo, con el fin de conocer lo que estos ofrecen en cuanto a seguridad se refiere, así como evitar las probables vulnerabilidades a las que se exponen las aplicaciones web.

En el último tema, se muestran aspectos de seguridad del lado del cliente, principalmente se consideran herramientas antivirales, antispyware, cortafuegos personales, el estándar de encriptación PGP, para ser usados en equipos personales, inalámbricos y móviles.

Es fundamental que el estudiante se integre y colabore activamente en un equipo de trabajo, con el fin de facilitar las actividades que se deberán de realizar durante el curso, observando para ello hábitos de estudio y trabajo y caracterizándose en su actuar, por la responsabilidad,, el interés, la tenacidad, la flexibilidad y la autonomía.

El docente debe proyectar a los estudiantes, una visión innovadora, profesional y competente para facilitar su integración en equipos de desarrollo de aplicaciones web con alta fiabilidad.

El docente debe enfatizar la realidad existente, relacionada con el contexto en el que se ejecutan las aplicaciones web en donde la seguridad es un aspecto fundamental a considerar. Así mismo, se debe concientizar al estudiante que las transacciones realizadas sobre las aplicaciones en internet requieren un soporte tecnológico que garantice su legalidad.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Zacatepec. Abril de 2014	Enrique López Durán Mario Humberto Tiburcio Zuñiga Ofelia Espinosa Baca	Reunión para el diseño de la especialidad para la carrera de Ing. en Tic's

4. Competencias a desarrollar

Competencia general de la asignatura
Integrar los conocimientos y habilidades metodológicas para proponer soluciones de seguridad de cómputo mediante la configuración e instalación de herramientas de seguridad que permitan implementar esquemas de protección de datos en servidores de aplicaciones web.

5. Competencias previas

- Aplicar el uso de comandos y teclas rápidas de algunas herramientas de software.
- Manejar comandos y funciones en varios sistemas operativos.
- Diseñar, modelar e instalar redes de computadoras.
- Aplicar lógica matemática y algorítmica en la solución de problemas informáticos.
- Instalar y configurar sistemas operativos, manejadores de bases de datos, servidores web y servidores de aplicaciones web.

6. Temario

No.	Temas	Subtemas
1	• Seguridad de cómputo	1.1 Introducción a la seguridad de cómputo 1.1.1 Conceptos 1.1.2 Intrusos y ataques 1.2 Políticas de seguridad de cómputo 1.3 Análisis de riesgos y Plan de contingencias 1.4 Mecanismos de protección de datos 1.5 Encriptación
2	Protocolos SSL y TLS	2.1 Seguridad en la capa de transporte 2.2 Protocolo SSL 2.3 Protocolos TLS y DLTS 2.4 Certificados de llave pública y PKIs
3	Seguridad de servidores	3.1 Servidores seguros 3.1.1 Ssh/scp 3.1.2 Https 3.1.3 Correo 3.3 Redes Privadas Virtuales 3.4 Firewalls transversales 3.4.1 Túneles 3.4.2 Proxies 3.5 Detección de intrusos 3.6 Técnicas de Análisis forense
4	Seguridad web	4.1 Seguridad en J2EE 4.2 Seguridad en frameworks 4.2.1 Struts 4.2.2 Spring 4.2.3 Rails 4.3 Seguridad en la arquitectura SOAP.
5	Seguridad del lado del cliente	5.1 Herramientas 5.1.1 Antivirus 5.1.2 Anti spybots 5.1.3 Firewalls de computadoras personales. 5.1.4 Pgp y autenticación de correo 5.2 Implantación de seguridad en computadoras personales y laptops 5.3 Implantación de seguridad en dispositivos móviles 5.4 Seguridad en redes inalámbricas

7. Actividades de aprendizaje

1. Seguridad de cómputo	
Competencias	**Actividades de aprendizaje**
Específica: Aplicará los conceptos de seguridad de cómputo para establecer políticas y procedimientos de seguridad y conocer los mecanismos encriptación. **Genéricas:** Capacidad de análisis y síntesis, capacidad de diseñar modelos abstractos, representa e interpreta conceptos en diferentes formas: gráfica, escrita y verbal, habilidades básicas para elaborar diagramas, solución de problemas, capacidad crítica y autocrítica, trabajo en equipo, compromiso ético, aplicar conocimientos a la práctica.	• Realizar lecturas sobre seguridad de cómputo y contestar cuestionarios • Usando una webquest realizar investigación del análisis de riesgos, planes de contingencia de seguridad de cómputo y materializarla el documento de políticas de seguridad de cómputo para una empresa. • Realizar prácticas y tareas para aplicar los mecanismos de encriptación.

2. Protocolos SSL y TLS	
Competencias	**Actividades de aprendizaje**
Específica: Conocerá los protocolos de seguridad para aplicarlos en la generación de llaves	• Realizar lecturas sobre la seguridad en la capa de transporte y realizar exposiciones. • Realizar exposiciones de los protocolos de SSL y TLS/DTLS

de encriptación, certificados de autenticación y firmas digitales. **Genéricas:** Capacidad de análisis y síntesis, capacidad de diseñar modelos abstractos, representa e interpreta conceptos en diferentes formas: gráfica, escrita y verbal, habilidades básicas para elaborar diagramas, solución de problemas, capacidad crítica y autocrítica, trabajo en equipo, compromiso ético, aplicar conocimientos a la práctica.	para crear un mapa mental de sus características y aplicaciones. • Utilizar herramientas (OpenSSL, PGP) disponibles crear llaves, certificados y firmas • Realizar dinámicas con materiales y/o objetos simples como papel, lápices, etc., que permitan entender los procesos de transporte seguro de datos

3. Seguridad en servidores	
Competencias	**Actividades de aprendizaje**
Específica: Implementar seguridad en servidores y realizar análisis forense. **Genéricas:** Capacidad de análisis y síntesis, capacidad de diseñar modelos abstractos, solución de problemas, capacidad crítica y autocrítica, trabajo en equipo, compromiso ético, aplicar conocimientos a la práctica.	• Investigar y exponer temas relacionados con la seguridad en servidores. • Instalar y configurar servidores con seguridad: SSH, HTTPS, etc., • Configurar cortafuegos simples que permitan filtrar tráfico de red en base a políticas permisivas y restrictivas. • Investigar y comentar en grupo diversas técnicas de detección de intrusos y de análisis forense • Utilizar Objetos de Aprendizaje para entender los procedimientos de configuración de servidores seguros.

4. Seguridad Web	
Competencias	**Actividades de aprendizaje**
Específica: Reconocer las capacidades de la arquitectura J2EE, de los frameworks web y los servicios web en materia de seguridad. **Genéricas:** Capacidad de análisis y síntesis, capacidad de diseñar modelos abstractos, representa e interpreta conceptos en diferentes formas: gráfica, escrita y verbal, habilidades básicas para elaborar diagramas, solución de problemas, capacidad crítica y autocrítica, trabajo en equipo, habilidad de planificar como un todo y diseñar nuevos sistemas, compromiso ético, aplicar conocimientos a la práctica, habilidades de investigación, creatividad e innovación	• Realizar lecturas sobre la seguridad en la arquitectura J2EE. • Usando una webquest realizar investigación de las capacidades de seguridad de las bibliotecas (APIs) de los frameworks MVC de desarrollo web para crear un mapa mental de estas capacidades • Implementará seguridad en una aplicación web usado alguno de los frameworks Web disponibles. • Utilizar Objetos de Aprendizaje para conocer seguridad para aplicaciones web

5. Seguridad del lado del cliente	
Competencias	**Actividades de aprendizaje**
Específica: Implementar la seguridad en computadoras cliente y dispositivos móviles	• Realizar lecturas sobre la seguridad en computadoras personales , redes inalámbricas y dispositivos móviles y contestar cuestionarios • Realizar una investigación de la

Genéricas: Capacidad de análisis y síntesis, capacidad de diseñar modelos abstractos, solución de problemas, capacidad crítica y autocrítica, trabajo en equipo, compromiso ético, aplicar conocimientos a la práctica.	seguridad de la tecnología Wifi y Bluetooth. • Implementará seguridad básica en computadoras personales y laptops. • Configurar la seguridad en dispositivos móviles • Utilizar Objetos de Aprendizaje para conocer el software de seguridad en computadoras personales, redes inalámbricas y dispositivos móviles

8. Prácticas

Práctica No. 1 Elaborar un el análisis de riego, plan de contingencias y políticas de seguridad de cómputo.
Práctica No. 2 Aplicación de los mecanismos de encriptación
Práctica No. 3 Usar software para la generación de llaves y certificados y emisión de firmas digitales
Práctica No.4 Configurar los servidores SSH y HTTPS.
Práctica No.5 Configurar un servidor de correo seguro
Práctica No.6 Implementar un firewall transversal, que incluya túneles y proxies, en una red privada virtual
Práctica No.7 Usar un software de análisis forense.
Práctica No.8 Implementar una aplicación web segura en alguno de los Frameworks disponibles.
Práctica No.9 Implementar seguridad de cómputo en computadoras, laptops y dispositivos móviles.
Práctica No.10 Implementar seguridad en redes inalámbricas configurando un Access Point.

9. Proyecto de asignatura

Se propone la elaboración de un proyecto de asignatura aplicando competencias adquiridas por el estudiante en el curso de su carrera.

- **Fundamentación:** Para la formulación y evaluación del proyecto se sugiere aplicar una metodología propia para ello, que permita obtener la factibilidad de los estudios de mercado y técnico, así como el rendimiento financiero.

- **Planeación:** Se recomienda que los estudiantes se integren en equipo para la elaboración del proyecto de inversión y que planifiquen la realización de cada uno de los temas y requerimientos del proyecto, mediante un cronograma de actividades, responsabilidades y de recursos necesarios.

- **Ejecución:** Se propone que el proyecto de inversión integre en un documento final la justificación, información y resultados pertinentes en cada uno de los temas de la asignatura, integrando además los siguientes apartados: portada, contenido, resumen ejecutivo, resultados, conclusiones y recomendaciones, bibliografía y los anexos y formatos pertinentes.

- **Evaluación:** Se recomienda evaluar el proyecto de asignatura periódicamente, mediante los avances realizados al término de cada uno de los estudios, a través de la revisión del contenido y los requisitos de calidad establecidos. Este proyecto le permitirá al estudiante considerarlo como medio para su titulación integral.

10. Evaluación por competencias

Evaluación:

- La evaluación debe ser permanente y continua.
- Se debe hacer una evaluación diagnostica, formativa y sumativa.
- Se debe aplicar la autoevaluación, evaluación y heteroevaluación.

Se debe generar un portafolio de evidencias, de preferencia en forma digital.

- Evaluación Teórica-Práctica
- Prácticas y tareas

- Avances del proyecto integrador
  - ✓ Análisis
  - ✓ Sustento teórico
  - ✓ Funcionalidad

11. Fuentes de información

1. Egan, M.,The Executive Guide to Information Security, Estados Unidos 2004 Editorial Addison Wesley.
2. Oppliger, R., SSL and TLS Theory and Practice, Estados Unidos 2009, Editorial ArtechHouse.
3. Brown, D., Struts 2 in Action, EstadosUnidos 2007, Editorial MannigPublications.
4. Lüppken, S., Spring Web Flow 2 Web Development, México 2009, Editorial Packtpublishing.
5. Zygmuntowicz, E., Deploying Rails Applications: A Step-by-Step Guide, EstadosUnidos. 2008, Editorial PragmaticProgrammers LLC
6. Dwivedi, I., Mobile Application Security, Estados Unidos 2010, Editorial Mc Graw Hill.