1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad Web
Clave de la asignatura:	CSD-2104
SATCA[1]:	2 – 3 – 5
Carrera:	Ingeniería en Informática

2. Presentación

Caracterización de la asignatura

Esta asignatura aporta al perfil del egresado los conocimientos de ciberseguridad fundamentados en el manejo de la seguridad web, permiten al ingeniero en informática ser un ente de seguridad informática dentro de las empresas a través de la aplicación de estándares internacionales en el manejo de seguridad web, aplicando marcos de referencia de seguridad informática, así como estrategias en el manejo de problemáticas de ciberataques a los sistemas alojados en la nube.

También dentro de las capacidades que aporta esta materia al egresado se encuentra el manejo de protocolos de transmisión de información de datos por internet seguros y el uso de tecnologías necesarias para mantener la seguridad en la trasmisión de datos ya sea internamente dentro de la empresa u organización, así como fuera de la empresa, manteniendo y gestionando el manejo de información y datos digitales a través de la nube.

En esta materia se estudiarán los diferentes tipos de ataques a los sitios web o sistemas en la nube con el fin de que el egresado pueda identificar, prevenir y gestionar los posibles ataques que atenten a la seguridad de los datos que se encuentren en sistemas informáticos en la nube, así como en sitio o páginas web, todo esto en conjunto con herramientas informáticas que permitan realizar escaneos o búsquedas de vulnerabilidades que atenten a la seguridad de la información así como al buen funcionamiento de los sistemas en la nube.

Intención didáctica

La asignatura se encuentra organizada en cuatro temas.

En el primer tema se enfoca en el conocimiento e implementación de estándares de ciberseguridad para aplicación, sistemas y sitios web necesarios para la generación y

[1] Sistema de Asignación y Transferencia de Créditos Académicos

aplicación de estrategias que mejoren la seguridad informática aplicando las normativas que marcan cada uno de los estándares en seguridad web.

El tema dos llamado seguridad en el trasporte de datos trata todo lo referente a los protocolos de comunicación en la nube relacionados con la seguridad, así como de las diferentes tecnologías de certificados digitales necesarios para mejorar los canales de trasporte de información a través de la nube.

El tercer tema es un punto muy importante en la seguridad web debido a que en este se estudian los principales ataques a aplicaciones, sistemas o sitio web, los cuales comprometen el buen funcionamiento de estos, así como la información que estos contienen, por tanto, el conocimiento de los diferentes ciberataques es fundamental con el fin de poder aplicar estrategias de prevención y fortalecimiento de la seguridad que permita mantener la integridad de los datos.

El tema cuatro nos proveerá de conocimientos de las diferentes herramientas de software que permitan la detección de posibles brechas de seguridad en todo lo relacionado a sistemas en la nube con lo cual permitirá que el egresado pueda identificar las problemáticas de seguridad web de una forma oportuna a través de herramientas como sitios de testeo de seguridad, aplicaciones de escaneo de puertos, detección de posibilidad de ciber ataques etc.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Revisión del 26 al 30 de abril del 2021 por parte del Tecnológico Nacional de México Campus Lerdo.	Representantes de los Institutos Tecnológicos Superiores de: Instituto Tecnológico Superior de Lerdo.	Reunión para el Análisis y Diseño por competencias de la Especialidad de “Ciberseguridad”.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
● Conocer los diferentes estándares de seguridad web ● Conoce el estándar internacional de seguridad web OWASP ● Emplear estrategias de fortalecimiento de seguridad web con base en estándares internacionales. ● Detecta los diferentes ataques informáticos que atentan a la seguridad de aplicaciones y sistemas en la nube ● Conocer y entender el uso de herramientas informáticas para la detección de vulnerabilidades y posibles ataques que atentan con la seguridad web.

5. Competencias previas

- Se recomiendan las competencias desarrolladas y adquiridas en las asignaturas relacionadas con el desarrollo de sistemas web, así como de redes en cuanto a protocolos de trasmisión de datos en la nube.
- Habilidades de gestión de información, en la búsqueda y análisis de información de diferentes fuentes.
- Habilidades cognitivas de abstracción, análisis, síntesis y reflexión.

6. **Temario**

No.	Temas	Subtemas
1	Estándares de Seguridad Web	1.1 Introducción a OWASP (Open Web Aplicación Security Proyect) 1.1 Guía de Desarrollo Web OWASP 1.2 OWASP Top 10 1.3 Guía de Testing OWASP
2	Seguridad en el Transporte de Datos	2.1 Comunicaciones Inseguras HTTP 2.2 Protocolo seguro de transferencia de hipertexto (HTTPS) 2.3Certificados Digitales 2.3.1 Secure Sockets Layer (SSL) 2.3.2 Transport Layer Security (TSL)
3	Vulnerabilidades Sitios Web	3.1 Denegación de Servicio (DoS) 3.2 Inyección SQL 3.3 Inyección de Comandos 3.4 Ejecución Remota de Código 3.5 Broken Authentication and Session Management 3.6 Falsificación de petición (CSRF) 3.7 Cross-Site Scripting (XSS) 3.8 Inclusion de Ficheros Remotos (RFI)
4	Herramientas de Escaneo de Vulnerabilidades	4.1 Aplicaciones de Pruebas de Seguridad Web 4.2 Aplicaciones de Pruebas de Sevidor SSL 4.3 Pentesting Sitios Web

7. Actividades de aprendizaje de los temas

Estándares de Seguridad Web	
Competencias	Actividades de aprendizaje
Específica(s): Conocer cuáles son las normativas actúales de seguridad web a partir del estudio los estándares que existen. Genéricas: ● Capacidad de abstracción, análisis y síntesis. ● Capacidad de comunicación oral y escrita. ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Compromiso con la calidad.	● Realizar investigación de estándares de seguridad web ● Realizar análisis y presentación de estándar OWSP ● Realizar análisis y presentación buenas prácticas de desarrollo OWSP ● Realizar plan de trabajo testing de sitio web según estándar OWSP
Seguridad en el Transporte de Datos	
Competencias	Actividades de aprendizaje
Específica(s): Conocer los diferentes protocolos de trasmisión de información a través de internet, así como las diferentes tecnologías para la protección de los datos que viajan a través este. Genéricas: ● Capacidad de abstracción, análisis y síntesis. ● Capacidad de comunicación oral y escrita. ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Compromiso con la calidad.	● Realizar investigación de protocolo HTTP ● Realizar investigación de protocolo HTTPS ● Realizar investigación y presentación de certificado SSL ● Realizar investigación y presentación de certificado TSL ● Generar un certificado gratuito SSL con Lets Encrypt y aplicación en un servidor
Vulnerabilidades Sitios Web	
Competencias	Actividades de aprendizaje
Específica(s): Conocer las principales vulnerabilidades que pueden llegar a tener aplicaciones o sistemas en la nube, con el fin de mejorar la seguridad a partir de la prevención y	● Realizar un ataque DoS Simulado ● Desarrollar una aplicación con vulnerabilidad inyección SQL ● Realizara practica de Ejecución de Código Remoto

mejores prácticas en el desarrollo de software. Genéricas: ● Capacidad de abstracción, análisis y síntesis. ● Capacidad de comunicación oral y escrita. ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Compromiso con la calidad.	● Desarrollar aplicación con vulnerabilidad CSRF ● Desarrollar aplicación con vulnerabilidad XSS
Herramientas de Escaneo de Vulnerabilidades	
Competencias	Actividades de aprendizaje
Específica(s): Conocer las diferentes herramientas disponibles para el escaneo de vulnerabilidades con el fin de analizar vulnerabilidades en los sistemas web y mejorar la seguridad de estos. Genéricas: ● Capacidad de abstracción, análisis y síntesis. ● Capacidad de comunicación oral y escrita. ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Compromiso con la calidad.	● Realizar investigación de mercado de las diferentes herramientas informáticas de detección de vulnerabilidades en sistemas en la nube ● Realizara practica con software para detección de vulnerabilidades en sistemas en la nube ● Realizar practica con software de pruebas de seguridad SSL y TSL ● Realizar investigación de las diferentes herramientas informáticas para realizar Pentesting

8. Práctica(s)

● Realizar investigación de estándares de seguridad web ● Realizar análisis y presentación de estándar OWSP ● Realizar análisis y presentación buenas prácticas de desarrollo OWSP ● Realizar plan de trabajo testing de sitio web según estándar OWSP ● Realizar investigación de protocolo HTTP ● Realizar investigación de protocolo HTTPS ● Realizar investigación y presentación de certificado SSL ● Realizar investigación y presentación de certificado TSL ● Generar un certificado gratuito SSL con Lets Encrypt y aplicación en un servidor ● Realizar un ataque DoS Simulado ● Desarrollar una aplicación con vulnerabilidad inyección SQL ● Realizara practica de Ejecución de Código Remoto

- Desarrollar aplicación con vulnerabilidad CSRF
- Desarrollar aplicación con vulnerabilidad XSS
- Realizar investigación de mercado de las diferentes herramientas informáticas de detección de vulnerabilidades en sistemas en la nube
- Realizara practica con software para detección de vulnerabilidades en sistemas en la nube
- Realizar practica con software de pruebas de seguridad SSL y TSL
- Realizar investigación de las diferentes herramientas informáticas para realizar Pentesting

9. Proyecto de asignatura

Realizar un auditoria de seguridad a un sitio o sistema web implementado los conocimientos de los estándares de seguridad web, así como herramientas informáticas para la detección de vulnerabilidades de seguridad web.

10. Evaluación por competencias

La evaluación debe ser continua, formativa y sumativa por lo que se debe considerar el desempeño en cada una de las actividades de aprendizaje, haciendo especial énfasis en:

- Evaluación diagnóstica.
- Investigación en diversas fuentes de información.
- Desarrollo de actividad(es) y reporte de prácticas.
- Exposición de temas específicos.
- Exámenes teóricos - prácticos que demuestre parte del conocimiento adquirido durante la asignatura.

11. Fuentes de información

- Wichers, D. (2013). Owasp top-10 2013. *OWASP Foundation, February*.
- Montaña Ramos, O. A. (2016). *Síntesis OWASP gestión de riesgos de la seguridad en aplicaciones* (Bachelor's thesis, Universidad Piloto de Colombia).
- Parra, J. D. R. APLICACIÓN DE LAS DIRECTRICES DE DESARROLLO MÓVIL SEGURO DE OWASP.
- Miessler, D. (2015). Securing the internet of things: Mapping attack surface areas using the OWASP IoT top 10. In *RSA Conference*.
- Ochoa Clavijo, B. G. (2011). *Análisis de las técnicas de tunelizado por HTTP para evitar ataques hacker* (Bachelor's thesis, Quito: Universidad Israel, 2011).
- Priego García, L. Estudio del protocolo TLS (Transport Layer Security).
- Naylor, D., Finamore, A., Leontiadis, I., Grunenberger, Y., Mellia, M., Munafò, M., ... & Steenkiste, P. (2014, December). The cost of the" s" in https. In *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies* (pp. 133-140).

- Chomsiri, T. (2007, May). HTTPS hacking protection. In *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)* (Vol. 1, pp. 590-594). IEEE.
- Wagner, D., & Schneier, B. (1996, November). Analysis of the SSL 3.0 protocol. In *The Second USENIX Workshop on Electronic Commerce Proceedings* (Vol. 1, No. 1, pp. 29-40).
- Garfinkel, S., Spafford, G., & Riverol, M. C. (1999). *Seguridad y Comercio en el Web*. McGraw-Hill.
- Aas, J., Barnes, R., Case, B., Durumeric, Z., Eckersley, P., Flores-López, A., ... & Warren, B. (2019, November). Let's Encrypt: An automated certificate authority to encrypt the entire web. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2473-2487).
- Márquez Díaz, J. (2019). Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. *Revista de Bioética y Derecho*, (46), 85-100.
- Chicaiza, G., Ponce, L., & Velázquez Campos, G. Inyección de SQL, caso de estudio OWASP. *Sangolquí, SF*.
- Tovar Valencia, O. (2015). *Inyección de SQL, tipos de ataques y prevención en ASP. NET-C* (Bachelor's thesis, Universidad Piloto de Colombia).
- Blatz, J. (2007). Csrf: Attack and defense. *McAfee® Foundstone® Professional Services, White Paper*.
- Vogt, P., Nentwich, F., Jovanovic, N., Kirda, E., Kruegel, C., & Vigna, G. (2007, February). Cross site scripting prevention with dynamic data tainting and static analysis. In *NDSS* (Vol. 2007, p. 12).