1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad Web
Clave de la asignatura:	CSD-2404
SATCA[1]:	2 – 3 – 5
Carrera:	Ingeniería en Informática

2. Presentación

Caracterización de la asignatura

Esta asignatura proporciona al egresado conocimientos en ciberseguridad, centrándose en la seguridad web. Esto capacita al ingeniero en informática para desempeñarse como experto en seguridad informática en empresas, mediante la implementación de estándares internacionales y marcos de referencia en seguridad web, así como estrategias para enfrentar ciberataques en sistemas alojados en la nube.

Los estudiantes adquieren habilidades para gestionar protocolos seguros de transmisión de datos por Internet y utilizar tecnologías necesarias para garantizar la seguridad en la transferencia de datos, tanto internamente en la empresa u organización como externamente. Esto implica la gestión adecuada de información y datos digitales a través de la nube.

Se exploran diversos tipos de ataques a sitios web y sistemas en la nube para que los egresados puedan identificar, prevenir y gestionar posibles amenazas a la seguridad de los datos en sistemas informáticos en la nube, así como en páginas web. Esto se realiza con el apoyo de herramientas informáticas que permiten realizar escaneos o búsquedas de vulnerabilidades que puedan comprometer la seguridad de la información y el funcionamiento de los sistemas en la nube.

Intención didáctica

La asignatura se encuentra organizada en cinco 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 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

[1] Sistema de Asignación y Transferencia de Créditos Académicos

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 suministrará conocimientos sobre las diversas tecnologías utilizadas en la criptografía de sistemas web, así como los distintos algoritmos de cifrado necesarios para preservar la integridad de los datos. Además, se abordarán temas relacionados con la autenticación de usuarios, un aspecto crucial en los sistemas web.

Durante el quinto y último tema, se explorarán las implicaciones de las nuevas tecnologías web en la seguridad informática, utilizando como punto de partida los datos y conceptos previamente discutidos en la materia.

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, Payment Card Industry Data Security Standard e ISO/IEC 27001 ● Emplear estrategias de fortalecimiento de seguridad web con base en estándares internacionales. ● Conocer los protocolos de seguridad inalámbrica. ● Comprender la importancia el uso de certificados digitales y sus implicaciones en las seguridad de los sitemas web. ● Usar diferentes algoritmos de cifrado de datos para la seguridad de los datos ● Conocer las tendencias de las nuevas tecnologías y su impacto en 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 1.4 PCI DSS (Payment Card Industry Data Security Standard) 1.4 ISO/IEC 27001 Norma para la gestión de la seguridad de la información
2	Seguridad en el Transporte de Datos	2.1 Comunicaciones Inseguras HTTP 2.2 Protocolos de seguridad inalámbrica (WPA2, WPA3, etc.) 2.3 Protocolo seguro de transferencia de hipertexto (HTTPS) 2.4Certificados Digitales 2.3.1 Secure Sockets Layer (SSL) 2.3.2 Transport Layer Security (TSL) 2.3.3 Tipos de certificados SSL/TLS (DV, OV, EV)
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	Criptografía y Autenticación	4.1 Algoritmos criptográficos simétricos (AES, DES, 3DES, etc.) 4.2 Algoritmos criptográficos asimétricos (RSA, ECC, etc.) 4.3 Funciones hash criptográficas (SHA-256, MD5, etc.) 4.3. Autenticación de usuarios: contraseñas seguras, multifactor y biometría
5	Tendencias y Futuro de la Seguridad Web	5.1 Seguridad en Dispositivos IoT y Web de las Cosas (Web of Things) 5.2 Desafíos emergentes y técnicas avanzadas de defensa

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 análisis y presentación de estándar PCI DSS (Payment Card Industry Data Security Standard) ● 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:	● Realizar investigación de protocolo HTTP ● Realizar investigación de protocolo HTTPS ● Realizar investigación y presentación de certificado SSL ● Realizar investigación y presentación de certificado TSL

● 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.	● 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 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.	● 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
Criptografía y Autenticación	
Competencias	Actividades de aprendizaje
Específica(s): Conocer las diferentes tecnologías empleadas en la criptografía de datos que permiten la seguridad de los datos en sistema web. 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 los diferentes algoritmos criptográficos simétricos (AES, DES, 3DES). ● Realizara practica de generación de hash criptográfico SHA-256 ● Realizara practica de cifrado de datos con MD5 ● Realizar investigación de contraseñas seguras, multifactorial y biometría

Tendencias y Futuro de la Seguridad Web	
Competencias	Actividades de aprendizaje
Específica(s): Conocer cuáles son las tendencias que marcan el futuro de la seguridad informática y sus repercusiones en el uso y aplicación de nuevas tecnologías. 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 sobre las tendencias de seguridad en dispositivos IoT y Web de las Cosas (Web of Things) ● Realizar un ensayo sobre la perspectiva que el alumno tiene de las nuevas tecnologías web y su impacto en la seguridad.

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 análisis y presentación de estándar PCI DSS (Payment Card Industry Data Security Standard)
- 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 los diferentes algoritmos criptográficos simétricos (AES, DES, 3DES).
- Realizara practica de generación de hash criptográfico SHA-256
- Realizara practica de cifrado de datos con MD5
- Realizar investigación de contraseñas seguras, multifactorial y biometría
- Realizar investigación de sobre las tendencias de seguridad en dispositivos IoT y Web de las Cosas (Web of Things)
- Realizar un ensayo sobre la perspectiva que el alumno tiene de las nuevas tecnologías web y su impacto en la seguridad.

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.
- Morse, E. A., & Raval, V. (2008). PCI DSS: Payment card industry data security standards in context. *Computer Law & Security Review*, *24*(6), 540-554.
- Garzón Ramos, L. F. (2023). Payment Card Industry Data Security Standard (PCI DSS) and Network Security.
- Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL*, *28*(5).
- 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).
- Vargas, Y. T. M., & Mnedez, H. A. M. (2015). Comparación de algoritmos basados en la criptografía simétrica DES, AES y 3DES. *Mundo Fesc*, *5*(9), 14-21.
- Gilbert, H., & Handschuh, H. (2003, August). Security analysis of SHA-256 and sisters. In *International workshop on selected areas in cryptography* (pp. 175-193). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Dobbertin, H. (1996). Cryptanalysis of MD5 compress. *rump session of Eurocrypt*, *96*, 71-82.
- González García, A. J. (2017). IoT: Dispositivos, tecnologías de transporte y aplicaciones.