

## 1. Datos Generales de la asignatura

<b>Nombre de la asignatura:</b>	<b>Seguridad en los Sistemas de Información</b>
<b>Clave de la asignatura:</b>	<b>ESD-2105</b>
<b>SATCA<sup>1</sup>:</b>	<b>2-3-5</b>
<b>Carrera:</b>	<b>Ingeniería Informática</b>

## 2. Presentación

<p><b>Caracterización de la asignatura:</b> La presente asignatura aporta al perfil de egreso del Ingeniero Informático, los conocimientos necesarios para facilitar los aspectos relacionados con la seguridad en base de datos y en aplicaciones web, así como las herramientas y módulos de seguridad más utilizadas en la industria.</p> <p>La importancia de esta asignatura involucra al alumno en los conceptos básicos de la seguridad en los sistemas de información que desarrollará, así como los ciclos de vida de la misma, de las técnicas empleadas por la industria de desarrollo de software para alcanzar una mayor seguridad en el manejo de la información, además de enrolar al estudiante en las herramientas de seguridad empleadas en el desarrollo de software.</p>
<p>Los conocimientos de la materia de seguridad de sistemas de información se relacionan con las materias de:</p> <p><b>Seguridad Informática:</b></p> <p><b>Tema:</b> Directrices de Seguridad Informática</p> <p><b>Competencia específica:</b> Analiza las distintas técnicas y directrices de la seguridad informática para implementar soluciones integradoras en la protección de los activos críticos de la organización permitiendo la continuidad del servicio.</p>
<p><b>Intención didáctica</b></p> <p>Esta materia el docente participará de forma teórico práctica, explicando el contenido de cada una de las unidades para que el alumno comprenda la importancia de manejar la seguridad en los sistemas de información y visualice la importancia de realizar sistemas con un alto nivel de seguridad.</p> <p>La materia consta de cuatro unidades en las que se dan a conocer diferentes aspectos relacionados con la importancia e implementación de la seguridad que se debe de manejar en los sistemas.</p> <p>En la primera unidad se dan a conocer los conceptos básicos de la seguridad de sistemas de información, así como la importancia y beneficios de su implementación en</p>

<sup>1</sup> Sistema de Asignación y Transferencia de Créditos Académicos

los sistemas de información del mundo globalizado, esto permitirá en los alumnos tener presente esta característica en el proceso de desarrollo de software.

En la unidad dos el alumno conocerá los aspectos de seguridad que se deben tomar en cuenta en las aplicaciones web, así como también las consecuencias de no implementar la seguridad en estos sistemas, además de conocer las nuevas formas de negocio y beneficios de estos sistemas.

En la unidad tres se darán a conocer los aspectos relacionados con la seguridad en base de datos, así como las herramientas y módulos de seguridad de las bases de datos más utilizadas en la industria.

En la cuarta unidad se aborda la construcción de un ejercicio práctico bajo las herramientas y técnicas apropiadas de seguridad en los sistemas de información aplicando los conceptos adquiridos en las unidades anteriores.

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

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico Superior de Ciudad Serdán, Junio de 2021.	Mtra. Norma Angélica Fuentes Sandoval. Lic. Oscar Cortes Sánchez. Mtro. José Misrhaim Sandoval Lozada. Mtro. Adán Canico Hernández Mtro. Isaac Alberto Aldave Rojas Lic. Gerardo Espinoza Ramírez Ing. Porfirio Medina de la Rosa Lic. María Eugenia Cisneros Aguilar	

#### 4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
<ul style="list-style-type: none"> <li>Conoce, analiza e implementa técnicas de seguridad informática aplicadas a las bases de datos y a los sistemas de información para el resguardo de la integridad de la información de las empresas.</li> </ul>

#### 5. Competencias previas

<ul style="list-style-type: none"> <li>Usar manejadores de base de datos mediante SQL.</li> <li>Conoce y manipula el lenguaje SQL.</li> <li>Aplica principios de ingeniería de software en etapas de análisis y diseño de sistemas de información.</li> <li>Aplica normas y estándares de calidad en el entorno del desarrollo de sistemas de información.</li> <li>Programación orientada a objetos</li> <li>Programación web.</li> </ul>
--

#### 6. Temario

No.	Temas	Subtemas
1.	Fundamentos de seguridad de sistemas de información	1.1. Definiciones y conceptos de gestión de seguridad de la información 1.2. Confidencialidad, Integridad y Disponibilidad 1.3. Marco normativo nacional e internacional
2.	Seguridad en aplicaciones web	2.1. Proceso de Código Seguro 2.2. Tipos de desastres que deben considerarse 2.3. Análisis de Impacto del Negocio 2.4. Desarrollo de estrategias de mitigación 2.5. Plan de continuidad del negocio/ Plan de recuperación 2.6. Entrenamiento, testeo y auditoría del Plan de Continuidad del Negocio
3.	Seguridad en base de datos	3.1 Tipos de Bases de Datos. 3.2 Seguridad en Base de datos. 3.3 Modelos de Seguridad. 3.4 Características de las bases de datos seguras 3.4.1 Confidencialidad en las Bases de datos. 3.4.2 Integridad en las Bases de datos. 3.4.3 Disponibilidad en las Bases de datos. 3.5 Herramientas para el análisis de vulnerabilidades en Bases de datos. 3.6 Funciones del Administrador de la Base de datos.

4.	Implementación de seguridad empresarial	4.1 Código seguro a través de OWASP 4.2 Protocolos de seguridad web.
----	---	---

## 7. Actividades de aprendizaje de los temas

Nombre de tema: Fundamentos de seguridad de sistemas de información	
Competencias	Actividades de aprendizaje
<p>Específica(s): Conoce técnicas de seguridad informática aplicadas a las bases de datos y a los sistemas de información para el resguardo de la integridad de la información de las empresas.</p> <p><b>Genéricas</b></p> <ul style="list-style-type: none"> <li>Habilidades para buscar, procesar y analizar información procedente de diversas fuentes.</li> <li>Capacidad de abstracción, análisis y síntesis.</li> <li>Capacidad de aprender por cuenta propia.</li> <li>Capacidad de comunicación oral y escrita.</li> <li>Capacidad de trabajo en equipo</li> </ul>	<ul style="list-style-type: none"> <li>Investigar en diversas fuentes de información el concepto de seguridad para participar y discutir en grupo y enviar documento impreso al sitio de la asignatura o vía correo electrónico.</li> <li>Realizar una tabla comparativa de las distintas técnicas de seguridad aplicables a los sistemas.</li> <li>Realizar un Análisis de Riesgo de una organización de la entidad y exponerlo en clase.</li> <li>Conocer las principales amenazas que una empresa se expone con el manejo de sistemas de información.</li> </ul>
Nombre de tema: Seguridad en aplicaciones web	
Competencias	Actividades de aprendizaje
<p>Específica(s): Implementa técnicas de seguridad a una aplicación web de manera segura.</p> <p><b>Genéricas</b></p> <ul style="list-style-type: none"> <li>Habilidades para buscar, procesar y analizar información procedente de diversas fuentes.</li> <li>Capacidad de abstracción, análisis y síntesis.</li> <li>Capacidad de aprender por cuenta propia.</li> <li>Capacidad de comunicación oral y escrita.</li> <li>Capacidad de trabajo en equipo</li> </ul>	<ul style="list-style-type: none"> <li>Realizar un reporte de lectura acerca de las técnicas de seguridad que pueden aplicarse a un sitio web.</li> <li>Investigar acerca de la evolución de las técnicas de seguridad aplicables a los sistemas de información.</li> <li>En equipos de trabajo realizar un reporte de la visita a un sitio web o sistema de información que describa el nivel de seguridad utilizado.</li> </ul>

Nombre de tema: Seguridad en base de datos	
Competencias	Actividades de aprendizaje
<p><b>Específica(s):</b> Conoce y aplica los aspectos relacionados con la seguridad en base de datos, así como las herramientas y técnicas apropiadas.</p> <p><b>Genéricas</b></p> <ul style="list-style-type: none"> <li>Habilidades para buscar, procesar y analizar información procedente de diversas fuentes.</li> <li>Capacidad de abstracción, análisis y síntesis.</li> <li>Capacidad de aprender por cuenta propia.</li> <li>Capacidad de comunicación oral y escrita.</li> <li>Capacidad de trabajo en equipo</li> </ul>	<ul style="list-style-type: none"> <li>Por equipos de trabajo realizan la propuesta de aplicación de técnicas, modelos o metodologías de seguridad en base de datos.</li> <li>Elaborar un modelo de datos con problemas específicos de un entorno real que involucren técnicas de seguridad.</li> </ul>
Nombre de tema: Implementación de seguridad empresarial	
Competencias	Actividades de aprendizaje
<p><b>Específica(s):</b> Desarrolla una aplicación web o de escritorio implementando técnicas de seguridad enfocadas a base de datos.</p> <p><b>Genéricas</b></p> <ul style="list-style-type: none"> <li>Habilidades para buscar, procesar y analizar información procedente de diversas fuentes.</li> <li>Capacidad de abstracción, análisis y síntesis.</li> <li>Capacidad de aprender por cuenta propia.</li> <li>Capacidad de comunicación oral y escrita.</li> <li>Capacidad de trabajo en equipo</li> </ul>	<ul style="list-style-type: none"> <li>Por equipos de trabajo crean y desarrollan un proyecto web o de escritorio con la implementación de una o varias técnicas de seguridad que le permitan poner en práctica los conocimientos adquiridos durante el semestre.</li> </ul>

## 8. Práctica(s)

- Investigar las herramientas y técnicas de seguridad a base de datos.
- Investigar ejemplos de sistemas que presenten un mayor número de vulnerabilidades en temas de seguridad de información.
- Manipular operaciones de inserción, actualización y eliminación de registros en una base de datos con y sin otorgamiento de permisos.
- Implementar procesos que reduzcan operaciones no permitidas por los administradores de base de datos.
- Investigar otras herramientas que permitan identificar debilidades en los sitios web o sistemas de información.

## 9. Proyecto Integrador

### **Análisis y diseño de un sistema de información que permita implementar e identificar vulnerabilidades de integridad de información.**

- **Fundamentación:** Actualmente el desarrollo de aplicaciones de software tiene una gran demanda, tanto en las organizaciones como en la sociedad, esto implica la responsabilidad de ofrecer sistema con un alto nivel de seguridad, la cual, es una característica que debe tener todo sistema, por lo que permite a sus usuarios alcanzar objetivos específicos (como escribir una carta o enviar un mensaje SMS) con efectividad, eficiencia y satisfacción. Es decir, que cuanto mejor permita hacer algo un sistema mayor seguridad tendrá.
- **Planeación:** el análisis y diseño de la aplicación se desarrollará basándose en el Ciclo de vida de la ingeniería de usabilidad según Mayhew, en el cual, en cada fase implementarán técnicas y herramientas que les permita evaluar la seguridad en el sistema de información.
- **Ejecución:** El desarrollo del proyecto se deberá trabajar en equipo y llevar a cabo cada una de las tareas establecidas en las etapas del ciclo de vida según Mayhew. Se propone el uso de herramientas y técnicas de software que permitan apoyar el desarrollo del sistema con un alto nivel de seguridad que será evaluado por los usuarios.
- **Evaluación:** El proyecto integrador será evaluado a partir de la cuarta unidad, con la propuesta de aplicación a desarrollar, así mismo se irá evaluando el avance del sistema en base a los siguientes puntos:
  - Dinámica de equipo:
    - Capacidad de organización.
    - Colaboración entre sus miembros.
    - Resolución de conflictos.

- Evidencias de actividades:
  - Entrega en tiempo y forma de las evidencias correspondientes a cada etapa del ciclo de vida de usabilidad.
  - Entrega de observaciones y correcciones realizadas a las evidencias.
  - Documentación final del proyecto.

## 10. Evaluación por competencias

- Evaluación diagnóstica.
- Se debe generar un portafolio de evidencias, de preferencia en formato digital.
- Exposición de temas por parte de los alumnos con apoyo y asesoría del profesor.
- Evaluación trabajos de investigación entregados en forma escrita.
- Evaluación por unidad para comprobar el manejo de aspectos teóricos.
- Evaluación de las actividades por unidad, considerando los temas que ésta contiene.
- Reporte escrito de un proyecto final que describa las actividades realizadas y las conclusiones del mismo.

## 11. Fuentes de información

1. PPSILON, (2011) "Seguridad informática - Ethical Hacking" Edit ACISSI
2. EDWARDS, CHRIS; JOHN WARD y ANDY BYTHEWAY. Fundamentos de Sistemas de Información. 2da. Edición. Ed. Prentice Hall. 1998.
3. Kaufman, Charlie; Perlman, Radia; Spencer, Mike. "Network Security: Private Communication in a Public World". Prentice Hall.
4. KENDALL, KENNETH E. Y KENDALL, JULIE E. Análisis y Diseño de Sistemas. 6ª Edición; Ed. Pearson Educación México. 2005.
5. Larman, Craig. UML y Patrones. 2ª. edición. Pearson
6. Laudon K. Laudon, J.; Sistema de Información Gerencial. Administración de la Empresa Digital. 10ª Edición; Ed. Pearson Prentice Hall. 2008.
7. PRESSMAN, ROGER S.; Ingeniería de software un Enfoque práctico; Ed. Mc. Graw. Hill. 2007.

Digitales:

8. Aguirre, Jorge R. "Libro Electrónico de Seguridad Informática y Criptografía". (2006); Depósito Legal M-10039-2003. Disponible en Internet en [http://www.criptored.upm.es/guienteoria/gt\\_m001a.htm](http://www.criptored.upm.es/guienteoria/gt_m001a.htm)
9. Zimmermann, P. (1999), "An Introduction to Cryptography". Network Associates. available at: <ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf>