

1. Datos Generales de la asignatura

Nombre de la asignatura:	Administración de la Seguridad en Aplicaciones.
Clave de la asignatura:	ASD-1905
SATCA¹:	2-3-5
Carrera:	Ingeniería en Sistemas Computacionales.

2. Presentación

Caracterización de la asignatura
La asignatura de Administración y Seguridad en Aplicaciones aporta al perfil del Ingeniero en Sistemas Computacionales la habilidad de establecer técnicas y estrategias que garanticen la seguridad informática en el ámbito donde se desempeñe. La importancia de esta materia para un Ingeniero en Sistemas Computacionales es la de aplicar los conocimientos adquiridos para utilizar las herramientas informáticas que ayuden a mejorar la calidad, confidencialidad, integridad y persistencia de la información que se maneja en las instituciones, la industria y en los negocios. Esta asignatura agrupa los conocimientos necesarios para diseñar e implementar técnicas y algoritmos de cifrado que permitan ocultar la información para garantizar su confidencialidad. Es una asignatura que requiere la aplicación de políticas, normas y estándares para administrar la seguridad informática, evitando el acceso a intrusos, detectando amenazas a la información.
Intención didáctica
Los temas de la asignatura están integrados de tal forma para que el alumnado sea capaz de analizar, diseñar y aplicar algoritmos de cifrado y establecer políticas y normas para su uso antes, durante y después de alguna amenaza a los sistemas de información. En las actividades de aprendizaje sugeridas, se propone la formalización de los conceptos a partir de experiencias; se busca que el alumnado tenga el primer contacto con el concepto en forma concreta y sea a través de la observación, la reflexión y la discusión; que se dé la formalización, la resolución de problemas se hará después de este proceso. El alumnado evaluará los diferentes algoritmos de cifrado y será capaz de elegir el más adecuado para aplicarlo en un caso real. También conocerá los problemas de seguridad

¹ Sistema de Asignación y Transferencia de Créditos Académicos

en las bases de datos, el control de acceso y las arquitecturas de seguridad, asimismo aplicará los conceptos estudiados en un caso real.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Tecnológico de Estudios Superiores de Coacalco Agosto del 2013.	Docentes de la Academia de la Ingeniería en Sistemas Computacionales del TESCO	Análisis y formulación de competencias para la especialidad de Auditoría y Seguridad Informática de la Ingeniería de Sistemas Computacionales.
Tecnológico de Estudios Superiores de Coacalco Agosto del 2015.	Representantes: Tecnológico de Estudios Superiores de Coacalco	Actualización del módulo de
Tecnológico de Estudios Superiores de Coacalco Junio del 2019.	Docentes de la Academia de la Ingeniería en Sistemas Computacionales del TESCO	la especialidad de Auditoría y Seguridad Informática de la Ingeniería en Sistemas Computacionales.
TESCo, Coacalco Estado de México. Fecha: 01 al 14 de junio de 2019	Representantes: Tecnológico de Estudios Superiores de Coacalco	

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
- Analiza, diseña y aplica algoritmos de cifrado. - Establece políticas y normas para su uso antes, durante y después de alguna amenaza a los sistemas de información

5. Competencias previas

- Conoce las normas, marcos y estándares utilizados para la auditoría informática. - Identifica los principios de control interno y su relación con la auditoría informática. - Conoce las propiedades ACID en las bases de datos. - Identifica conceptos básicos de Sistemas de Información con bases de datos. Implementa perfiles de usuario para acceso a un servidor de base de datos.
--

6. Temario

No.	Temas	Subtemas
1	Introducción a la Seguridad informática.	1.1 Introducción y conceptos. 1.2 Teoría de la información. 1.3 Criptología. 1.3 Misión, políticas, normas y mecanismos de seguridad.
2	Teoría de números.	2.1 Matemática discreta y congruencias. 2.2 Aritmética modular. 2.2.1 Operaciones 2.2.2 Cálculo de inversos 2.2.3 Exponenciación 2.2.4 Sistemas de congruencias 2.2.5 Teorema chino de restos
3	Cifrado de datos.	3.1 Conceptos Matemáticos. 3.2 Clasificación. 3.3 Sistemas de Criptografía clásica. 3.4 Sistemas de Criptografía Moderna. 3.4.1 Criptografía Simétrica. 3.4.2 Cifrado en Bloque. 3.4.3 Cifrado por Flujo. 3.5 Criptografía Asimétrica. 3.5.1 Criptografía de Llave Pública. 3.5.2 Esquema Diffie-Hellman. 3.6 Funciones Hash. 3.7 Estenografía.
4	Seguridad en Bases de datos	4.1 Problemas de seguridad en bases de datos. 4.2 Amenazas a la seguridad en bases de datos. 4.3 Control de acceso y arquitecturas de seguridad. 4.3.1 Privilegios. 4.4 Ataques a los sistemas de base de datos.

7. Actividades de aprendizaje de los temas

Unidad 1. Introducción a la seguridad informática	
Competencias	Actividades de aprendizaje
Específica(s): Comprende los conceptos básicos de la seguridad informática y el cifrado de datos.	- Investigar los conceptos básicos de criptografía y seguridad informática. - Investigar el concepto de entropía.

Explica las políticas y normas que brindan Seguridad mediante modelos de encriptación. Genéricas: • Capacidad de análisis y síntesis. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Capacidad crítica y autocrítica. • Compromiso ético	• Analizar la complejidad de los algoritmos para poder elegir el menos vulnerable. • Realizar un cuadro comparativo de las diferentes normas y estándares para la seguridad informática.
Unidad 2. Teoría de números	
Competencias	Actividades de aprendizaje
Específica(s): Aplica la teoría de números para generar claves de cifrado y descifrado de datos. Genéricas: • Capacidad de análisis y síntesis. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Capacidad crítica y autocrítica. • Capacidad de generar nuevas ideas (creatividad). • Capacidad de aplicar los conocimientos en la práctica. • Compromiso ético	• Investigar el concepto de congruencia y sus aplicaciones para la generación de claves de cifrado. • Analizar el comportamiento de la aritmética modular y sus aplicaciones en el cifrado de datos. • Analizar los diferentes procedimientos para la resolución de problemas que involucren números muy grandes. Desarrollar prácticas de laboratorio que le permitan utilizar diversas técnicas en la resolución de problemas de generación de claves de cifrado con ayuda de software.
Unidad 3. Cifrado de datos	
Competencias	Actividades de aprendizaje
Específica(s): Aplica diferentes tipos de cifrado en diferentes lenguajes de programación y sistemas operativos para garantizar la seguridad e integridad de la información. Genéricas:	• Investigar los sistemas de criptografía clásica, simétrica, asimétrica, funciones Hash y esteganografía. • Determinar ventajas y desventajas de los distintos sistemas de criptografía. • Diseñar e implementar un algoritmo donde se aplique alguna técnica de criptografía.

• Capacidad crítica y autocrítica. • Trabajo en equipo • Habilidades interpersonales • Capacidad de comunicarse con profesionales de otras áreas - Compromiso ético	
Unidad 4. Seguridad en bases de datos	
Competencias	Actividades de aprendizaje
Específica(s): Utiliza técnicas de seguridad en base de datos a fin de garantizar la integridad y confiabilidad de la información Genéricas: • Capacidad de análisis y síntesis. • Capacidad de aplicar los conocimientos en la práctica • Habilidades de investigación • Capacidad de generar nuevas ideas (Creatividad) • Capacidad de diseñar y gestionar proyectos • Compromiso ético	• Investigar y analizar los diferentes tipos de ataques a sistemas de bases de datos. • Investigar los diferentes tipos de control de acceso a sistema de base de datos. • Investigar y analizar técnicas de prevención de ataques a sistemas de bases de datos. • Investigar las vulnerabilidades hacia los sistemas

8. Práctica(s)

• Realizar ejercicios de congruencias matemáticas. • Realizar un caso práctico de problemáticas y definición de la seguridad informática, utilizando las políticas y normativas de la seguridad. • Realizar un cifrado por desplazamiento puro. • Realizar un cifrado simétrico para las debilidades y ataques del DES. • Realizar un cifrado asimétrico utilizando el RSA. • Realizar el MD5 utilizando la función HASH. • Realizar un sistema de información que cumpla los métodos aplicables a la seguridad de la Base de Datos.
--

9. Proyecto de asignatura

El objetivo del proyecto que planteé 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:** marco referencial (teórico, conceptual, contextual, legal) en el cual se fundamenta el proyecto de acuerdo con un diagnóstico realizado, mismo que permite a los estudiantes lograr la comprensión de la realidad o situación objeto de estudio para definir un proceso de intervención o hacer el diseño de un modelo.
- **Planeación:** con base en el diagnóstico en esta fase se realiza el diseño del proyecto por parte de los estudiantes con asesoría del docente; implica planificar un proceso: de intervención empresarial, social o comunitario, el diseño de un modelo, entre otros, según el tipo de proyecto, las actividades a realizar los recursos requeridos y el cronograma de trabajo.
- **Ejecución:** consiste en el desarrollo de la planeación del proyecto realizada por parte de los estudiantes con asesoría del docente, es decir en la intervención (social, empresarial), o construcción del modelo propuesto según el tipo de proyecto, es la fase de mayor duración que implica el desempeño de las competencias genéricas y específicas a desarrollar.
- **Evaluación:** es la fase final que aplica un juicio de valor en el contexto laboral-profesión, social e investigativo, ésta se debe realizar a través del reconocimiento de logros y aspectos a mejorar se estará promoviendo el concepto de “evaluación para la mejora continua”, la metacognición, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10. Evaluación por competencias

- Evaluación teórica
- Evaluación continua
- Exposiciones
- Proyecto integrador
- Reporte de prácticas de laboratorio
- Ejercicios prácticos sobre algoritmos de cifrado.

11. Fuentes de información

- A., S. R. (2003). *CyberEthics: morality and law in cyberspace*. Jones and Bartlett Publishers.
- Al], D. G. (2007). *La seguridad de la Información*. Editorial Limusa.
- Álvaro, G. V. (2007). *Enciclopedia de la seguridad informática*. Alfaomega Grupo Editor.
- César, P. L. (2008). *MySQL para Windows y Linux*. Alfaomega Grupo Editor.
- Danielle, R. (2009). *Windows Server 2008: manual de referencia*. McGraw-Hill Interamericana Editores.
- Enrique, N. G. (2007). *Delitos informáticos*. Editorial Porrúa.
- Fernando, P. R. (2007). *Hacking y seguridad en Internet*. Alfaomega Grupo Editor.
- Jakub, Z. (2005). *Cracking sin secretos: ataque y defensa de software*. Alfaomega Grupo Editor.
- John, R. (2002). *Guía esencial Linux*. Pearson Educación.
- Julio, G. L. (2007). *Administración de sistemas operativos Windows y Linux: un enfoque práctico*. Alfaomega.
- Manuel, D. S. (2009). *GNU/Linux y el software libre y sus multiples aplicaciones*. Alfaomega Grupo Editor.
- Martín, S. E. (2010). *Ethical hacking: un enfoque metodológico para profesionales*. Alfaomega Grupo Editor Argentino.
- Patt, M. M. (2002). *Seguridad digital: estrategias de defensa digital para proteger la reputación y la cuota del mercado de su compañía*. McGraw-Hill/Interamericana de España.
- Sebastián, S. P. (2008). *Linux, guía práctica*. Alfaomega Grupo Editor.
- Vicente, A. C. (2007). *Seguridad de la información: expectativas, riesgos y técnicas de protección*. Editorial Limusa.
- Yago, F. H. (2009). *AAA/ RADIUS/ 802.1x Sistemas basados en la autenticación en Windows y Linux/ GNU: seguridad máxima*. Alfaomega Grupo Editor.
- C.A, H. (2016). *FUNDAMENTALS OF CRYPTOLOGY A Professional Reference and Interactive Tutorial*. KLUWER ACADEMIC PUBLISHERS.
- Nakov, S. (2018). *Practical Cryptography for Developers*. MIT license.
- Sweigart, A. (2013). *Hacking Secret Ciphers with Pytho*. Creative Commons Attribution-Noncommercial-Share.