

1. Datos Generales de la asignatura

Nombre de la asignatura:	Administración de la Seguridad en Comunicaciones.
Clave de la asignatura:	ASH-1901
SATCA¹:	1-3-4
Carrera:	Ingeniería en Sistemas Computacionales.

2. Presentación

Caracterización de la asignatura
La asignatura de Administración y Seguridad en Comunicaciones aporta al perfil del Ingeniero en Sistemas Computacionales la habilidad de elegir técnicas, estrategias y normas que ayuden a mejorar la seguridad informática, en el uso de las Telecomunicaciones en 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 orientadas al hardware y software 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, implementar y configurar estrategias y herramientas que ayuden a mejorar la confidencialidad, integridad, disponibilidad y autenticación de los datos durante su transferencia haciendo uso de las Telecomunicaciones, identificando los diferentes elementos que se pueden utilizar para estos procesos. Es una asignatura que requiere comprender la configuración de diferentes sistemas operativos de red para incrementar la seguridad al acceder a los sistemas informáticos de la organización.
Intención didáctica
Los temas de la asignatura están integrados para que el alumnado sea capaz de conocer y configurar sistemas operativos seguros en un entorno de red. 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

¹ Sistema de Asignación y Transferencia de Créditos Académicos

con el concepto de seguridad informática 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.

Se abordan conceptos básicos de la problemática que concierne la seguridad informática desde el punto de vista de las Telecomunicaciones, además de dar un panorama general de los factores a considerar para temas posteriores.

El alumnado debe identificar y configurar los protocolos utilizados en una conexión a Internet para garantizar la comunicación y seguridad durante la transferencia de información.

En esta asignatura el alumnado conocerá y aplicará herramientas que permiten detectar el acceso no autorizado a los sistemas informáticos, así como llevar el registro y monitoreo del uso de las telecomunicaciones; documentará los sucesos que se presentan durante una amenaza para la elaboración o corrección de las políticas de seguridad empleadas.

El alumnado evaluará los diferentes sistemas operativos de red para elegir el más adecuado acorde al tipo de información y aplicaciones donde se desee implementar. Asimismo, aplicará los conceptos vistos a un caso real configurando los perfiles adecuados de acuerdo con cada usuario.

En el transcurso de las actividades programadas es muy importante que el alumnado aprenda a valorar las actividades que lleva a cabo y entienda que se debe conducir con ética y valores y en consecuencia actúe de una manera profesional; de igual manera, aprecie la importancia del conocimiento y los hábitos de trabajo; desarrolle la precisión y la curiosidad, la puntualidad, el entusiasmo y el interés, la tenacidad, la flexibilidad y la autonomía.

Es necesario que el profesor ponga atención y cuidado en estos aspectos en el desarrollo de las actividades de aprendizaje de esta asignatura, que promueva el establecimiento de relaciones objetivas entre los conocimientos que el alumnado va construyendo y la realidad social y profesional de su entorno y así vaya ampliando su cultura.

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	Representantes:	

Agosto del 2015. Tecnológico de Estudios Superiores de Coacalco Junio del 2019. TESCo, Coacalco Estado de México. Fecha: 01 al 14 de junio de 2019	Tecnológico de Estudios Superiores de Coacalco Docentes de la Academia de la Ingeniería en Sistemas Computacionales del TESCo Representantes: Tecnológico de Estudios Superiores de Coacalco	Actualización del módulo de la especialidad de Auditoría y Seguridad Informática de la Ingeniería en Sistemas Computacionales.
---	---	---

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
- Identifica los principales conceptos acerca de la Seguridad Informática. - Estudia y conoce las herramientas de uso actual para la administración de la seguridad en Telecomunicaciones. - Localiza los principales elementos críticos de la red de una organización y evalúa los principales riesgos de seguridad. - Conoce los principales pasos a seguir para elaborar un proyecto de Gestión de la Seguridad de la Información. - Toma decisiones para elegir las medidas de seguridad más apropiadas ante un determinado escenario de riesgos.

5. Competencias previas

- Conoce los modelos de referencia de redes (OSI y TCP/IP) - Conoce los estándares y normas vigentes para el diseño de una red. - Identifica los elementos básicos de una red informática.
--

6. Temario

No.	Temas	Subtemas
1	Introducción a la Seguridad Informática.	1.1 Concepto de seguridad informática. 1.2 Visión global de la seguridad informática. 1.3 Generalidades sobre la seguridad. 1.4 Tipos de seguridad informática. 1.5 Normas y estándares para la seguridad informática.
2	Comunicaciones Seguras y la Seguridad en Internet.	2.1 Riesgos 2.2 Amenazas. 2.3 vulnerabilidades. 2.4 Tipos de ataques. 2.5 Fases de un ataque informático.

		2.6 Planeación de un SGSI.
3	Herramientas para la seguridad informática.	3.1 Herramientas de reconocimiento. 3.2 Herramientas de escaneo. 3.3 Herramientas para ganar acceso. 3.4 Herramientas para mantener acceso. 3.5 Herramientas para borrar huellas. 3.6 Contramedidas.
4	Configuración de un Sistema Operativo para la Seguridad	4.1 Seguridad de las estaciones de trabajo. 4.2 Seguridad de servidores.

7. Actividades de aprendizaje de los temas

Unidad 1. Introducción a la Seguridad	
Competencias	Actividades de aprendizaje
Específica(s): Identifica los problemas de la seguridad informática y proponer los mecanismos para resolverlos. Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Comunicación oral y escrita. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones. • Conocimiento de una segunda lengua • Compromiso ético	• Analizar cómo se debe realizar el planteamiento del problema y las generalidades de la seguridad. • Analizar el impacto de la seguridad informática en la vida cotidiana y los negocios. • Analizar las técnicas y mecanismos de seguridad, así como la manera de plantear una solución
Unidad 2. Comunicaciones Seguras y la Seguridad en Internet.	
Competencias	Actividades de aprendizaje
Específica(s): Diseña e implementa estrategias para obtener seguridad en las comunicaciones y el Internet.	• Investigar las fases de que establece un SGSI. • Investigar los diferentes tipos de ataques, vulnerabilidades amenazas y riesgos en los sistemas de información.

Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Comunicación oral y escrita. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones. • Conocimiento de una segunda lengua • Compromiso ético	• Analizar las técnicas y mecanismos de seguridad, así como las fases de un ataque cibernético.
Unidad 3. Herramientas para la seguridad informática.	
Competencias	Actividades de aprendizaje
Específica(s): Manipula y configura adecuadamente las herramientas que se utilizan para generar seguridad en las comunicaciones. Genéricas: • Capacidad crítica y autocrítica. • Trabajo en equipo • Habilidades interpersonales • Capacidad de comunicarse con profesionales de otras áreas • Compromiso ético	• Investigar las diferentes herramientas de seguridad informática. • Analizar la configuración y resultados de la ejecución de las diferentes herramientas de seguridad informática. • Investigar las contramedidas que se pueden aplicar en las diferentes fases de un ataque cibernético. • Investigar planes de contingencia para mitigar los efectos de un ataque cibernético. • Investigar planes de pruebas para evaluar la seguridad informática.
Unidad 4. Configuración de un Sistema Operativo para la Seguridad	
Competencias	Actividades de aprendizaje
Específica(s): Aplica y opera las diferentes formas de realizar la configuración de un sistema operativo para la seguridad de la comunicación.	• Investigar las actualizaciones de seguridad y seguridad en las estaciones de trabajo. • Determinar ventajas y desventajas de la seguridad servidores.

Genéricas: • 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 las redes privadas virtuales y su utilización dentro de la seguridad. Analizar las características de los cortafuegos para la implementación de la seguridad
--	--

8. Práctica(s)

• Realizar un caso práctico de problemáticas y definición de la seguridad en comunicaciones. • Realizar la configuración para encriptar archivos. • Realizar una simulación de contraseñas simples y contraseñas de frase. • Realizar una configuración de correo electrónico, dentro un servidor • Realizar la configuración de un firewall. • Realizar la configuración de un servidor para seguridad, en Internet, de correos, Web, y de 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 de la asignatura
- Reporte de prácticas de laboratorio

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.