1. Datos Generales de la asignatura

Nombre de la asignatura:	**Tópicos selectos de la seguridad de redes.**
Clave de la asignatura:	***GRD-1805***
SATCA[1]:	***3-2-5***
Carrera:	Ingeniería en Sistema Computacionales ISIC-2010-224 e Ingeniería en Tecnologías de la Información y Comunicaciones. ITIC-2010-225.

2. Presentación

Caracterización de la asignatura

- La asignatura de tópicos selectos de la seguridad en redes aporta al Ingeniero en Sistemas Computacionales y al Ingeniero en Tecnologías de la Información y Comunicaciones los conocimientos, habilidades y la capacidad para analizar, diseñar e implementar los mecanismos y las herramientas necesarias para optimizar la seguridad en las redes de datos así como garantizar la disponibilidad de los servicios ofertados dentro de las redes de datos en producción.
- La seguridad es un tópico fundamental debido al crecimiento exponencial de las amenazas, intrusiones y sus posibles impactos en las organizaciones, de ahí la importancia del conocimiento de las herramientas especializadas para optimizar y garantizar la seguridad en las redes de datos y disponibilidad de los servicios.
- Para atender las nuevas circunstancias que implican estos cambios, se requieren profesionales preparados y capacitados, que estén en condiciones adecuadas para asumir estas responsabilidades.
- El contenido de esta asignatura permite desarrollar las competencias en los estudiantes para plantear soluciones a problemas que impacten en el ámbito de la seguridad de las redes de datos y optimizar la calidad y disponibilidad de los servicios ofertados.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

Intención didáctica

Esta asignatura sugiere el desarrollo práctico de cada una de sus unidades es decir, el profesor propone el planteamiento de un problema y el estudiante deberá resolverlos con las herramientas sugeridas por el profesor o propuestas por el estudiante para desarrollar cada una de las competencias.

- El tema uno introduce al estudiante en la fundamentación teórica de los potenciales ataques contra las redes basadas en protocolo TCP/IP. La asignatura se inicia con la estructura del protocolo TCP/IP para determinar el nivel de seguridad sobre las redes que operan con esta arquitectura. Se estudian los métodos de escucha, de fragmentación y de ataques; que son las formas principales de vulnerar las redes de datos.
- En el segundo tema se estudian los diferentes mecanismos de prevención y protección para las redes de datos, implementando sistemas perimetrales de protección hacia la red como son los firewalls en sus diferentes clasificaciones, estableciendo zonas militarizadas y otros esquemas que permitan mejorar u optimizar la seguridad, protección a nivel de red con IPsec y a nivel de transporte (SSL/TLS/WTLS), VPN.
- En el tercer tema se enfoca en los conceptos e importancia de los mecanismos actuales para la detección de ataques e intrusiones, proporcionando el sustento teórico - práctico que le permita identificar los distintos tipos de accesos no autorizados.
- En el cuarto tema se ve un estudio detallado de cada uno de los protocolos inseguros, la estructura, características y vulnerabilidades que presentan; así como el estudio de protocolos seguros que permitan mejorar la seguridad y calidad de los servicios ofertados.
- En el quinto tema se ve un estudio detallado de los diferentes comandos y herramientas para evaluar el tráfico en la red de datos, con la finalidad de conocer el estado y rendimiento de la red así como de los equipos que integran la misma, evaluando de esta manera el uso, tráfico, rendimiento y seguridad de la red.
- Se sugiere presentar diferentes tipos de problemas para desarrollar las capacidades lógicas de los estudiantes y analizar las soluciones. También es importante que se realicen actividades integradoras, desarrollando prácticas donde se requiera involucrar los diferentes conceptos en ejercicios.
- El docente debe:

Dominar ampliamente los contenidos de esta asignatura para que pueda abordar cada uno de los temas en su totalidad, además contar con la capacidad para coordinar, trabajar de forma individual y/o en equipo , orientar el trabajo del estudiante; potenciar en él la capacidad de análisis y síntesis, el trabajo cooperativo y la toma de decisiones. Mostrar flexibilidad en el seguimiento del proceso formativo y propiciar la interacción entre los estudiantes. Tomar en cuenta el conocimiento de los estudiantes como punto de partida y como obstáculo para la construcción de nuevos conocimientos.

• Utilizar el aprendizaje basado en problemas, trabajando en grupos pequeños, para sintetizar y construir el conocimiento necesario para resolver problemas relacionados con situaciones reales. • Proponer prácticas de redes que permitan al estudiante la integración de contenidos de la asignatura y entre distintas asignaturas, para su análisis y solución. • Propiciar en el estudiante, el desarrollo de actividades intelectuales de inducción, deducción y análisis-síntesis, encaminadas hacia la investigación, la aplicación de conocimientos y la solución de problemas. • Relacionar los contenidos de la asignatura con el cuidado del medio ambiente; así como con las prácticas de una ingeniería con enfoque sustentable.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Villahermosa, Tabasco. Junio 28, 2017.	Academia de: Ingeniería en sistemas computacionales e ingeniería en tecnologías de la información y comunicaciones del Instituto Tecnológico de Villahermosa.	Reunión para elaboración de asignaturas de la especialidad.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
• Conoce e implementa los mecanismos y herramientas necesarios para la detección de intrusiones en las redes de datos para mitigar los accesos no autorizados y maximizar la disponibilidad de los servicios. • Identifica e implementa los mecanismos y herramientas que optimicen la seguridad en las redes de datos para garantizar el buen funcionamiento de la misma.

5. Competencias previas

• Conoce y aplica los conocimientos obtenidos en fundamentos de redes para la segmentación de las redes basadas en TCP/IP, configuración básica de redes LAN y dispositivos de red.

• Conoce y aplica los conocimientos obtenidos en redes de computadoras para la conectividad en redes WAN con distintos protocolos de enrutamiento.

6. Temario

No	Temas	Subtemas
1	Ataques contra les redes TCP/IP	1. Seguridad en redes TCP/IP 2. Actividades previas a la realización de un ataque 3. Escuchas de red 4. Fragmentación IP 5. Ataques: DOS, SYN, DDoS; otros.
2	Mecanismos de prevención y protección	1.- conceptos básicos de los mecanismos de prevención y protección en las redes de datos.
		2.- Mecanismos de prevención: sistemas firewalls, construcción de firewalls, zonas desmilitarizadas, características adicionales de los sistemas cortafuegos. 3.- Mecanismos de protección: criptografía, sistemas de autenticación, protección a nivel de red (IPsec) y a nivel de transporte (SSL/TLS/WTLS), redes privadas virtuales (VPN).
3	Mecanismos para la detección de ataques e intrusiones	1. Necesidad de mecanismos en la prevención y protección 2. Sistemas de detección de intrusos 3. Escáner de vulnerabilidades 4. Prevención de intrusos 5. Detección de ataques distribuidos
4	Protocolos inseguros	1.- presentación 2 .- telnet 3.- ftp 4.-SNMP Ver. 1 5.- NetBios 6.- CDP 7.- SSH ver 1 8.- HTTP en vez de HTTPS

		9.- Ausencia de tunelización. 10.- Como detectar, analizar y recolectar Evidencias de estos protocolos inseguros.
5	Trabajo con Diferentes comandos Y herramientas	1.- presentación 2.- como evaluar SNMP 3.- Wireshark 4.-Sistema Syslog 5.- Nmap

7. Actividades de aprendizaje de los temas

1. Ataques contra les redes TCP/IP	
Competencias	Actividades de aprendizaje
Específica(s): • Identifica los diferentes tipos de ataques potenciales que se pueden llevar a efecto sobre las redes basadas en protocolos tcp/ip. Genéricas: • Capacidad de análisis y síntesis • Capacidad de diseñar modelos abstractos • Representa e interpreta conceptos en diferentes formas: Gráfica, escrita y • verbal • Habilidades básicas para elaborar diagramas	•Investigar en fuentes diversas de información los tipos y características de los diferentes tipos de ataques sobre redes tcp/ip. •Analizar y discutir en el aula la Investigación realizada en el punto anterior, donde se resalten los tipos de ataques más frecuentes y los daños o efectos sobre las redes tcp/ip. •Realizar un mapa conceptual sobre los tipos de ataques. •Uso de un portal de Internet para apoyo didáctico de la materia. •Desarrollar escenarios en clase para generar intercambio, discusiones y lluvias de ideas. •Identificar y hacer clasificaciones de los tipos de ataques y discutir en el aula los criterios seguidos para realizar tal clasificación.
2. Mecanismos de prevención y protección	
Competencias	Actividades de aprendizaje
Específica(s): • Conoce y configura los diferentes mecanismos y herramientas para la prevención, protección de la información así como la disponibilidad	• Uso de un portal de Internet para apoyo didáctico de la materia. • Ejercicios en clase para el planteamiento y solución de problemas seguridad implementando los mecanismos propuestos por el profesor.

de los servicios en las redes de datos. Genéricas: • Capacidad de análisis y síntesis • Capacidad de diseñar modelos abstractos • Representa e interpreta conceptos en diferentes formas: Gráfica, escrita y verbal • Habilidades básicas para elaborar diagramas	• Desarrollar escenarios en clase para generar Intercambio, discusiones y conclusiones. • Uso de sistemas operativos basados en Linux para la implementación de mecanismos de seguridad planteados por el profesor. • Uso de sistemas operativos propietarios para la implementación de mecanismos de seguridad planteados por el profesor. • Desarrollar escenarios en clase para generar intercambio, discusiones y lluvias de ideas.
3. Mecanismos para la detección de ataques e intrusiones	
Competencias	Actividades de aprendizaje
Específica(s): • Identifica los principales mecanismos para de detección y prevención de ataques e intrusiones en las redes de datos. Genéricas: • Capacidad de análisis y síntesis • Capacidad de diseñar modelos abstractos • Representa e interpreta conceptos en diferentes formas: Gráfica, escrita y verbal • Habilidades básicas para elaborar diagramas	• Realizar prácticas de búsqueda de información a través de diferentes navegadores o buscadores de información. • Investigación en diversa bibliografía y tutoriales. • Emplear software que permita la detección de intrusos y vulnerabilidades. • Emplear mecanismos para la detección de intrusos y ataques distribuidos. • Trabajo en equipo para la solución de casos prácticos.

4. Protocolos inseguros	
Competencias	Actividades de aprendizaje
Específica(s): • Identifica las principales características, vulnerabilidades y desventajas de los protocolos de red inseguros. Genéricas: • Capacidad de análisis y síntesis • Capacidad de diseñar modelos abstractos • Representa e interpreta conceptos en diferentes formas: Gráfica, escrita y verbal • Habilidades básicas para elaborar diagramas	• Uso de un portal de Internet para apoyo didáctico de la materia. • Ejercicios en clase para solución de problemas. • Desarrollar escenarios en clase para generar intercambio, discusiones y conclusiones. • Uso de hardware y software para realización de prácticas con los distintos protocolos • Trabajo en equipo para la solución de casos prácticos.
5. Trabajo con Diferentes comandos Y herramientas	
Competencias	Actividades de aprendizaje
Específica(s): • Conoce y aplica el manejo de herramientas y comandos que le permitan evaluar el tráfico en la red y el estado de los dispositivos para una mejor administración. Genéricas:	•Investigar en fuentes diversas de información las características principales de los analizadores de paquetes en redes tcp/ip. •Analizar y discutir en el aula la Investigación realizada en el punto anterior, donde se resalten las principales características de cada analizador. • Comparar las ventajas y desventajas para

• Capacidad de análisis y síntesis • Capacidad de diseñar modelos abstractos • Representa e interpreta conceptos en diferentes formas: Gráfica, escrita y verbal • Habilidades básicas para elaborar diagramas	cada caso. •Realizar un mapa conceptual sobre agentes y consolas del protocolo SNMP. •Uso de un portal de Internet para apoyo didáctico de la materia. •Ejercicios en clase que permitan la evaluación del wireshark u otro software analizador propuesto. •Desarrollar escenarios en clase para generar intercambio, discusiones y lluvias de ideas. •Seleccionar la red de una empresa y realizar los análisis y evaluaciones del tráfico de paquetes y estado de los equipos mediante las herramientas propuestas por el profesor o el alumno.

8. Práctica(s)

- Realizar prácticas de ataques sobre el protocolo tcp/ip como son: escuchas de red, fragmentación ip, DOS, SYN, DDoS; otros.
- Instalar y configurar cortafuegos (firewalls.)
- Configurar mecanismos de protección a nivel de red y de transporte: Ipsec, SSL/TLS/WTLS, VPN.
- Configurar una red instalando servicios basados en telnet, ftp, snmp v1, Netbios etc, con fines de vulneración y/o penetración.
- Instalar y configurar analizadores de tráfico y sistemas basados en agentes y consolas (SNMP).

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 especificas 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

- Para evaluar las actividades de aprendizaje se recomienda solicitar: mapas conceptuales o mentales, reporte de investigación, reportes de prácticas, tablas comparativas, estudio de casos, exposiciones en clase, portafolio de evidencias, entre otros.
- Para verificar el nivel del logro de las competencias del estudiante se recomienda utilizar: listas de cotejo, listas de verificación, matrices de valoración, guías de observación, rúbricas, entre otros.

11. Fuentes de información

- Tanenbaum Andrew S. Redes de computadoras. Ed. Prentice Hall.
- Comer, Douglas E. Redes Globales de Información TCP/IP, Principios básicos, protocolos y arquitectura. Ed. Prentice Hall.
- García Tomás Jesús; Santiago Ferrando y Piattini Mario. Redes para proceso distribuido. Ed. Computec.
- Ariganello Ernesto. Redes CISCO. Ed.Alfaomega Ra-Ma.
- Guijarro Coloma Luis. Redes ATM. Principios de interconexión y su aplicación. Ed. McGraw Hill.
- Fundamentos de seguridad en redes – Aplicaciones y estándares. Willian Stalling. Ed. Pearson
- Aspectos avanzados de seguridad en redes Joaquin Garcia Alfaro. Ed, UOC