1. Datos Generales de la asignatura

Nombre de la asignatura:	**Seguridad en Redes**
Clave de la asignatura:	**STD-1901**
SATCA[1]:	**2-3-5**
Carrera:	**Ingeniería en Sistemas Computacionales**

2. Presentación

Caracterización de la asignatura

Los conocimientos de los profesionales en seguridad y riesgos, están entre las más altamente solicitadas después de los conocimientos de redes, y la demanda global continua en crecimiento. Las organizaciones alrededor del mundo están experimentando la escases de profesionales en Tecnología de Comunicación e Información (ICT) con la especialización en conocimientos y habilidades necesarias para administrar dispositivos y aplicaciones para una infraestructura segura, sin vulnerabilidades de redes y con la mitigación de las amenazas de seguridad.

Esta asignatura aporta al perfil del Ingeniero en Sistemas Computacionales la capacidad para integrar eficientemente la infraestructura de redes existente en una organización, con el propósito de apoyar la toma de decisiones.

En ésta asignatura se provee una introducción a los conceptos básicos de seguridad y los conocimientos necesarios para la instalación, solución de problemas y monitoreo de dispositivos de redes para mantener la integridad, confidencialidad y disponibilidad de datos y dispositivos.

Aplica conocimientos de otras asignaturas, tales como: Fundamentos de telecomunicaciones, Redes de Computadoras, Conmutación y Enrutamiento de Redes y Administración de Redes.

Intención didáctica

Seguridad en Redes es una solución de aprendizaje práctica orientado al mundo profesional que hace hincapié en la experiencia práctica para ayudar a los alumnos a desarrollar conocimientos de seguridad especializados para promocionar profesionalmente. El programa de estudios ayuda a preparar a los alumnos para oportunidades laborales de seguridad de nivel básico.

La asignatura se puede impartir como un programa de estudios independiente o integrado en un campo más amplio de estudio, como los programas de tecnología o formación continua. El programa de estudios se puede ofrecer en un entorno totalmente presencial o combinado con actividades a distancia (BDL). Todos los

[1] Sistema de Asignación y Transferencia de Créditos Académicos

laboratorios prácticos del curso se pueden realizar en el equipo físico real.

También se debe propiciar mediante prácticas, la implementación de casos de estudio reales que ofrezcan escenarios distintos que permitan la aplicación de los conceptos para lograr que el aprendizaje sea significativo para el desarrollo de las competencias.

En el desarrollo de la materia, deberá observarse:

- Que los contenidos sean abordados en su totalidad.
- Que se cuente con la infraestructura necesaria para realizar las prácticas
- Que el laboratorio de prácticas cuente con el equipo necesario que deberá utilizarse durante el desarrollo de la asignatura.
- Que todas prácticas diseñadas por el docente sean afín a los temas del plan de estudios.
- Que los estudiantes adquieran las competencias específicas de cada tema.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	**Participantes**	**Observaciones**
Instituto Tecnológico de Toluca del 13 al 17 de Enero de 2014	Integrantes de la Línea de Investigación: Desarrollo y Seguridad sobre Sistemas Abiertos: Martha Escamilla Zepeda, Rosa Elvira Moreno González, Eugenio Falcon Izunza, Imelda Vertti Guzmán, María Luisa Gómez Santamarina, Ana Lilia Sosa Albarrán	

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
• Desarrolla un entendimiento teórico en profundidad de los principios de seguridad de la red, así como de las herramientas y configuraciones disponibles. • Hincapié en la aplicación práctica de los conocimientos necesarios para diseñar, implementar y respaldar la seguridad de la red. • Desarrolla un pensamiento crítico y habilidades de resolución de problemas complejos, a través de las prácticas desarrolladas en los laboratorios. • Fomenta la exploración de los conceptos de seguridad de la red y permita experimentar con el comportamiento de la red y formular preguntas del tipo "¿qué pasaría si?", las actividades de aprendizaje basadas en simulaciones de Packet Tracer.

5. Competencias previas

• Identificar los diferentes estándares de comunicación actuales para establecer interoperabilidad entre diferentes componentes. • Conocer las características de las diferentes topologías y clasificación de redes. • Aplicar normas y estándares oficiales vigentes que permitan un correcto diseño de red. • Diseñar, instalar y probar infraestructuras de red cumpliendo con las normas vigentes de cableado estructurado. • Identificar y aplicar conceptos fundamentales de las telecomunicaciones, para analizar redes computacionales. • Utilizar metodologías para el análisis de requerimientos, planeación, diseño e Instalación de una red. • Utilizar normas y estándares de la industria para diseñar e integrar soluciones de red dentro de las organizaciones. • Seleccionar, conocer y usar adecuadamente los diferentes sistemas operativos para lograr un uso más eficiente así como diferenciar y aplicar las técnicas de manejo de recursos para el diseño, organización, utilización y optimización de los sistemas operativos. También conocer y saber usar técnicas y/o herramientas de administración de los sistemas operativos para la optimización de recursos existentes.

6. Temario

Temas		Subtemas
No.	**Nombre**	
1.	Riesgos de seguridad en redes modernas	1.1 Principios fundamentales de la seguridad de la red 1.2 Virus, gusanos, caballos de troya 1.3 Metodologías de ataque
2.	Dispositivos de redes seguros	2.1 Protegiendo el acceso al dispositivo 2.2 Asignación de roles administrativos 2.3 Monitorizando y gestionando dispositivos 2.4 Automatizando la función de seguridad
3.	Autentificación, Autorización y Facturación	3.1 Finalidad de la AAA 3.2 Autentificación local AAA 3.3 Servidor basado en AAA 3.4 Servidor basado en AAA, autorización y contabilidad
4.	Implementación de tecnologías de Firewall	4.1 Listas de Control de Acceso 4.2 Seguridad de las redes con firewalls 4.3 Características CBAC 4.4 Características de políticas de firewall basadas en zone 4.5 Operación ZPF
5.	Implementación de dispositivos ASA (Adaptive Security Appliance)	5.1 Definición de los dispositivos ASA 5.2 Funcionamiento 5.3 Tipos de dispositivos 5.4 Configuración

7. Actividades de aprendizaje de los temas

Tema 1	Actividades de aprendizaje
Riesgos de seguridad en redes modernas	Explica los riesgos de redes, técnicas de mitigación y los conceptos básicos de seguridad en redes.
Competencia específica y genéricas (a desarrollar y fortalecer por tema)	
Competencias específicas: • *Describe la evolución de la seguridad de red* • *Describe las políticas de seguridad de red* • *Comprende como mitigar los ataques de red* *Competencias genéricas:* • Capacidad de abstracción, análisis y síntesis • Capacidad de aplicar los conocimientos en la práctica • Capacidad de comunicación oral y escrita • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas • Capacidad para identificar, plantear y resolver problemas • Capacidad para tomar decisiones • Capacidad de trabajo en equipo • Habilidad para trabajar en forma autónoma	

Tema 2	Actividades de aprendizaje
Dispositivos de redes seguros	Configura y administra el acceso seguro a dispositivos de capa 3: ruteadores
Competencia específica y genéricas (a desarrollar y fortalecer por tema)	
Competencias específicas: • *Configura la instalación física de la seguridad y el acceso administrativo en los routers cisco* • *Configura administrativa de reglas usando los niveles de privilegios* • *Implementar la administración y reporte de características de syslog, SNMP, SSH y NTP* • *Examinar la configuración del router utilizando el auditor de seguridad* *Competencias Genéricas:* • Capacidad de abstracción, análisis y síntesis • Capacidad de aplicar los conocimientos en la práctica • Capacidad de comunicación oral y escrita • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas • Capacidad para identificar, plantear y resolver problemas	

- Capacidad para tomar decisiones
- Capacidad de trabajo en equipo
- Habilidad para trabajar en forma autónoma

Tema 3	Actividades de aprendizaje
Autorización y Autentificación, Facturación	Configura y administra el acceso seguro a dispositivos de capa 3: ruteadores a través del protocolo AAA

Competencia específica y genéricas (a desarrollar y fortalecer por tema)

Competencia específica:

- *Configura de autentificación en ruteadores*
- *Configura de usuarios y determinar sus privilegios*
- *Configurarla facturación para monitoreo de los usuarios*

Competencias Genéricas:

- Capacidad de abstracción, análisis y síntesis
- Capacidad de aplicar los conocimientos en la práctica
- Capacidad de comunicación oral y escrita
- Habilidades para buscar, procesar y analizar información procedente de fuentes diversas
- Capacidad para identificar, plantear y resolver problemas
- Capacidad para tomar decisiones
- Capacidad de trabajo en equipo
- Habilidad para trabajar en forma autónoma

Tema 4	Actividades de aprendizaje
Implementación de tecnologías de Firewall	Implementa tecnologías de firewall para perímetros de redes seguras

Competencia específica y genéricas (a desarrollar y fortalecer por tema)

Competencia Específica

- *Comprende el funcionamiento de un firewall*
- *Identifica los tipos de firewall y en donde se instalan*
- *Configura elementos básicos del firewall*
- *Implementa y prueba funcionamiento de firewall*

Competencias Genéricas:

- Habilidad para buscar y analizar información proveniente de fuentes diversas.
- Toma de decisiones.
- Trabajo en equipo
- Capacidad de aplicar los conocimientos en la práctica

Tema 5	Actividades de aprendizaje

Implementación de dispositivos ASA (Adaptive Security Appliance)	Implementa tecnologías de firewall a través de dispositivos ASA para perímetros de redes seguras.
Competencia específica y genéricas (a desarrollar y fortalecer por tema)	
Competencias específicas: • *Comprende el funcionamiento de un dispositivo ASA* • *Identifica los tipos de dispositivos ASA y en donde se instalan* • *Configura elementos básicos del dispositivo ASA* • *Implementa y prueba funcionamiento de un dispositivo ASA* *Competencias Genéricas:* • Capacidad de abstracción, análisis y síntesis • Capacidad de aplicar los conocimientos en la práctica • Capacidad de comunicación oral y escrita • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas • Capacidad para identificar, plantear y resolver problemas • Capacidad para tomar decisiones • Capacidad de trabajo en equipo • Habilidad para trabajar en forma autónoma	

8. Práctica(s)

Tema 1
Configuración básica de seguridad(práctica en simulador) Configuración básica de seguridad (práctica en laboratorio)
Tema 2
Administrar los archivos de configuración IOS de Cisco y el sistema de archivos
Establecer y utilizar el SDM (Security Device Manager) de Cisco y el SDM Express para configurar la seguridad avanzada del router
Tema 3
Configuración del protocolo AAA en diferentes topologías de red Tema 4
Configuración de firewall en diferentes topologías de red Tema 5
Configuración de dispositivos ASA en diferentes topologías de red

9. Proyecto de asignatura

El proyecto integrador debe considerar las siguientes fases:

- Contextualización y/o diagnóstico
- Fundamentación
- Planeación
- Ejecución
- Evaluación
- Socialización

Debe integrar las competencias de las asignaturas que los estudiantes estén cursando en el periodo semestral y tomar como base las competencias de asignaturas señaladas como previas.

El proyecto integrador debe tener un criterio de evaluación.

10. Evaluación por competencias

La evaluación debe ser permanente y continua. Se debe hacer una evaluación diagnóstica, formativa y sumativa. Se debe aplicar la autoevaluación, coevaluación y heteroevaluación.

Se debe generar un portafolio de evidencias, de preferencia en formato digital.

Instrumentos:

Mapa conceptual
Tablas comparativas Examen teórico Examen Práctico
Reportes escritos de investigación
Reporte de prácticas de laboratorio y simulador Guía de proyecto

Herramientas:

Rubricas
Matriz de valoración
Matriz Avance de proyecto integrador

11. Fuentes de información

1. Graff, Jon C., Cryptography and E-Commerce, John Wiley & Sons, 2001
2. Goldreich, O, Modern Cryptography, Probabilistic Proofs and Pseudo-Randomness, Springer-Verlag, 2000
3. Horak,Ray, How Secure is your Connection? Nueva York:M&T books, 2000
4. Hutt,A.E.,S. Bosworth y D.B. Hoyt, eds, Computer Security Handbook, 3rd ed., Nueva York; John Wiley & Sons, 1995

5. Knudsen, Jonathan, Java Cryptography, O Reilly, 1998
6. Lai, Xuejia, On the design and Security of Block Ciphers, ETH Series in Information Processing, vol.1, 1992
7. Martin,Frederick Thomas, Top Secret Intranet: Hoe the U.S. Intelligent built intelink-The Worlds Largest, Most Secure Network, Prentice Hall,1997

* American Psychological Association (APA)

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico Superior de Coatzacoalcos Noviembre 2018	H. Academia de Sistemas	Reunión de especialidad

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Aplicar los paradigmas, técnicas y herramientas emergentes más utilizadas para establecimiento de la Seguridad dentro de la programación Web, para el desarrollo de aplicaciones Web seguras y confiables.

5. Competencias previas

Identificar la tecnología de la computación a través de las arquitecturas de diferentes modelos y desarrollar habilidades que le permitan sugerir soluciones óptimas utilizando los sistemas de cómputo.

Diseñar e implementar objetos de programación que permitan resolver situaciones reales y de ingeniería.

Diseñar e implementar aplicaciones Web que permitan resolver situaciones reales y de ingeniería.

6. Temario

No.	Temas	Subtemas
1	Introducción a la seguridad Web	1.1 Las fallas más comunes de seguridad en los sistemas de cómputo. 1.2 Políticas de Seguridad Informática.
2	Técnicas de análisis y tratamiento de riesgo.	2.1 Análisis de amenazas 2.2 Análisis de Activos 2.3 Análisis de Riesgos 2.4 Riesgo Residual y Salvaguardas

3	Puntos débiles en Seguridad Web.	3.1 Scripts 3.2 Http 3.3 Ingeniería Social 3.4 Ruteadores
4	Procedimientos para una programación segura.	4.1 J2EE Security Model 4.2 Autenticación en Servidores Web
5	Técnicas adicionales para protección.	5.1 Seguridad en instalaciones. 5.2 Seguridad en los usuarios. 5.3 Seguridad en los equipos.

7. Actividades de aprendizaje de los temas

1. Introducción a la seguridad Web	
Competencias	Actividades de aprendizaje
Específica(s) • Comprenda las necesidades, principios y definiciones inherentes a la seguridad en el desarrollo de aplicaciones Web. Genéricas: • Capacidad de comunicación oral y escrita. • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. • Capacidad de trabajo en equipo. • Habilidad para trabajar en forma autónoma.	• Investiga las actividades que incluye la seguridad en los sistemas de cómputo en general tanto de un aspecto físico, incluyendo instalaciones, no sólo equipos, así como lo referente a los distintos esquemas de software. • Elaborar un reporte que sea una evidencia de aprendizaje de la investigación realizada.
2. Técnicas de análisis y tratamiento de riesgo.	
Competencias	Actividades de aprendizaje
Específica(s): • Comprende las Técnicas de análisis de riesgos. • Desarrolla actividades para el tratamiento de errores.	• Conocer las distintas técnicas de análisis y tratamiento de errores. • Investigar los requerimientos para la utilización de algunas de las técnicas y tratamientos de errores. Entrega una

Genéricas: • Capacidad de abstracción, análisis y síntesis • Capacidad de aplicar los conocimientos en la práctica • Capacidad de comunicación oral y escrita • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas • Capacidad para identificar, plantear y resolver problemas • Capacidad para tomar decisiones • Capacidad de trabajo en equipo • Habilidad para trabajar en forma autónoma	evidencia de aprendizaje. • Realizar una práctica en la que aplique una de las técnicas de tratamientos de errores.
3. Puntos débiles en Seguridad Web.	
Competencias	Actividades de aprendizaje
Específica(s): • Conocer y Comprender las prácticas en el desarrollo de aplicaciones Web que originan huecos en la seguridad. Genéricas: • Capacidad de abstracción, análisis y síntesis • Capacidad de aplicar los conocimientos en la práctica • Capacidad de comunicación oral y escrita • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas • Capacidad para identificar, plantear y resolver problemas	• El docente expone cómo son por malas prácticas de programación los puntos débiles en la Seguridad Web. • El estudiante elabora prácticas correspondientes.

• Capacidad para tomar decisiones • Capacidad de trabajo en equipo • Habilidad para trabajar en forma autónoma	
4. Procedimientos para una programación segura.	
Competencias	Actividades de aprendizaje
Específica(s): • Conocer y comprender el Modelo de Seguridad de J2EE. • Conocer y comprender el establecimiento de procedimientos adecuados para la autentificación en servidores. Genéricas: • Capacidad de abstracción, análisis y síntesis • Capacidad de aplicar los conocimientos en la práctica • Capacidad de comunicación oral y escrita • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas • Capacidad para identificar, plantear y resolver problemas • Capacidad para tomar decisiones • Capacidad de trabajo en equipo • Habilidad para trabajar en forma autónoma	• El docente expone el Modelo de Seguridad de J2EE. • El estudiante elabora prácticas que sirvan de ejemplos de dicho modelo y entrega reportes de las mismas. • Investigar los procedimientos de autenticación para por lo menos dos diferentes tipos de servidores Web • El estudiante elabora una práctica de autenticación en un servidor en particular y entrega reporte.
5. Técnicas adicionales para protección.	
Competencias	Actividades de aprendizaje
Específica(s): • Conocer y comprender, las políticas	• El docente expone en clase los subtemas • El estudiante realiza un y entrega un

utilizadas en las instalaciones de equipos de cómputo para mejorar la seguridad. • Conocer algunas de las estrategias implementadas en los equipos de cómputo para mejorar la seguridad. • Conocer, comprender e implementar las prácticas que refuerzan la seguridad con los usuarios de sistemas Web. Genéricas: • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Toma de decisiones. • Trabajo en equipo • Capacidad de aplicar los conocimientos en la práctica	ensayo como evidencia de aprendizaje. • El estudiante realiza una investigación documental (de textos en inglés), más a fondo sobre alguno de los subtemas expuestos, para lo cual deberá escribir y entregar un artículo de 5 cuadrillas.

8. Práctica(s)

Tema 2 Aplicar una de las técnicas de tratamiento de errores. Tema 3 Demostrar los errores en los scripts que ocasionan fallas en la seguridad. Tema 4 Crear un esquema de autenticación con roles en un servidor Web. Crear una aplicación que implemente el modelo de seguridad de J2EE

9. Proyecto de asignatura

Dado que en el programa se realizan únicamente prácticas sueltas de cada tema no se requiere de un proyecto integrador.

10. Evaluación por competencias

La evaluación debe es continua. Se hacen evaluaciones formativas El portafolio de evidencias constará de: Reportes escritos de investigación Reporte de prácticas

11. Fuentes de información

1. Hacking Exposed Web Applications, Joel Scambray and Mike Shema,McGraw-Hill/Osborne © 2002
2. ImprovingWebApplicationSecurity:ThreatsandCountermeasures,Microsoft Corporation , Microsoft Press © 2003
3. Auditing Web Applications, Nilesh Chaudhari, McGraw-Hill/Osborne © 2002
4. Information Security Practice and Experience, Kefei Chen, Springer
5. Network Security Tools, Nitesh Dhanjani, Justin Clarke, O'Really
6. TheArtofSoftwareSecurityTesting:IdentifyingSoftwareSecurityFlaws,Chris Wysopal, Lucas Nelson, Elfriede Dustin, Dino Dai Zovi, Pearson Education.
7. Application Level Security Management, Michael Neuhaus, Diplomarbeiten Agentur.