



1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad de redes inalámbricas
Clave de la asignatura:	CBD-2428
SATCA¹:	2-3-5
Carrera:	Ingeniería en Ciberseguridad.

2. Presentación

Caracterización de la asignatura

Esta asignatura aporta el perfil del ingeniero en ciberseguridad las siguientes habilidades:

- Dirige el monitoreo, análisis y control de la información utilizando herramientas y marcos de referencia, con perspectiva ética, de respeto por la persona y de responsabilidad social.
- Evalúa riesgos de seguridad y vulnerabilidad en aplicaciones o instalaciones de tecnologías de la información con apoyo de herramientas de vanguardia automatizadas de acuerdo a metodologías, normas y estándares de excelencia.
- Gestiona incidentes y eventos de seguridad de informática para reducir la afectación negativa de la seguridad de la información y dar continuidad a las operaciones de la organización, atendiendo los principios de no discriminación, Inclusión y equidad social.
- Emplea métodos criptográficos para establecer protocolos de seguridad en el transporte de datos seguros a nivel de aplicación, usando herramientas de seguridad basadas en dichos protocolos integrando excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.
- Propone soluciones para proteger la transmisión y almacenamiento de información sensible dentro de un área funcional o técnica, a partir de marcos de referencia con excelencia, vanguardia e innovación social aplicando mejores prácticas del mercado.

A su vez aporta al perfil del ingeniero en ciberseguridad los conocimientos y habilidades necesarias para comprender, configurar y mantener redes inalámbricas seguras.

La materia proporciona una base sólida que prepara a los estudiantes para enfrentar los desafíos de la seguridad en entornos inalámbricos, equipándolos con las habilidades y el conocimiento necesario para proteger eficazmente las redes y los datos contra amenazas potenciales, adquiriendo conocimientos fundamentales sobre los principios de seguridad de redes, autenticación, autorización, cifrado e integridad de datos.

Al comprender sobre la seguridad de redes inalámbricas, los estudiantes pueden desarrollar habilidades para configurar estas redes de manera segura, incluyendo la selección de protocolos de seguridad adecuados, la configuración de contraseñas robustas y la implementación de políticas de seguridad. Así mismo tendrán la habilidad para implementar medidas de protección avanzadas, como el filtrado de direcciones MAC, la segmentación de redes, la limitación de la potencia de las antenas y la desactivación de funciones de riesgo como WPS.

¹ Sistema de Asignación y Transferencia de Créditos Académicos



Así, obtendrían experiencia en la realización de auditorías de seguridad en redes inalámbricas, evaluando el cumplimiento con acciones y regulaciones de seguridad, y recomendando correctivas cuando sea necesario.

Intención didáctica

El contenido general de la asignatura de seguridad de redes Inalámbricas abarca una amplia gama de conceptos teóricos y prácticos relacionados estrechamente con una variedad de temas dentro del ámbito de la seguridad informática y las redes de computadoras, y a menudo se considera como parte integral de un enfoque completo de seguridad cibernética. Esta materia está estructurada en cuatro temas, los cuales se describen a continuación:

En tema uno se abordan temas relacionados con la explicación de los fundamentos de la ciberseguridad, incluyendo la importancia de proteger la integridad, confidencialidad y disponibilidad de los datos, se analizan los riesgos asociados con la falta de seguridad en las redes Wi-Fi, incluyendo la exposición a ataques maliciosos y la pérdida de datos sensibles. Se define y ejemplifica como se manifiestan estos ataques que pueden dirigirse a redes Wi-Fi, como el spoofing de direcciones MAC, el ataque de desautenticación y el ataque de descifrado de tráfico.

En el tema dos de protocolos y medidas de seguridad en Wi-Fi, se explica el protocolo WEP, su propósito inicial y sus debilidades de seguridad, incluyendo la vulnerabilidad a ataques de fuerza bruta y la fácil interceptación de tráfico, se analiza una introducción a los protocolos de seguridad WPA, WPA2 y WPA3, destacando sus mejoras en comparación con WEP y su capacidad para proporcionar una autenticación y cifrado más robustos, además se destaca la importancia de implementar un servidor de detección de intrusos (IDS) para monitorear y detectar actividades maliciosas en la red Wi-Fi, y discutir cómo puede contribuir a mejorar la seguridad general.

Para el tema tres protección de redes Wi-Fi, se describe cómo implementar medidas de control de acceso, como el filtrado de direcciones MAC, listas blancas y listas negras, para autorizar dispositivos específicos y prevenir el acceso no autorizado a la red, se realiza la presentación de la configuración de redes Wi-Fi separadas para invitados como una medida de seguridad para limitar el acceso a recursos sensibles de la red principal, y discutir las mejores prácticas para configurar y proteger estas redes, se investiga sobre herramientas y técnicas para monitorear y detectar intrusiones en redes Wi-Fi, incluyendo el uso de sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusiones (IPS), así como la revisión regular de registros de eventos y la identificación de actividades anómalas.

En último tema se describe el proceso de instalación del servidor de detección de intrusos (IDS) en la red Wi-Fi, incluyendo la selección del software adecuado y la configuración inicial, se explica el proceso de instalación y configuración del servidor RADIUS en la red Wi-Fi para la autenticación centralizada de usuarios, así como también se guía a los estudiantes a través de los pasos necesarios para configurar el servidor RADIUS y establecer la comunicación con los puntos de acceso Wi-Fi.



3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Tecnológico Nacional de México del 4 al 6 de marzo del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Ciudad Juárez, La Paz, Jiquilpan, Mérida, Morelia, Tuxtla Gutiérrez, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas	Propuesta sintética de la carrera de Ingeniería en Ciberseguridad.
Tecnológico Nacional de México del 22 al 26 de abril del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Ciudad Juárez, La Paz, Jiquilpan, Mérida, Morelia, Tuxtla Gutiérrez, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas. Representante de Ciencias Básica de los Institutos de: Celaya, Morelia CENIDET y CIIDET.	Diseño y/o desarrollo curricular de la carrera de Ingeniería en Ciberseguridad
Tecnológico Nacional de México del 27 al 31 de mayo del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Jiquilpan, Mérida, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas	Consolidación curricular de la carrera de Ingeniería en Ciberseguridad.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
<ul style="list-style-type: none">Desarrolla la habilidad de comprender los protocolos de seguridad inalámbrica, así como la capacidad para configurar y administrar redes Wi-Fi seguras, conociendo las técnicas de detección y prevención de intrusiones.



5. Competencias previas

- Identifica y explica el proceso de comunicación entre dispositivos conectados a una red aplicando normas y estándares vigentes en las redes de datos.
- Diseña e implementa diferentes tipos de redes de datos analizando y aplicando normas y estándares vigentes en redes de datos.
- Analiza y evalúa diferentes tipos de redes de datos aplicando normas y estándares vigentes en redes de datos para inferir problemas de diseño, implementación y/o desempeño.
- Diseña, analiza y optimiza sistemas de comunicación basados en señales, que incluye la capacidad para comprender, modelar y manipular señales en diferentes dominios (temporal, frecuencial, espacial), así como seleccionar y aplicar técnicas de procesamiento y transmisión de señales para satisfacer requisitos específicos de rendimiento y calidad en sistemas de telecomunicaciones.

6. Temario

No.	Temas	Subtemas
1	Introducción a la ciberseguridad Wi-Fi.	<ul style="list-style-type: none">1.1 Conceptos básicos de ciberseguridad y redes inalámbricas.1.2 Amenazas y riesgos comunes en redes wifi.1.3 Importancia de la ciberseguridad en Wi-Fi.1.4 Ataques activos.1.5 Ataques pasivos.
2	Protocolos y medidas de seguridad en Wi-Fi.	<ul style="list-style-type: none">2.1. Protocolo WEP.2.2. Protocolo WPA/WPA2/WP3.2.3. Protocolo RADIUS.<ul style="list-style-type: none">2.3.1. Métodos de autenticación.2.4. Medidas de seguridad.<ul style="list-style-type: none">2.4.1. Seguridad mediante MAC ADDRESS.2.4.2. Reducción de rangos de direcciones IP.2.4.3. Limitar cobertura y potencia de las antenas.2.4.4. Deshabilitar WPS.2.4.5. Crear redes Wi-Fi para invitados.2.5. Utilizar servidor de detección de intrusos.
3	Protección de redes Wi-Fi.	<ul style="list-style-type: none">3.1. Configuración segura del router wifi: cifrado, contraseñas y actualizaciones.3.2. Control de acceso a la red wifi: MAC filtering, listas blancas y negras.3.3. Redes wifi para invitados: configuración y seguridad.3.4. Monitoreo y detección de intrusiones en redes wifi.



4	Implementación de seguridad en redes Wi-Fi.	<p>4.1. Implementación servidor de detección de intrusos.</p> <p>4.1.1. Instalación y configuración.</p> <p>4.1.2. Detección de intrusos.</p> <p>4.2. Implementación de servidor RADIUS.</p> <p>4.2.1. Instalación y configuración.</p> <p>4.2.2. Alta de usuarios y contraseñas.</p>
---	---	---

7. Actividades de aprendizaje de los temas

1. Introducción a la ciberseguridad Wi-Fi.	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i></p> <ul style="list-style-type: none">Identifica y comprende los fundamentos de la ciberseguridad aplicados a redes inalámbricas, incluyendo la identificación de amenazas comunes. <p><i>Genérica(s):</i></p> <p><i>Transversal(es):</i></p> <ul style="list-style-type: none">Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	<ul style="list-style-type: none">Investigar y clasificar los riesgos involucrados en la ciberseguridadRealizar un análisis de los tipos de ataques a una red Wi-FiElaborar un video animado de mínimo 3 minutos y máximo de 5 minutos en donde identifiquen un caso de ciberseguridad, involucrando los conceptos vistos
2. Protocolos y medidas de seguridad en Wi-Fi.	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i></p> <ul style="list-style-type: none">Analiza y aplica los protocolos de seguridad inalámbrica, incluyendo WPA2, WPA3 y otros estándares relevantes, para diseñar e implementar medidas efectivas de seguridad en redes Wi-Fi.	<ul style="list-style-type: none">Investigación sobre los diferentes tipos de ataques a redes wifi.Práctica de la protección contra ataques a redes wifi.Utilización de herramientas para detectar y prevenir ataques a redes wifi.



<p>Genérica(s):</p> <ul style="list-style-type: none">• Capacidad de abstracción, análisis y síntesis• Capacidad de aplicar los conocimientos en la práctica• Habilidades para buscar, procesar y analizar información procedente de fuentes diversas• Capacidad para identificar, plantear y resolver problemas• Capacidad para tomar decisiones• Trabaja en equipo• Habilidades interpersonales• Habilidad para trabajar en forma autónoma• Compromiso ético• Compromiso con la calidad <p>Transversal(es):</p> <ul style="list-style-type: none">• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.• Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	
3. Protección de redes wifi.	
Competencias	Actividades de aprendizaje
<p>Específica(s):</p> <ul style="list-style-type: none">• Diseña e implementar estrategias integrales de protección para redes Wi-Fi, incluyendo la identificación y mitigación de vulnerabilidades, la configuración de políticas de seguridad robustas.	<ul style="list-style-type: none">• Investigación sobre los diferentes tipos de ataques a redes wifi.• Práctica de la protección contra ataques a redes wifi.• Utilización de herramientas para detectar y prevenir ataques a redes wifi.



<p>Genérica(s):</p> <ul style="list-style-type: none">• Capacidad de abstracción, análisis y síntesis• Capacidad de aplicar los conocimientos en la práctica• Habilidades para buscar, procesar y analizar información procedente de fuentes diversas• Capacidad para identificar, plantear y resolver problemas• Capacidad para tomar decisiones• Trabaja en equipo• Habilidades interpersonales• Habilidad para trabajar en forma autónoma• Compromiso ético• Compromiso con la calidad <p>Transversal(es):</p> <ul style="list-style-type: none">• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.• Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano,	
4. Implementación de seguridad en redes Wi-Fi.	
Competencias	Actividades de aprendizaje
<p>Específica(s):</p> <ul style="list-style-type: none">• Aplica medidas de seguridad avanzadas en redes Wi-Fi, incluyendo la configuración de autenticación robusta, la aplicación de cifrado adecuado, la segmentación de redes inalámbricas, la configuración de políticas de control de acceso, y la integración de soluciones de detección y prevención de intrusiones.	<ul style="list-style-type: none">• Selección de una solución de seguridad para una red wifi real o virtual.• Instalación y configuración de la solución de seguridad seleccionada (Por ejemplo, Firewall, servidores GLADIADOR o IPS) y de un servidor RADIUS.• Monitorización de la red wifi y detección de amenazas.• Simulación de ataques a redes wifi y respuesta a incidentes de seguridad.



Genérica(s):

- Capacidad de abstracción, análisis y síntesis
- Capacidad de aplicar los conocimientos en la práctica
- Habilidades para buscar, procesar y analizar información procedente de fuentes diversas
- Capacidad para identificar, plantear y resolver problemas
- Capacidad para tomar decisiones
- Trabaja en equipo
- Habilidades interpersonales
- Habilidad para trabajar en forma autónoma
- Compromiso ético
- Compromiso con la calidad

Transversal(es):

- Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.
- Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.
- Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.



8. Práctica(s)

- Configuración básica de una red wifi.
- Identificación de redes wifi en el entorno.
- Habilitación de opciones de seguridad como WPA2 y MAC filtering en un AP/Router.
- Actualización del firmware del router.
- Detección de redes wifi vulnerables.
- Bloqueo de ataques de fuerza bruta.
- Configuración de los puntos de acceso wifi para utilizar el servidor RADIUS para la autenticación y autorización de usuarios.
- Implementación de medidas para mejorar la seguridad del servidor RADIUS.
- Instalación y configuración de un servidor Gladiator.
- Implementar diferentes medidas de seguridad en una red wifi utilizando un servidor Gladiator.
- Monitorizar y analizar la seguridad de la red wifi mediante el servidor Gladiator.
- Realización de una auditoría de seguridad de una red wifi.
- Análisis de los resultados de la auditoría de seguridad.
- Implementación de medidas adicionales para optimizar la seguridad de la red wifi.

9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance del(los) logro(s) formativo(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 los saberes, habilidades y destrezas 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”, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.



10. Evaluación de saberes, habilidades y destrezas

La evaluación debe ser continua y formativa por lo que se debe considerar el desempeño en cada una de las actividades de aprendizaje, haciendo especial énfasis en:

- Proyecto transversal
- Elaboración de trabajos de investigación
- Autoevaluaciones
- Resúmenes
- Reportes de prácticas de laboratorio
- Participaciones en actividades como:
- Exámenes escritos
- Solución de problemario
- Desempeño integral del alumno

La evaluación se dará en tres momentos al inicio, durante y al final del proceso educativo por lo cual será diagnóstica, acumulativa y elaboración de un portafolio de evidencias que contenga:

- Cuadros comparativos
- Informes y reportes
- Diseño y fundamentación del proyecto transversal
- Reporte de investigación documental
- Cuadros sinópticos
- Listados de preguntas reflexivas

Reporte de investigación bibliográfica y electrónica

11. Fuentes de Información

1. Wireless Security: Models, Threats, and Solutions, Autor: Randall K. Nichols, Panos C. Lekkas. Editorial: McGraw-Hill, 2002.
2. Hacking Exposed Wireless: Wireless Security Secrets & Colutions, Johnny Cache, Vincent Liu, Joshua Wright. Editorial: McGraw-Hill, 2007.
3. 802.11 Wireless Networks: The Definitive Guide, Matthew Gast. Editorial: O'Reilly Media, 2005.
4. Security for Wireless Sensor Networks. Autor: Jesús Hamilton Ortiz. Editorial: Springer, 2013.
5. Wi-Foo: The Secrets of Wireless Hacking. Autor: Andrew Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky. Editorial: Addison-Wesley Professional, 2004.
6. Seguridad en Redes Inalámbricas - Wi-Fi Security. David Espinel. Editorial: Alfaomega, 2010.
7. Seguridad de redes inalámbricas. Óscar Salazar, Elisa Martín. Editorial: Ra-Ma Editorial, 2013.
8. Seguridad en redes inalámbricas. Autor: José Manuel Riera González. Editorial: Delta Publicaciones, 2006.
9. Seguridad en redes inalámbricas: Guía de supervivencia. Nelson Murillo. Editorial: CreateSpace Independent Publishing Platform, 2017.
10. Seguridad de Redes Inalámbricas. Néstor Nocetti, Julián Salinas. Editorial: RedUSERS, 2006.
11. Asociación Nacional de Instituciones de Educación en Tecnologías de Información A.C. (2024). Modelo curricular por competencias. ANIEI.