



1. Datos Generales de la asignatura

Nombre de la asignatura:	Fundamentos de seguridad en IoT
Clave de la asignatura:	CBD-2419
SATCA¹:	2-3-5
Carrera:	Ingeniería en Ciberseguridad.

2. Presentación

Caracterización de la asignatura
<p>Esta asignatura aporta el perfil del ingeniero en ciberseguridad las siguientes habilidades:</p> <ul style="list-style-type: none">• Utiliza sistemas operativos, lenguajes de programación, redes y entornos tecnológicos para integrar soluciones de seguridad con responsabilidad e inclusión social en las organizaciones.• 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.• Diseña políticas de seguridad informática para establecer controles de seguridad pertinentes atendiendo los principios de no discriminación, Inclusión y equidad social.• 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.• Gestiona planes y proyectos de seguridad de la información de acuerdo con las necesidades del negocio, considerando riesgos y contingencias, promoviendo el cumplimiento de los principios de no discriminación, inclusión, equidad social, políticas, normas y acuerdos de nivel de servicio.• Aplica procedimientos y técnicas de auditoría informática para detectar si se protegen los activos y recursos de la organización, si se mantiene la integridad de los datos, si se utiliza eficientemente los recursos, si se atienden los principios de no discriminación, inclusión y equidad social y si se cumple con las leyes y regulaciones establecidas.

¹ Sistema de Asignación y Transferencia de Créditos Académicos



Tiene el objetivo de fortalecer las habilidades y capacidades del ingeniero en ciberseguridad explorando los fundamentos teóricos y prácticos necesarios para comprender los desafíos y las soluciones relacionadas con la protección de dispositivos interconectados en entornos IoT. Desde la comprensión de los protocolos de comunicación hasta el análisis de vulnerabilidades y la implementación de medidas de seguridad, los participantes adquirirán las habilidades necesarias para salvaguardar la integridad, confidencialidad y disponibilidad de los sistemas IoT en el contexto de la ciberseguridad.

Intención didáctica

Se organiza el temario en cuatro temas, donde abordan temas sobre los datos, IoT, Ataques conceptos y técnicas para evitarlos, como analizar los datos y evaluarlos y el procesamiento de imágenes en tiempo real, donde el estudiante podrá brindar a la empresa la seguridad requerida para evitar la pérdida de información.

En el curso de las actividades programadas es importante que el estudiante valore las actividades que realiza y entienda que está construyendo su futuro y actúe de manera profesional.

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">Desarrollar la capacidad para diseñar, implementar y mantener sistemas de internet de las cosas (IoT) seguros, aplicando técnicas avanzadas de ciberseguridad para proteger la integridad y la privacidad de la información en entornos interconectados.

5. Competencias previas

<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.Identifica, analiza y clasifica diferentes tipos de malware utilizando técnicas de análisis estático y dinámico, aplicando metodologías de detección y técnicas avanzadas de análisis para evaluar la integridad, confidencialidad y disponibilidad de los sistemas informáticos en entornos controlados y reales.Diseña sistemas y técnicas específicas para asegurar los sistemas informáticos de la empresa y diversos dispositivos.
--

6. Temario

No.	Temas	Subtemas
1	Introducción al IoT y el rol de la ciberseguridad.	1.1 Introducción a internet de las cosas (IoT). 1.2 Aplicación del IoT en la vida diaria. 1.3 Aplicación del IoT en la empresa y organizaciones. 1.4 Aplicaciones de la IoT en la industria. 1.5 Retos de ciberseguridad en entornos de dispositivos de IoT.
2	Captación de datos de diversas fuentes.	2.1. Dispositivos IoT desde fuente RFID. 2.1.1. Captar, almacenar y procesar. 2.1.2. Analizar datos. 2.2. Dispositivos IoT desde fuente Bluetooth. 2.2.1. Captar, almacenar y procesar. 2.2.2. Analizar datos.



		<p>2.3. Dispositivos IoT desde fuente Infrarroja.</p> <p>2.3.1. Captar, almacenar y procesar.</p> <p>2.3.2. Analizar datos.</p> <p>2.4. Dispositivos IoT desde fuente Wi-Fi.</p> <p>2.4.1. Captar, almacenar y procesar.</p> <p>2.4.2. Analizar datos.</p> <p>2.5. Protocolos para captar información.</p> <p>2.5.1. Protocolo MQTT en el campo en la industria</p> <p>2.5.2. LoRaWAN.</p>
3	Ataques, conceptos y técnicas.	<p>3.1. Vulnerabilidades en dispositivo IoT.</p> <p>3.2. Ataques y explotación en dispositivos del IoT.</p> <p>3.3. Evaluación e impacto de incidentes de seguridad en entornos de IoT.</p> <p>3.4. Gestión de riesgos en entornos IoT.</p>
4	Monitoreo y defensa.	<p>4.1. Autenticación y autorización de dispositivos IoT.</p> <p>4.2. Seguridad en la capa de red y transporte.</p> <p>4.3. Seguridad en la capa de aplicación (APIs, interfaces de usuario).</p> <p>4.4. Monitoreo de seguridad en dispositivos y redes IoT.</p> <p>4.5. Detección y respuesta ante incidentes en tiempo real.</p> <p>4.6. Estrategias de recuperación y continuidad del negocio en entornos IoT.</p>

7. Actividades de aprendizaje de los temas

1. Introducción al IoT y el rol de la ciberseguridad	
Competencias	Actividades de aprendizaje
<p>Específica(s): Identificar y comprender los principios fundamentales de la seguridad en el contexto del internet de las cosas (IoT), así como reconocer los desafíos y riesgos asociados con la interconexión de dispositivos.</p> <p>Genérica(s):</p> <ul style="list-style-type: none">Habilidad en el uso de tecnologías de información y comunicación.Capacidad para identificar, plantear y resolver problemas.Capacidad para trabajar en equipo interdisciplinario.	<ul style="list-style-type: none">Participar en debates sobre los beneficios y riesgos de la proliferación de dispositivos IoT en la sociedad moderna.Realizar una tabla comparativa acerca de los campos de aplicación del IoT en distintos sectores.Realizar un análisis de casos de estudio sobre brechas de seguridad en dispositivos IoT.



<ul style="list-style-type: none">• Capacidad crítica y autocrítica.• Habilidades interpersonales.• Capacidad de aplicar los conocimientos en la práctica• Liderazgo. <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.	
2. Captación de datos de diversas fuentes	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i> Comprender el funcionamiento de los protocolos de comunicación más apropiados para entornos IoT, así como las características de seguridad que operan en los dispositivos del IoT para proteger la confidencialidad e integridad de los datos transmitidos.</p> <p><i>Genérica(s):</i></p> <ul style="list-style-type: none">• Habilidad en el uso de tecnologías de información y comunicación.• Capacidad para identificar, plantear y resolver problemas.• Capacidad para trabajar en equipo interdisciplinario.• Capacidad crítica y autocrítica.• Habilidades interpersonales.• Capacidad de aplicar los conocimientos en la práctica• Liderazgo.	<ul style="list-style-type: none">• Generar prácticas de laboratorio realizando configuraciones de dispositivos IoT utilizando diferentes protocolos de comunicación.• Desarrollo de escenarios de prueba para evaluar la seguridad de la transmisión de datos en entornos IoT.



<i>Transversal(es):</i> <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.	
Tema 3. Ataques, conceptos y técnicas	
Competencias	Actividades de aprendizaje
<i>Específica(s):</i> Identificar y explotar evaluar los distintos tipos de vulnerabilidades en dispositivos IoT. <i>Genérica(s):</i> <ul style="list-style-type: none">• Habilidad en el uso de tecnologías de información y comunicación.• Capacidad para identificar, plantear y resolver problemas.• Capacidad para trabajar en equipo interdisciplinario.• Capacidad crítica y autocrítica.• Habilidades interpersonales.• Capacidad de aplicar los conocimientos en la práctica.• Liderazgo. <i>Transversal(es):</i> <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.	<ul style="list-style-type: none">• Realizar una clasificación de los distintos tipos de vulnerabilidades y amenazas que están presentes en escenarios de IoT.• Implementación de escenarios de prueba para realizar ataques comunes en escenarios de IoT.• Debatir acerca de la importancia de medidas de seguridad estrictas en entornos IoT.



<ul style="list-style-type: none">• 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.	
Tema 4. Monitoreo y defensa	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i> Capacidad para monitorear de forma proactiva la seguridad en entornos IoT, detectar y responder rápidamente a posibles incidentes de seguridad, y aplicar estrategias de recuperación y continuidad del negocio.</p> <p><i>Genéricas:</i></p> <ul style="list-style-type: none">• Habilidad en el uso de tecnologías de información y comunicación.• Capacidad para identificar, plantear y resolver problemas.• Capacidad para trabajar en equipo interdisciplinario.• Capacidad crítica y autocrítica.• Habilidades interpersonales.• Capacidad de aplicar los conocimientos en la práctica• Liderazgo <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">• Configuración de sistemas de autenticación de dispositivos IoT basados en certificados digitales.• Diseño e implementación de políticas de encriptación de datos para proteger la confidencialidad de la información en dispositivos IoT.• Simulación de ataques cibernéticos a dispositivos IoT para practicar la detección y respuesta de incidentes.• Elaboración de planes de continuidad del negocio centrados en la recuperación de sistemas IoT después de un incidente de seguridad.



8. Práctica(s)

- Generar el glosario de conceptos clave de cada tema.
- Desarrollar mapas conceptuales correspondientes a cada unidad temática.
- Desarrollar modelos prototipo mediante software de aplicación y optimización de recursos.
- Elaboración de las diferentes formas de conexión de dispositivos del IoT utilizando distintos tipos de arquitecturas, lenguajes de programación, escenarios de red y simuladores.

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

- Rúbrica.
- Listas de cotejo.
- listas de verificación.
- Manual de prácticas.



11. Fuentes de Información

1. Alvear-Puertas, V., Rosero-Montalvo, P., Peluffo-Ordóñez, D., & Pijal-Rojas, J. (2017). Internet de las Cosas y Visión Artificial, Funcionamiento y Aplicaciones: Revisión de Literatura. *Enfoque UTE*, 8(1), 244–256.
2. Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, 12(9), 157. DOI: <https://doi.org/10.3390/fi12090157>
3. Russell, B., & Duren, D. V. (2016). Practical Internet of Things Security. In Google Books. Packt Publishing Ltd.
4. Asociación Nacional de Instituciones de Educación en Tecnologías de Información A.C. (2024). Modelo curricular por competencias. ANIEI.