



### 1.- Datos Generales de la asignatura

<b>Nombre de la asignatura:</b>	Seguridad en redes IoT
<b>Clave de la asignatura:</b>	RIF-2203
<b>Créditos (Ht-Hp_ créditos):</b>	3-2-5
<b>Carrera:</b>	Ingeniería en Tecnologías de la Información y Comunicaciones

### 2.- Presentación

#### Caracterización de la asignatura

La asignatura de seguridad en redes IoT otorga al perfil del Ingeniero en Tecnologías de la Información y Comunicaciones obteniendo las habilidades fundamentales para garantizar la conectividad y transportación de los diferentes dispositivos asimismo implementará mecanismos autenticación y cifrado para protección de los datos.

El alumno analizará los procedimientos, políticas de seguridad y adecuación a la normativa al incorporar dispositivos IoT, considerando también su administración, su ciclo de vida y toda la información que generan e intercambian.

#### Intención didáctica

Esta materia tiene un enfoque práctico donde se espera que los estudiantes adquieran las habilidades necesarias para aumentar la productividad y acelerar la innovación del entorno, así como generar seguridad ante los cambios y la incertidumbre.

En el tema uno se definen los conceptos básicos que debe dominar el estudiante al elaborar un proyecto IOT.

En el tema dos el estudiante adquiere la capacidad de diseñar e implementar la interfaz asegurando la interacción con el usuario tanto en la parte interna como externa.

En el tema tres el estudiante conoce los componentes físicos a nivel hardware.

En el tema cuatro el estudiante se enfoca en los conceptos de sensores empleados en la industria, adquiriendo los conocimientos para modelar propuestas sobre el contexto y resaltando la importancia en su uso.

El tema cinco analiza procesos simples y hace uso de las herramientas de IOT, explotando su verdadero potencial en proyectos e incorporando como parte fundamental un motor SDK.





El docente deberá promover que el estudiante desarrolle las competencias de análisis, diseño e implementación para dar solución a problemas reales tanto en su entorno como en la industria.

### 3.- Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Apizaco, Tlax., del 21 de Marzo al 31 de Marzo del 2022 Instituto Tecnológico de Apizaco	MIA, Carlos Pérez Corona, Lic. Martin Rojas Ramírez, Ing. Saul Olaf Loaiza Meléndez, Lic. Eliut Flores Jiménez, M.C. Nicolás Alonzo Gutiérrez, Lic. Marcial Molina Sarmiento, Lic. Lauro Carlos Payan Reyes, Lic. Carlos Días Gutiérrez.	Taller de Creación de Módulos de Especialidad.

### 4.- Competencias a desarrollar

Competencias específicas de la asignatura
<ul style="list-style-type: none"> <li>• Aporta inteligencia de negocio y análisis competitivo.</li> <li>• Integrar las nuevas lógicas digitales en su trabajo profesional.</li> <li>• Capacidad para comunicarse, relacionarse y colaborar de forma eficiente con herramientas y en entornos digitales.</li> <li>• Gestiona de manera apropiada la identidad digital corporativa y propia.</li> <li>• Busca, obtiene, evalúa, organiza y comparte información en contextos digitales.</li> <li>• Se comunica, relaciona y colabora de forma eficiente con herramientas y en entornos digitales.</li> <li>• Trabaja, colabora y coopera en entornos digitales.</li> <li>• Gestiona su aprendizaje de manera autónoma, conoce y utiliza recursos digitales, mantiene y participa en comunidades de aprendizaje.</li> <li>• Se desenvuelve profesional y personalmente en la economía digital.</li> <li>• Entiende, comprende, sabe interactuar y satisface las necesidades de los nuevos clientes en contextos digitales.</li> <li>• Dirige y coordina equipos de trabajo distribuido en red y en entornos digitales.</li> <li>• Comprende el fenómeno digital y lo incorpora en la orientación estratégica de los proyectos de organización.</li> <li>• Mejora la eficiencia de los procesos.</li> </ul>

### 5.-Competencias previas

<ul style="list-style-type: none"> <li>• Utiliza técnicas de modelado para la solución de problemas.</li> <li>• Conocimientos de programación.</li> <li>• Conocimientos de lógica digital.</li> <li>• Conocimientos de redes.</li> </ul>
--





- Conocimientos sobre redes de ordenadores sistemas telemáticos.

## 6.-Temario

Temas		Subtemas
No.	Nombre	
1	Seguridad en IoT	1.1 Arquitectura de los dispositivos de IoT. 1.2 Amenazas y ataques de dispositivos de la IoT. 1.3 Modelos de seguridad actuales 1.3.1. Arquitectura de seguridad sistemática. 1.3.2 Arquitectura abierta.
2	Vectores de ataque en dispositivos IoT.	2.1 Fallos en la implantación 2.2 Interceptar datos en tránsito 2.3 Acceso a la plataforma de administración 2.4 Vulnerabilidad de software 2.5 Acceso físico al dispositivo 2.6 Los usuarios
3	Medidas de seguridad	3.1 Acceso seguro a dispositivos 3.2 Tipos de comunicaciones seguras 3.3 Actualizaciones de seguridad 3.4 Dispositivos de seguridad perimetral. 3.5 Concientización de usuarios 3.6 Seguridad física
4	Identificación control de servicios en la nube	4.1.- Amenazas y vulnerabilidad en los servicios públicos de la nube. 4.2 Estrategias multinube. 4.3 responsabilidades compartidas proveedor de servicios y clientes o usuarios.

\*

## 7.- Actividades de aprendizaje de los temas

1.- Seguridad en IoT	
Competencias	Actividades de aprendizaje
<p>Específica(s): Identifica los principales problemas de ataques informáticos y los mecanismos de protección de datos en plataformas de IoT.</p> <p>Genéricas:</p>	<ul style="list-style-type: none"> <li>• Conocerá la problemática del manejo seguro de datos de IoT.</li> <li>• Investigará cuales son las arquitecturas disponibles en</li> </ul>





<p>Capacidad de investigación Capacidad de abstracción, análisis y síntesis Capacidad de comunicación oral y escrita</p>	<p>dispositivos IoT y el tratamiento de información</p> <ul style="list-style-type: none"> <li>Investigar, analizar y exponer los casos de uso indebido de datos.</li> <li>Conocerá las buenas prácticas en la implantación de dispositivos de IoT.</li> </ul>
<p>2.- Vectores de ataque en dispositivos IoT.</p>	
<p>Competencias</p>	<p>Actividades de aprendizaje</p>
<p>Específica(s): Aplica metodologías y fallos de tratamiento de la información.</p> <p>Genéricas: Capacidad de identificar, plantear y resolver problemas. Capacidad de aplicar los conocimientos en la práctica. Capacidad de generar nuevas ideas de solución.</p>	<ul style="list-style-type: none"> <li>Conocerá el tránsito de la información y establecerá mecanismos de seguridad.</li> <li>Conocerá los principales mecanismos de comunicación a dispositivos y sensores para detectar procesos vulnerables de pérdida de datos.</li> </ul>
<p>3.- Medidas de seguridad</p>	
<p>Competencias</p>	<p>Actividades de aprendizaje</p>
<p>Específica(s): implementa las medidas de seguridad para proyectos IoT.</p> <p>Genéricas: Capacidad de análisis y síntesis. Capacidad de diseñar modelos abstractos. Habilidades básicas para elaborar diagramas. Representa e interpreta los conceptos de analógica digital en sus diversas formas, gráfica, escrita y verbal.</p>	<ul style="list-style-type: none"> <li>Analizar, diseñar e implementar medidas de seguridad para plataformas IoT.</li> <li>Implementar y desarrollar la seguridad que formará parte de su diseño.</li> <li>Diseñar y establecer los logs y debug.</li> <li>Diseñar e implementar el panel de control.</li> <li>Analizar y establecer el módulo de comunicación para control de dispositivos.</li> </ul>
<p>4.- Identificación control de servicios en la nube</p>	
<p>Competencias</p>	<p>Actividades de aprendizaje</p>
<p>Específica(s): Conoce, explora y toma precauciones de los diferentes servicios en la nube.</p> <p>Genéricas: Capacidad para proponer y aplicar los diversos tipos de sensores para resolver diversos problemas. Conocimientos sobre el área de estudio y la profesión. Habilidad para trabajar en forma autónoma.</p>	<ul style="list-style-type: none"> <li>Entregar reportes o informes sobre las diferentes plataformas de servicios de la nube.</li> <li>Conoce las responsabilidades de los servicios de la nube tanto de clientes como de proveedores.</li> </ul>





Habilidades en el uso de los tipos de sensores industriales.

### 8.- Evaluación por competencias (específicas y genéricas)

Para evaluar las actividades de aprendizaje se recomienda solicitar: Investigaciones, exposiciones, diseños, ontologías y desarrollo de aplicaciones.  
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.

### 9. Prácticas y ejercicios

Prácticas del tema 2

- Instalará dispositivos de sensores y analizará su proceso de testeo y tratamiento de información.
- Instalará una arquitectura abierta y probará su seguridad de transportación de datos

Prácticas del tema 3

- Diseña y expone la seguridad implementada en su proyecto y propondrá medidas para acceso.
- Establece mecanismos de seguridad para el buen funcionamiento de los sensores.

Prácticas del tema 4

- Analiza y determina el tipo de servicios comerciales en la nube y de distribución libre para implementar en su proyecto.

### 10. Proyecto integrador

A propuesta del docente, debe contemplar la:

- **Fundamentación:** que incluye el 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:** de acuerdo al diagnóstico, implica planificar un proceso: de intervención empresarial, social o comunitario, entre otros, según el tipo de proyecto, las actividades a realizar, que incluye las vistas en el curso, los recursos requeridos y el cronograma de trabajo.
- **Ejecución:** consiste en el desarrollo de la planeación del proyecto IOT realizado por parte de los estudiantes con asesoría del docente, cubriendo las necesidades de la academia, empresa o institución involucrada.





## 11.-Fuentes de información

Antonio Liñán Colina, Alvaro Vives y otros, *Internet de las cosas*, Attribution-NonCommercial-NoDerivatives 4.0 International License. 2015.

Fernández Martínez, Roberto y otros. *Redes inalámbricas de sensores. Teoría y aplicación práctica*. ISBN: 978-84-692-3007-7. Ed. Universidad de la Rioja. 2009. España.

García Jesús, M. Molina José. *Ciencia de datos*. 1ra. Capitulo 8. Edición. Ed. Alfaomega. 2018. España.

Marco Schwartz, *Internet of Things with Arduino Cookbook*. ISBN 978-1-78528-658-2. Ed., 2016. UK.

Marco Schwartz, *Internet of Things with Arduino Yún. Projects to help you build a world of smarter things*. ISBN 978-1-78328-800-7. Ed. Packt, 2014. UK.

Moisés Barrio, Andrés, 2018. *Internet de las cosas*. 1ra edición. Ed. Reus. 2018. España

Zanoni Leandro, *Futuro Inteligente*. 1ra. Edición. Ed. Bibliográfica. 2014. Argentina.

Roberto Fernández Martínez, Joaquín Bienvenido Ordieres Meré, Francisco Javier Martínez de Pisón Ascacíbar, Ana González Marcos, Fernando Alba Elías, Rubén Lostado Lorza, Alpha

Verónica Pernía Espinoza *Redes inalámbricas de sensores teoría y aplicación práctica* Universidad de La Rioja, 2009

Sixto Enrique Campaña Bastidas, Harold Emilio Cabrera Meza, Alvaro Jose Cervelion Bastidas, Adriana Aguirre Cabrera, *Redes de sensores Inalámbricas (WSN) caso de aplicación*, edit DAVINCI-unad

Jimena Garbarino, *Protocolos Para Redes Inalámbricas de Sensores*, Eae Editorial Academia Española, 2012)

