

CIBERTIC 2025

Por CUDI

Congreso Internacional de Ciberseguridad,
Tecnologías, Innovación y Ciencia

19 - 22 MAYO

GUADALAJARA, MÉXICO

Hotel Barceló

Smart Cities

Dr. José Antonio Orizaga Trejo

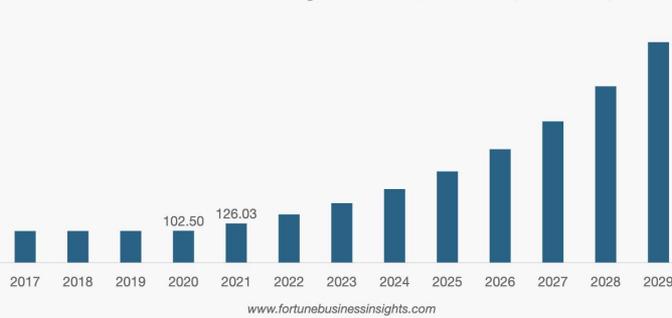
Agenda

- **Ciudades Inteligentes e Internet de las cosas (IoT)**
- **Cadena de valor IoT en Ciudades Inteligentes**
- **Aplicaciones en Ciudades Inteligentes**
- **Arquitectura IoT y la IA en Ciudades Inteligentes**
- **Actores IoT**
- **Conectividad y redes de nueva generación IoT**
- **Ciencia de datos para IoT**
- **Ciberseguridad en IoT**

Ciudades Inteligentes e Internet de las cosas (IoT)

- Dispositivos interconectados en arquitectura de red con características:
 - Integración de datos mediante sensores
 - Pre-Procesamiento de datos (Edge Computing)
 - Procesarlos y tomar decisiones en tiempo real

North America Internet of Things Market Size, 2018-2029 (USD Billion)



Cadena de valor IoT en Ciudades Inteligentes

- Se estima que en 2025 existan 500 dispositivos conectados en cada hogar.

Cómputo Personal Hogar



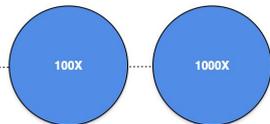
1990

Internet Móvil Personal

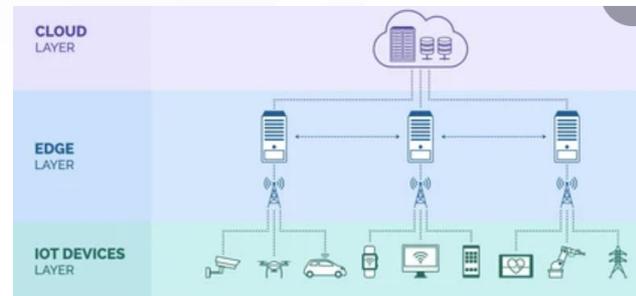


2010

IoT



2025



COSAS



CONECTIVIDAD



DATOS

10101
01010
00100

ANALITICA



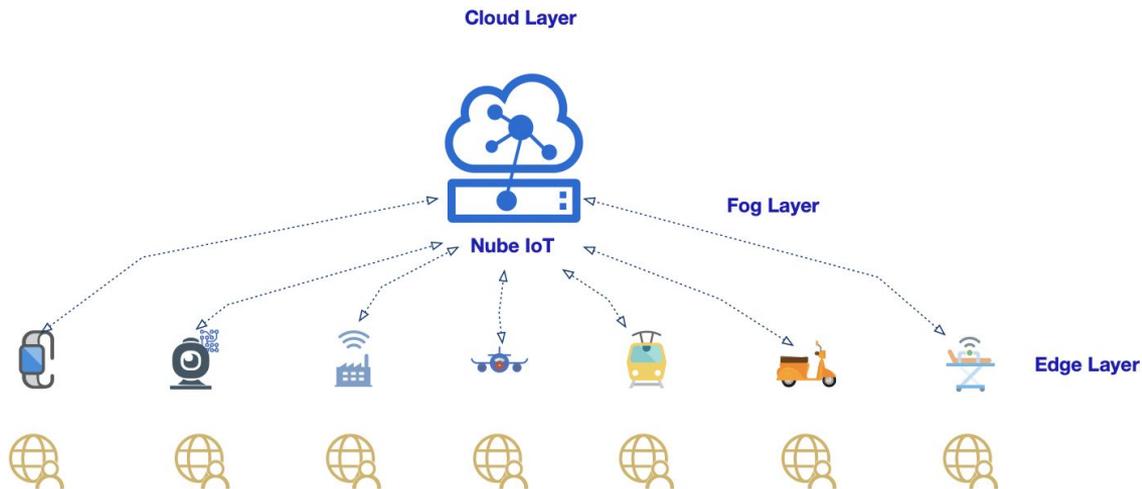
Cadena de valor IoT en Ciudades Inteligentes

- Las cosas influenciadas por:

- Rendimiento
- % Averías
- Calidad/precio
- Reputación online
- Preferencias de usuario

- Usuarios finales:

- Marketing
- Marcas
- Popularidad
- Precio



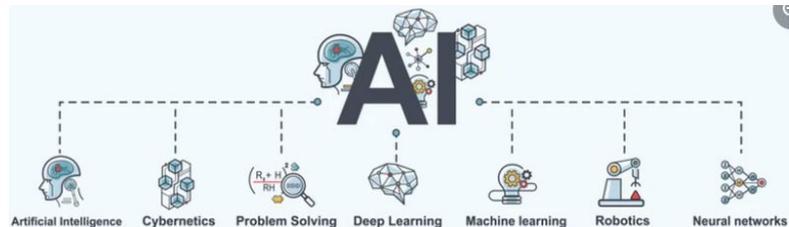
Cuando las “cosas” lideren el ciclo de pedido, los modelos basados en información definirán la venta, reputación online, precio y por tanto decidirán lo que el cliente final compra

Aplicaciones de IoT y la IA en Ciudades Inteligentes

- Optimización de tráfico
 - Eficiencia energética
 - Control de servicios
-
- Mantenimientos predictivos
 - Seguridad en el hogar
 - Hogar eficiente
 - Seguros en base a comportamiento



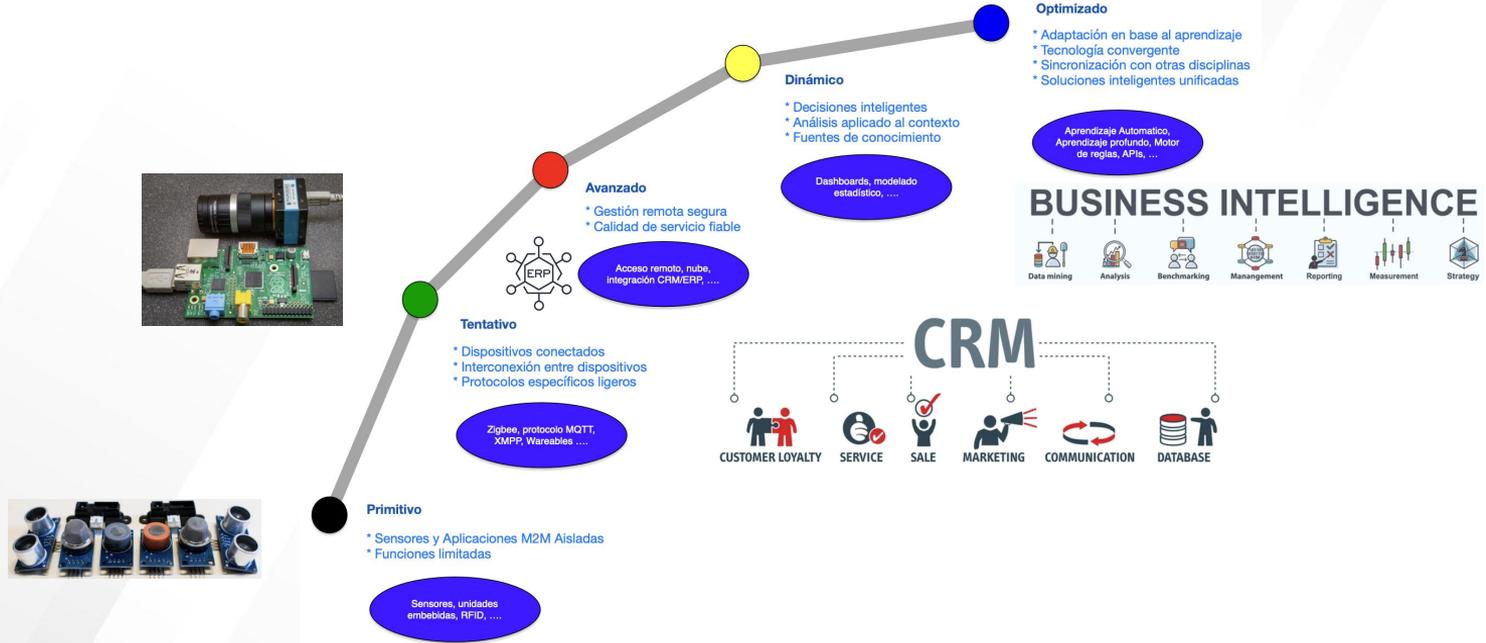
- Optimización de fabricación
 - Transporte
 - Logística (RFI)
 - Mantenimiento predictivo
-
- Monitoreo de pacientes en tiempo real
 - Análisis masivo de enfermedades
 - Gestión de inventarios médicos



Aplicaciones de IoT y la IA en Ciudades Inteligentes



- Niveles de madurez IoT



Aplicaciones de IoT y la IA en Ciudades Inteligentes



Actores IoT

Líderes Tecnológicos



Fabricante de Chips



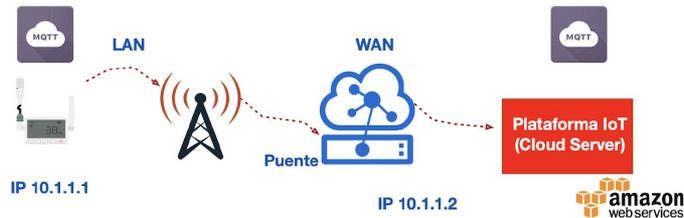
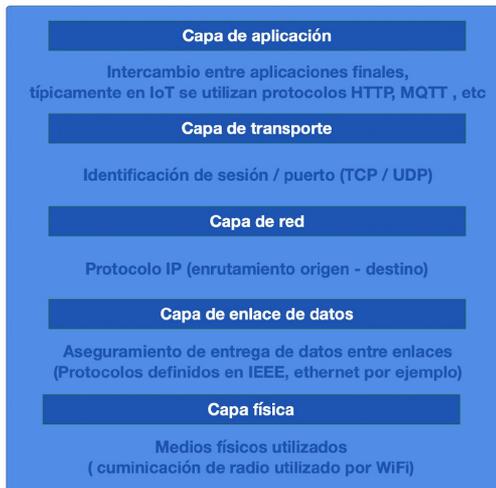
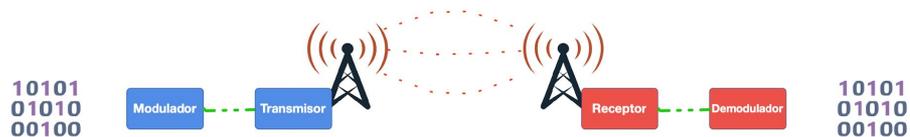
Operadores de Telecomunicaciones



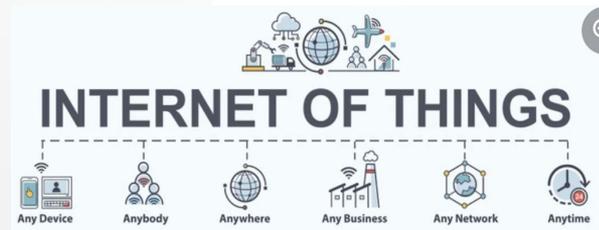
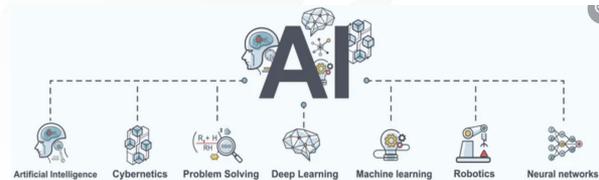
Startups



Conectividad y redes de nueva generación IoT



Ciencia de datos para IoT



Ciberseguridad IoT

Estándares Líderes en Ciberseguridad para IoT

- 1. NIST IR 8259r1 – Actividades Fundamentales de Ciberseguridad para Fabricantes de Productos IoT:** El Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. publicó en mayo de 2025 la versión revisada del informe NIST IR 8259r1. Este documento proporciona directrices actualizadas para fabricantes de dispositivos IoT, enfocándose en:
 - Identificación y autenticación de dispositivos.
 - Protección de datos y comunicaciones.
 - Gestión de vulnerabilidades y actualizaciones de seguridad.
 - Requisitos de seguridad durante todo el ciclo de vida del producto.Estas directrices son fundamentales para mejorar la seguridad de los dispositivos IoT en diversos sectores.
- 2. EN 17927 – Estándar Europeo SESIP para Evaluación de Seguridad en Plataformas IoT:** El estándar EN 17927, también conocido como SESIP (Security Evaluation Standard for IoT Platforms), fue adoptado por el Comité Europeo de Normalización (CEN) en 2023 y sigue vigente en 2025. SESIP proporciona un marco de evaluación de seguridad escalable para plataformas IoT, basado en cinco niveles de garantía. Este estándar facilita la conformidad con regulaciones como el Acta de Resiliencia Cibernética (CRA) de la UE y la Directiva de Equipos de Radio (RED).
- 3. NIST CSWP 42 – Automatización de la Seguridad en el Onboarding de Dispositivos IoT, ISO/IEC 27000 – Serie de Normas para la Gestión de Seguridad de la Información, ETSI EN 303 645 – Requisitos de Seguridad para Dispositivos IoT de Consumo.**
- 4. Código de Mejores Prácticas para la Ciberseguridad de Dispositivos IoT en México:** En México, el Instituto Federal de Telecomunicaciones (IFT) ha desarrollado un Código de Mejores Prácticas para la Ciberseguridad de Dispositivos IoT. Este documento proporciona recomendaciones para fabricantes y desarrolladores, incluyendo:
 - Uso de estándares abiertos y revisados por pares.
 - Aplicación del principio de privilegio mínimo en el software.
 - Cifrado de parámetros críticos de seguridad durante la transmisión

Ciberseguridad IoT

Técnicas Modernas de Ciberseguridad para IoT

1. **Autenticación y Autorización Sólida:** La implementación de tecnologías como OAuth 2.0 y el uso de certificados digitales permiten garantizar que solo los dispositivos autorizados puedan acceder a la red.
2. **Encriptación de extremo a extremo:** Asegura que los datos transmitidos entre dispositivos IoT y sistemas de control estén protegidos contra interceptaciones, utilizando cifrados como AES (Advanced Encryption Standard).
3. **Inteligencia Artificial (IA) para la Detección de Anomalías:** El uso de IA y Machine Learning permite identificar patrones inusuales en el tráfico de red que podrían indicar un ataque cibernético, proporcionando una detección temprana de amenazas.
4. **Blockchain para la Integridad de los Datos:** Las tecnologías de contabilidad distribuida (DLT) como blockchain se están utilizando para asegurar la integridad de los datos en las transacciones de IoT, creando un registro inmutable de eventos.

Ciberseguridad IoT

Tendencias Relevantes en la Ciberseguridad de IoT

1. **Zero Trust Architecture (ZTA):** Esta estrategia asume que ninguna entidad dentro o fuera de la red es de confianza, lo que requiere una verificación continua para cada acceso y movimiento de datos.
2. **Computación Perimetral (Edge Computing):** Reduce la latencia y mejora la seguridad al procesar datos localmente en el dispositivo IoT antes de enviarlos a la nube, limitando así la exposición a posibles vulnerabilidades.
3. **5G y su Impacto en IoT:** La adopción de 5G aumenta la capacidad de conexión de dispositivos IoT en las Smart Cities, lo que requiere nuevas medidas de ciberseguridad para proteger la gran cantidad de datos generados.
4. **Ciberseguridad como un Servicio (CaaS):** Proveedores de seguridad ofrecen soluciones escalables para proteger dispositivos IoT en ciudades inteligentes, lo cual es especialmente útil para municipios con recursos limitados.

Referencias

- [Internet of Things \(IoT\) Market Size, 2. \(2022\)](https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307). Internet of Things [IoT] Market Size, Share & Trends, 2029. Retrieved 18 July 2022, from <https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307>
- [IoT Connected Machines Market Size, 2. \(2022\)](https://www.fortunebusinessinsights.com/industry-reports/iot-connected-machines-market-101781). IoT Connected Machines Market Size, Share, & Forecast 2029. Retrieved 18 July 2022, from <https://www.fortunebusinessinsights.com/industry-reports/iot-connected-machines-market-101781>
- ETSI. (2020). Cyber Security for Consumer Internet of Things: Baseline Requirements (EN 303 645 V2.1.1). European Telecommunications Standards Institute. ISBN: 978-1-61417-891-3.
- [National Institute of Standards and Technology \(NIST\)](#). (2021). Security and Privacy Controls for Information Systems and Organizations (SP 800-53, Rev. 5). U.S. Department of Commerce. ISBN: 978-1-935627-27-3.
- [International Organization for Standardization \(ISO\)](#). (2021). Information Security Management (ISO/IEC 27001:2021). ISBN: 978-1-5044-6117-5.
- Li, Y., & Xie, X. (2022). A Comprehensive Review of IoT Security Standards and Their Applications in Smart Cities. *IEEE Internet of Things Journal*, 9(4), 2318-2330. ISSN: 2327-4662.
- Ziegler, M., & Wang, J. (2023). Advanced Encryption Techniques for IoT Devices in Smart Cities. *Springer Journal of Computer Security*, 31(2), 108-122. ISSN: 0926-227X.

Gracias:

Dr. José Antonio Orizaga Trejo



Centro de Innovación
en Ciudades Inteligentes

CIBERTIC²⁰₂₅

Por CUDI

Congreso Internacional de Ciberseguridad,
Tecnologías, Innovación y Ciencia

19 - 22 MAYO

GUADALAJARA, MÉXICO

Hotel Barceló

www.cibertic.mx

Dr. José Antonio Orizaga Trejo

jose.orizaga@academicos.udg.mx