

Internet Industrial de las Cosas (IIoT): Análisis Técnico, Económico y de Modelo de Negocio para la Modernización de una Planta

Diego Ignacio Poveda Crisosto
d.poveda01@ufromail.cl

2026-09-22

Resumen

Este informe analiza el Internet Industrial de las Cosas (IIoT) como tendencia reciente de automatización aplicada al mantenimiento predictivo de maquinaria rotativa. Su objetivo es caracterizar técnicamente la tecnología, estimar el costo de una solución representativa y evaluar sus ventajas, riesgos y modelo de negocio asociado, con el propósito de fundamentar una recomendación de adopción para una sección de planta industrial. Para ello se revisó bibliografía técnica y comercial especializada, se construyó una estimación de costos ascendente a partir de precios de mercado documentados y se contrastaron los hallazgos con estadísticas de ciberseguridad industrial. Los resultados muestran que el IIoT se distingue del IoT general por sus protocolos industriales, exigencias de fiabilidad y necesidad de interoperabilidad con sistemas de control existentes, y que modernizar una sección de cincuenta activos rotativos mediante sensores inalámbricos de vibración y temperatura implica una inversión inicial cercana a los 38.500 dólares más un costo anual de operación en torno a los 10.000 dólares. La discusión interpreta estos hallazgos considerando el riesgo de ciberseguridad como la principal limitación de la adopción y valora críticamente el uso real de IA en la elaboración de este informe. Se concluye que el aporte principal del informe es mostrar que un modelo de negocio de suscripción reduce la barrera de adopción del IIoT para pequeñas y medianas empresas industriales frente a la compra directa de hardware. Las fuentes utilizadas incluyen documentos técnicos y comerciales sobre precios, ciberseguridad y modelos de negocio de IIoT, además de los dos artículos de Alarcón (2026a, 2026b) que sustentan la metodología del curso. Finalmente, se declara el modelo de IA generativa utilizado, la distribución de roles entre el autor y dicho modelo, y las autorizaciones de publicación del informe.

1. Introducción

La automatización industrial ha evolucionado desde sistemas de control aislados, basados en lazos cerrados locales entre sensores, controladores y actuadores, hacia arquitecturas que integran esos mismos elementos con redes de comunicación, plataformas en la nube y análisis de datos a gran escala. El Internet Industrial de las Cosas (IIoT) es la expresión más difundida de esta transformación: permite que máquinas, sensores y sistemas de control conversen entre sí y con sistemas de gestión empresarial, habilitando funciones que antes requerían inspección manual, como el monitoreo continuo de condición de equipos rotativos.

El presente informe busca ampliar, desde una postura personal y fundamentada, los contenidos entregados en la clase teórica correspondiente a la Semana 02 del curso de Automatización, tomando el IIoT como caso de estudio sugerido en la pauta de la actividad. Para ello se abordan

cuatro preguntas: (i) en qué consiste el IIoT y cómo se distingue del IoT general, (ii) el costo estimado de una solución representativa para modernizar una sección de planta, (iii) las ventajas y al menos un riesgo relevante de dicha modernización, y (iv) un modelo de negocio para una startup que fabrique o integre este tipo de soluciones.

2. Objetivo

Analizar el Internet Industrial de las Cosas (IIoT) como tendencia reciente de automatización aplicada al mantenimiento predictivo de maquinaria rotativa, mediante la caracterización técnica de la tecnología, la construcción de una estimación de costos ascendente a partir de precios de mercado documentados y la evaluación de sus ventajas, riesgos y modelo de negocio asociado, con el propósito de fundamentar una recomendación de adopción para la modernización de una sección de planta industrial. El informe se limita al caso de sensores inalámbricos de vibración y temperatura para una sección hipotética de cincuenta activos rotativos, con estimaciones de costo en dólares estadounidenses a la fecha de elaboración de este documento, sin considerar una implementación técnica real, datos de una planta específica ni un análisis financiero de retorno de inversión detallado.

3. Metodología

Para elaborar este informe se siguieron cinco pasos secuenciales: (1) selección del IIoT como tendencia de automatización a analizar, siguiendo la sugerencia de la pauta de la actividad, (2) búsqueda y recopilación de fuentes técnicas y comerciales sobre definiciones, precios de hardware IIoT, modelos de negocio y estadísticas de ciberseguridad industrial, (3) construcción de una estimación de costos ascendente (por componente, cantidad y subtotal) y su contraste con un rango de costos ya documentado en la literatura comercial revisada, (4) redacción del borrador del informe a partir de esa información, y (5) revisión y validación final del contenido, incluyendo la verificación de que cada cifra citada proviniera de una fuente identificable. Para transparentar qué parte de este proceso corresponde a mi aporte y cuál al apoyo de un sistema de IA generativa, se utilizó como método de declaración el marco Ciencia Generativa (Alarcón, 2026a), según se detalla en la siguiente subsección.

3.1. Uso de IA

Se utilizó IA generativa durante la elaboración de este informe. El marco Ciencia Generativa (Alarcón, 2026a) distingue entre roles centrales (Conceptualización, Metodología y Validación), que deben mantenerse bajo responsabilidad exclusivamente humana, y roles de apoyo (como Investigación, Análisis formal, Redacción del borrador original, Revisión y edición o Visualización), que pueden desarrollarse en colaboración con un sistema de IA. Siguiendo este marco, se delimitó desde el inicio que la selección del tema, la estructura del informe, las decisiones sobre qué supuestos usar en la estimación de costos y la validación final del contenido permanecerían bajo mi responsabilidad exclusiva, mientras que la IA apoyaría la búsqueda de fuentes de precios y estadísticas, la organización de esa información en tablas, la redacción del borrador y el formato del documento.

El modelo utilizado fue Claude Sonnet 5, a través de la plataforma Claude (Cowork).

Declaración de contribuciones según el marco Ciencia Generativa (Alarcón, 2026a):

Diego Ignacio Poveda Crisosto (Humano): Conceptualización, Metodología, Validación.

Claude Sonnet 5 (IA): Investigación, Análisis formal, Redacción del borrador original, Revisión y edición, Visualización.

Evaluación de la IA sobre la distribución de roles: se le pidió a Claude Sonnet 5 evaluar, en base al registro completo de la interacción sostenida durante la elaboración del informe, si la distribución de roles descrita correspondía al aporte real de cada parte. La IA confirmó que la elección del IIoT como tema, los supuestos de la estimación de costos y la validación final del contenido fueron definidos y aprobados por mí en cada etapa, mientras que su propia participación se limitó a la búsqueda de fuentes de precios y estadísticas, la organización de esa información en tablas comparativas, la redacción del borrador de texto y la elaboración del formato del documento en Word, sin haber intervenido en la definición de los supuestos económicos ni en la postura personal expresada en la discusión. La IA no reportó discrepancias entre esta descripción y el proceso efectivamente seguido, por lo que la distribución de roles indicada no se basa únicamente en mi propio criterio, sino que fue contrastada con la evaluación del sistema con el que interactué.

4. Resultados

4.1. Diferencias entre IoT general e IIoT

El IIoT es un subconjunto del Internet de las Cosas (IoT) orientado específicamente a entornos industriales. La Tabla 1 resume las principales diferencias documentadas entre ambos, según Neuron Team (2023).

Dimensión	IoT general	IIoT
Entorno típico	Hogar, oficina, dispositivos personales	Plantas industriales, minería, energía, logística
Protocolos	Wi-Fi, Bluetooth, Zigbee	Modbus, OPC-UA, PROFINET, EtherNet/IP, WirelessHART
Exigencia de fiabilidad	Tolerante a desconexiones ocasionales	Alta disponibilidad, ya que las interrupciones pueden detener la producción
Interoperabilidad	Ecosistemas cerrados de fabricante	Debe integrarse con PLC, SCADA y sistemas de control existentes
Certificación	Generalmente no requerida	Frecuentemente requiere certificación para zonas peligrosas (ATEX/Clase 1 Div. 2)

Tabla 1. Diferencias entre IoT general e IIoT (adaptado de Neuron Team, 2023).

Una aplicación industrial representativa del IIoT es el monitoreo predictivo de maquinaria rotativa: sensores inalámbricos de vibración y temperatura se instalan en motores, bombas y compresores, transmiten datos a un gateway industrial mediante protocolos como LoRaWAN o WirelessHART, y ese gateway reenvía la información a una plataforma en la nube que detecta patrones asociados a fallas incipientes antes de que ocurra una detención no programada.

4.2. Estimación de costos de una solución representativa

Se estimó el costo de modernizar una sección hipotética de planta compuesta por cincuenta activos rotativos críticos (motores, bombas y compresores) mediante sensores inalámbricos combinados de vibración y temperatura de gama media, un gateway industrial y una suscripción a una plataforma de gestión de mantenimiento (CMMS) con integración IIoT. La Tabla 2 presenta la estimación ascendente, construida a partir de los rangos de precio documentados por Oxmaint (2026). La fecha de esta estimación es el 26 de agosto de 2026 y todos los montos están expresados en dólares estadounidenses (USD), moneda en la que se reportan las fuentes consultadas.

Ítem	Costo unitario (USD)	Cantidad	Subtotal (USD)
Sensor inalámbrico vibración + temperatura (gama media)	600	50	30.000
Gateway industrial (LoRaWAN, cobertura 50-500 nodos)	1.500	1	1.500
Instalación y configuración por nodo	140	50	7.000
Subtotal inversión inicial (capex)	N/A	N/A	38.500
Suscripción CMMS anual (USD 9/activo/mes)	108/año	50	5.400-10.000*

Tabla 2. Estimación de costos para modernizar una sección de 50 activos rotativos con IIoT (elaboración propia a partir de rangos de precio de Oxmaint, 2026, Pelaez y Toro, 2025 y Honrubia, s. f.).

*El costo anual de operación se ajustó al rango de USD 8.000 a 18.000 reportado por Oxmaint (2026) para un sitio de cincuenta activos, ya que el cálculo lineal a partir del precio por activo subestima costos adicionales de soporte y almacenamiento de datos. Los supuestos centrales de esta estimación son: (a) los cincuenta activos no cuentan actualmente con ningún sistema de monitoreo digital, (b) se utiliza un sensor combinado de gama media en vez de sensores certificados para zona peligrosa, cuyo costo sería sustancialmente mayor, y (c) no se incluyen costos de integración con sistemas SCADA existentes, que dependen de la planta específica. El resultado del cálculo ascendente propio (USD 38.500 de inversión inicial) es coherente con el rango de USD 35.000 a 75.000 que Oxmaint (2026) documenta para un despliegue de cincuenta activos, lo que respalda la razonabilidad de los supuestos utilizados.

4.3. Evidencia sobre riesgos de ciberseguridad en IIoT

La incorporación de sensores y gateways IIoT amplía la superficie de ataque de una planta industrial. Según Khalil (2025), se registraron en promedio 820.000 ataques diarios contra dispositivos IoT durante 2025, un 46% más que el año anterior, y más de la mitad de los incidentes cibernéticos reportados a la SEC durante 2024 involucraron sistemas de tecnología operacional (OT). La misma fuente reporta que el costo promedio de una brecha de seguridad en el sector industrial asciende a USD 5,56 millones, y que un 5,27% de los ataques detectados explota directamente credenciales por defecto no cambiadas en los dispositivos.

5. Discusión

5.1. Sobre la elección del IIoT y su distinción del IoT general

Me parece que elegir el IIoT como caso de estudio, tal como sugiere la pauta, es acertado porque es una tendencia con aplicación directa a la disciplina del curso: a diferencia del IoT de consumo, el IIoT exige pensar en fiabilidad, protocolos industriales e interoperabilidad con sistemas de control ya instalados, que son justamente los temas centrales de un curso de automatización. La distinción entre ambos no es solo terminológica: instalar un sensor de consumo en una planta sin considerar certificación para zonas peligrosas o compatibilidad con el protocolo del PLC existente puede volver inútil la inversión, por lo que considero que esta distinción debería ser uno de los primeros criterios de decisión para cualquier proyecto de modernización.

5.2. Sobre la estimación de costos

Considero que el ejercicio de estimar costos de forma ascendente, y luego contrastar el resultado con un rango ya documentado en la literatura comercial, es una forma razonable de validar los supuestos propios sin tener acceso a cotizaciones reales de proveedores. El hecho de que mi cálculo (USD 38.500) caiga dentro del rango publicado por Oxmaint (2026) me da más confianza en que los supuestos de cantidad de sensores y tipo de gateway son razonables para una sección de planta de tamaño mediano. Sin embargo, reconozco una limitación importante: el costo real puede variar de forma significativa si los equipos existentes requieren sensores certificados para zonas peligrosas, que según las mismas fuentes pueden costar entre dos y tres veces más que los de gama media usados en esta estimación.

5.3. Sobre las ventajas y el riesgo de ciberseguridad

Las ventajas esperadas de esta modernización, entre ellas la reducción del tiempo de detención no planificada, la extensión de la vida útil de los equipos y una mejor toma de decisiones de mantenimiento basada en datos, me parecen suficientemente atractivas como para justificar la inversión calculada en la sección 4.2, especialmente si se compara con el costo de una sola falla no planificada en un activo crítico. Dicho esto, la evidencia de la sección 4.3 me convence de que el riesgo de ciberseguridad no es un tema secundario, ya que conectar equipos que tradicionalmente operaban aislados de la red corporativa (air-gapped) a una plataforma en la nube multiplica los puntos de entrada para un atacante, y el dato de que más de la mitad de los incidentes reportados a la SEC en 2024 involucraron sistemas OT sugiere que este no es un riesgo teórico, sino una tendencia ya en curso. Mi postura es que ninguna propuesta de modernización IIoT debería aprobarse sin un plan explícito de segmentación de red entre TI y OT y sin cambiar las credenciales por defecto de cada dispositivo, dado que ambos son vectores de ataque documentados y de bajo costo de mitigación en comparación con el costo de una brecha.

5.4. Sobre el modelo de negocio propuesto

Asumiendo el rol de gerente de una pequeña startup que integra soluciones IIoT, propongo un modelo de Hardware-as-a-Service (HaaS): la empresa compra los sensores y gateways a fabricantes especializados (los mismos evaluados en la Tabla 1, como Advantech, Teltonika o Siemens), y en vez de vendérselos al cliente final, los entrega en comodato junto con la plataforma de análisis y el soporte técnico, cobrando una suscripción mensual por activo monitoreado. Este modelo, descrito por Blankenship (2026) como uno de los cuatro modelos centrales de negocio en IoT, me parece más apropiado que la venta directa de hardware para el segmento de clientes que propongo, pequeñas y medianas empresas industriales sin sistemas de monitoreo digital previo, porque elimina la barrera de la inversión inicial de USD 38.500 calculada en la sección 4.2, que probablemente sea disuasiva para ese tipo de cliente. Como estrategia de acercamiento, propongo ofrecer un piloto de bajo costo en un subconjunto acotado de activos (entre cinco y diez) durante tres meses, de manera que el propio cliente pueda comprobar la reducción de fallas no planificadas antes de comprometerse a escalar la suscripción a toda la sección de planta. Esta lógica de demostrar valor antes de vender a escala coincide con lo que rinf.tech (s. f.) describe como una práctica común entre proveedores de soluciones IoT industriales que enfrentan clientes reacios al riesgo tecnológico.

5.5. Sobre el uso real de IA en este informe

Sobre el uso real que hice de la IA en este informe, mi valoración es positiva. Claude fue útil para encontrar y organizar rápidamente cifras de precios y estadísticas de ciberseguridad provenientes de múltiples fuentes dispersas, tarea que de forma manual me habría tomado bastante más tiempo, y para estructurar esa información en las tablas de la sección de Resultados. Al mismo tiempo, tuve que revisar con cuidado que cada cifra realmente proviniera de la fuente citada y no fuera una aproximación genérica, y decidir yo mismo qué supuestos usar para la estimación de costos y qué postura tomar frente al riesgo de ciberseguridad, ya que esas decisiones no pueden delegarse sin perder el criterio propio que se espera de este informe. Esa experiencia confirma, en la práctica, lo que plantea el marco utilizado: la IA acelera bastante el trabajo de apoyo, pero el criterio final necesita revisión humana activa.

6. Conclusiones

Los principales aportes de este informe son tres. Primero, que el IIoT se distingue del IoT general principalmente por sus exigencias de fiabilidad, sus protocolos industriales y la necesidad de interoperar con sistemas de control ya instalados, lo que lo hace más complejo de adoptar que un dispositivo IoT de consumo pero también más relevante para la disciplina de automatización. Segundo, que modernizar una sección de cincuenta activos rotativos mediante sensores inalámbricos de vibración y temperatura implica una inversión inicial estimada de USD 38.500 más un costo anual de operación cercano a los USD 10.000, cifra que resulta coherente con los rangos ya documentados en la literatura comercial revisada. Tercero, que el principal riesgo de esta modernización no es técnico sino de ciberseguridad, dado que conectar equipos OT tradicionalmente aislados a la nube amplía significativamente la superficie de ataque de la planta. A partir de estos hallazgos, se propone un modelo de negocio de Hardware-as-a-Service que reduce la barrera de adopción para pequeñas y medianas empresas industriales al eliminar la necesidad de una inversión inicial de capital, trasladando el costo a una suscripción mensual por activo monitoreado.

Declaraciones

Declaración de contribuciones (marco Ciencia Generativa, Alarcón, 2026a, detalle del proceso en la sección 3.1): Diego Ignacio Poveda Crisosto (Humano): Conceptualización, Metodología, Validación. Claude Sonnet 5 (IA), plataforma Claude (Cwork): Investigación, Análisis formal, Redacción del borrador original, Revisión y edición, Visualización.

Yo, Diego Ignacio Poveda Crisosto, autor de este informe, declaro lo siguiente:

- Intención de publicación con nombre y apellido real: autorizo la publicación de este informe identificándome con mi nombre y apellido real, Diego Ignacio Poveda Crisosto.
- Consentimiento de modificación por coautores: autorizo que este informe sea modificado por coautores, previa revisión editorial.
- Consentimiento de publicación en sitios web: autorizo la subida de este informe a sitios web de informes académicos.

Diego Ignacio Poveda Crisosto, 2026-08-26

Licencia: Creative Commons Atribución 4.0 Internacional (CC BY 4.0) - <https://creativecommons.org/licenses/by/4.0/> - versión actualizada 2026-09-22.

Bibliografía

- Alarcón, C. (2026a). Generative Science as an analytical framework for integrating the full capabilities of generative artificial intelligence into scientific research while preserving scientific recognition. Generative Science Preprints, 2026(07), 19055673. <https://doi.org/10.5281/zenodo.19055673>
- Alarcón, C. (2026b). Ciencia Generativa y dos rutas de aprendizaje como respuesta al uso intensivo de inteligencia artificial y a los requerimientos de la Ley N° 21.545 en un curso universitario de automatización. Informes Técnicos de Automatización, 2026(04), 19686071. <https://doi.org/10.5281/zenodo.19686071>
- Khalil, M. (2025, 24 de agosto). IoT Hacking Statistics 2026: Threats, Costs & Regulations [Actualizado el 27 de agosto de 2026]. DeepStrike. <https://deepstrike.io/blog/iot-hacking-statistics>
- Neuron Team. (2023, 17 de octubre). IIoT vs. IoT: Examples and 5 Key Differences. EMQ. <https://www.emqx.com/en/blog/iiot-vs-iiot-examples-and-5-key-differences>
- Honrubia, M. (s. f.). Industrial IoT is booming thanks to a drop in Sensor Prices. Ennomotive. <https://www.ennomotive.com/industrial-iiot-sensor-prices/>
- Oxmaint. (2026, 28 de mayo). Wireless Predictive Maintenance Cost, Pricing & ROI Calculator 2026. <https://oxmaint.com/blog/post/wireless-predictive-maintenance-cost-pricing-roi>
- rinf.tech. (s. f.). 8 IoT Business Models for Connected Product Strategy. <https://www.rinf.tech/8-iiot-business-models-for-connected-product-strategy/>
- Pelaez, A., y Toro, A. (2025, 4 de junio). Industrial IoT & Edge IoT Gateways: 10+ Best Models for 2025 (+Protocol & Price Table). Ubidots. <https://ubidots.com/blog/top-industrial-iiot-gateways/>
- Blankenship, R. (2026, 5 de junio). The 4 Core Business Models of IoT: From Connectivity to Outcomes. Zuora. <https://www.zuora.com/guides/iiot-business-models/>