Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Reporte de Vulnerabilidades en IIoT. Proyecto DEFENDER.

Pedro Almansa Jiménez

Lorenzo Fernández Maimó

Ángel Luis Perales Gómez

Diciembre 2024

UNIVERSIDAD DE MURCIA

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Contents

1 Introducción IIoT

1.1 Objetivos del Reporte

El objetivo principal de este informe técnico es realizar un estudio exhaustivo sobre los dispositivos que operan en entornos del Internet Industrial de las Cosas (IIoT), describiendo los escenarios que caracterizan esta categoría y analizando las vulnerabilidades que comprometen su seguridad. Para ello, se busca identificar y analizar las principales clases de dispositivos IIoT, describiendo sus características, funcionalidades y roles dentro de los sistemas industriales. Este análisis permitirá comprender cómo estos dispositivos interactúan y cumplen con los requerimientos de entornos industriales críticos.

Asimismo, el informe examina los entornos específicos en los que operan estos dispositivos, destacando las particularidades de los escenarios industriales y las condiciones bajo las cuales funcionan. Además, se analizan las vulnerabilidades exponiendo los vectores, objetivos, impacto y consecuencia de las mismas. Posteriormente se explican las fases típicas de un ataques junto a una selección de casos reales de ataques documentados junto con su clasificación según la taxonomía expuesta en el apartado 3. Esto proporciona una visión integral de las posibles amenazas que comprometen la seguridad, evaluando el impacto que estas vulnerabilidades pueden tener en los entornos industriales.

Finalmente, se presentan una recopilación de algunas de las contra medidas de seguridad mas recientes y eficaces como soluciones a los problemas de seguridad de los sistemas industriales. Hace especial énfasis en enfocar la importancia del Machine Learning en el desarrollo de estos enfoques.

1.2 Definición y Características

El Internet Industrial de las Cosas (IIoT, por sus siglas en inglés) es una extensión especializada del Internet de las Cosas (IoT), enfocada en aplicaciones industriales y sistemas ciberfísicos. Mientras que el IoT conecta dispositivos de uso cotidiano como electrodomésticos, sensores domésticos y wearables, el IIoT se centra en la interconexión de máquinas, sensores avanzados, actuadores y sistemas industriales en entornos como fábricas, plantas energéticas y cadenas de suministro. Esta tecnología busca no solo recopilar y analizar datos, sino también optimizar procesos industriales críticos mediante la automatización.

Entre las principales características del IIoT destaca su alta conectividad y escalabilidad, diseñada para manejar una enorme cantidad de dispositivos y datos en tiempo real. A diferencia del IoT, el IIoT requiere protocolos de comunicación robustos y confiables que garanticen la integridad y disponibilidad de los datos en entornos industriales exigentes.

Otra característica clave del IIoT es su enfoque en la resiliencia y seguridad, dado que los dispositivos suelen operar en infraestructuras críticas donde cualquier vulnerabilidad puede tener consecuencias graves, como interrupciones operativas o riesgos para la seguridad humana hacen que el trabajo y la mejora de métodos y herramientas para mitigar estas amenazas se haya vuelto algo crucial.

Por último, el IIoT se caracteriza por su interoperabilidad y capacidad de integración con tecnologías emergentes como la computación en la nube, el edge computing y los sistemas de inteligencia artificial. Esto permite que los dispositivos no solo interactúen entre sí, sino que también integren los datos recopilados en plataformas de análisis para mejorar la toma de decisiones, reducir costos operativos y aumentar la eficiencia de las operaciones industriales.

1.3 Aplicaciones Clave

El Internet Industrial de las Cosas (IIoT) ha revolucionado múltiples industrias al introducir dispositivos conectados que mejoran la eficiencia y automatizan procesos volviéndose un elemento prácticamente imprescindible en multitud de sectores críticos. A continuación, se destacan las aplicaciones clave y los sectores donde el IIoT está teniendo un rol cada vez mayor:

- **Industrial y manufacturero**: El IIoT desempeña un papel fundamental en la automatización de líneas de producción, el mantenimiento predictivo de maquinaria y la optimización de la logística. Los sensores y dispositivos conectados recopilan datos en tiempo real, permitiendo la detección temprana de fallos, la reducción de tiempos de inactividad y el incremento de la productividad mediante análisis avanzados y sistemas de control.
- **Energía e infraestructuras críticas**: El IIoT se aplica para la monitorización de redes eléctricas, plantas de energía y sistemas de distribución. Dispositivos conectados permiten gestionar de manera eficiente el consumo energético, predecir fallos en infraestructuras como turbinas eólicas o redes de distribución, y garantizar la seguridad operativa en plantas nucleares o de petróleo y gas.
- **Transporte y logística**: El IIoT facilita la gestión de flotas mediante el rastreo de vehículos en tiempo real, la monitorización de condiciones de transporte de mercancías sensibles (como alimentos perecederos o productos

farmacéuticos) y la optimización de rutas logísticas. Esto se traduce en menores costos operativos y mayor confiabilidad en las cadenas de suministro.

- **Salud y medicina industrial**: El IIoT se utiliza en hospitales inteligentes y plantas farmacéuticas, donde sensores y dispositivos conectados garantizan el monitoreo de equipos médicos, el control de condiciones ambientales en laboratorios y la seguridad en procesos de producción farmacéutica, cumpliendo con estrictos estándares regulatorios.

1.4 Crecimiento del Mercado y su Impacto en la Seguridad

El mercado de IoT, y en particular el de IIoT, ha experimentado un crecimiento exponencial en los últimos años, impulsado por la creciente adopción de tecnologías digitales y la necesidad de soluciones inteligentes en entornos industriales críticos. El tamaño del mercado de Internet de las cosas se estima en USD 1,17 billones en 2024 y se espera que alcance los USD 2,37 billones para 2029.[1]. Según informes recientes, se espera que el número de dispositivos IoT activos supere los 30 mil millones para 2025, con una proporción significativa atribuida a dispositivos IIoT.

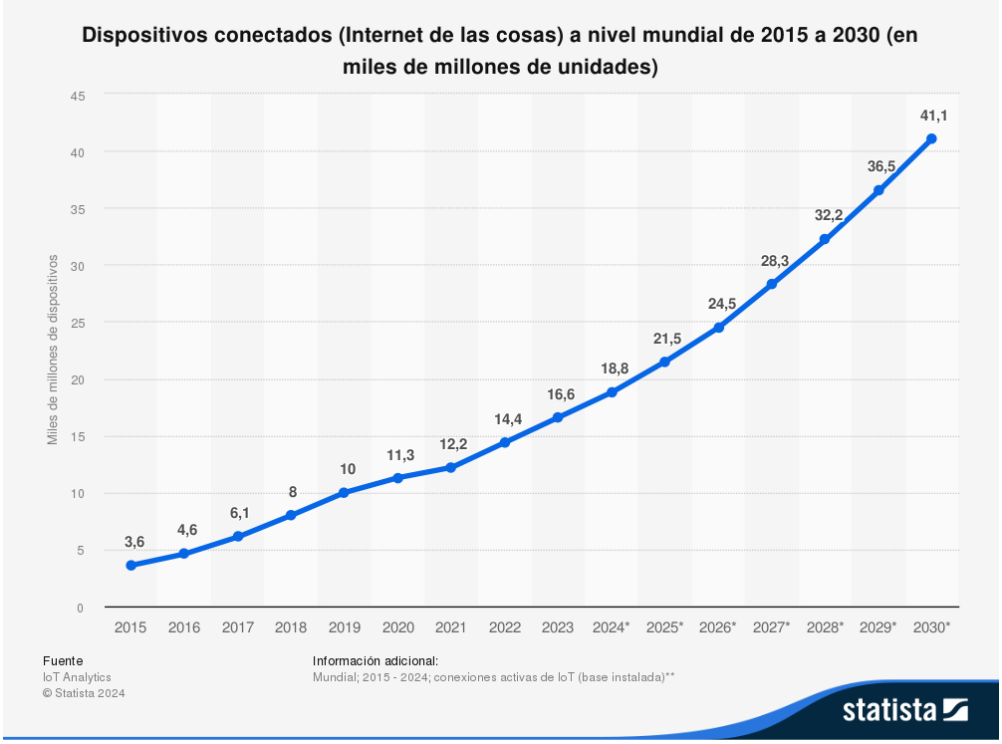

Figure 1: Proyección del crecimiento del mercado de IoT hasta 2030.

Dentro de la industria se espera que los avances en dispositivos de campo, sensores y robots amplíen aún más el alcance del mercado, especialmente en aplicaciones de la Industria 4.0. Las tecnologías IIoT están superando la escasez de mano de obra en el sector manufacturero y mejorando la eficiencia en la producción. Para cada vez más organizaciones, el uso de tecnologías como la robotización y el mantenimiento predictivo forma parte de las operaciones diarias. Un estudio realizado por la empresa de IoT Industrial (IIoT) Microsoft Corporation encontró que el 85% de las empresas tienen al menos un proyecto de caso de uso de IIoT.[2]

Sin embargo, este crecimiento también ha expuesto importantes retos de seguridad, particularmente en el ámbito de IIoT, donde los dispositivos forman parte de infraestructuras críticas. Muchos dispositivos carecen de diseños seguros, lo que los hace vulnerables a ataques como el acceso no autorizado, la manipulación de datos y el uso indebido para redes de botnets. La seguridad de los dispositivos IIoT no solo afecta a los usuarios finales, sino que también tiene implicaciones significativas para la infraestructura crítica y la economía global. Un informe de Kaspersky destaca que los ataques de

[1]Fuente: Statista Research Department, 2024. Disponible en: `https://es.statista.com/temas/6976/el-internet-de-las-cosas-iot/`

[2]Fuente: Microsoft Corporation. Disponible en: `https://news.microsoft.com/es-es/2019/08/06/microsoft-presenta-iot-signals-un-estudio-sobre-el-estado-de-adopcion-del-internet-of-things/`.

malware dirigidos a dispositivos IoT aumentaron significativamente en la primera mitad de 2023 en comparación con 2022.[3]

[3]Fuente: Kaspersky Lab, "IoT under attack: 400% increase in malware targeting connected devices", 2023. Disponible en: `https://www.kaspersky.com/`.

2 Entorno IIoT

Los entornos del **Internet Industrial de las Cosas (IIoT)** son sistemas complejos que combinan dispositivos físicos, software y redes avanzadas para operar en escenarios industriales críticos. A diferencia de las aplicaciones genéricas del IoT, los entornos IIoT requieren una infraestructura robusta y específica, diseñada para cumplir con las exigencias de sectores como la manufactura, la energía y el transporte.

Un entorno IIoT típico, como se ilustra en la Figura 2, integra múltiples niveles, desde los dispositivos de campo, como sensores y actuadores, hasta plataformas avanzadas para análisis de datos y gestión en la nube. Esta estructura modular permite la interoperabilidad entre diferentes componentes y sistemas, algo crucial en un entorno tan diverso.

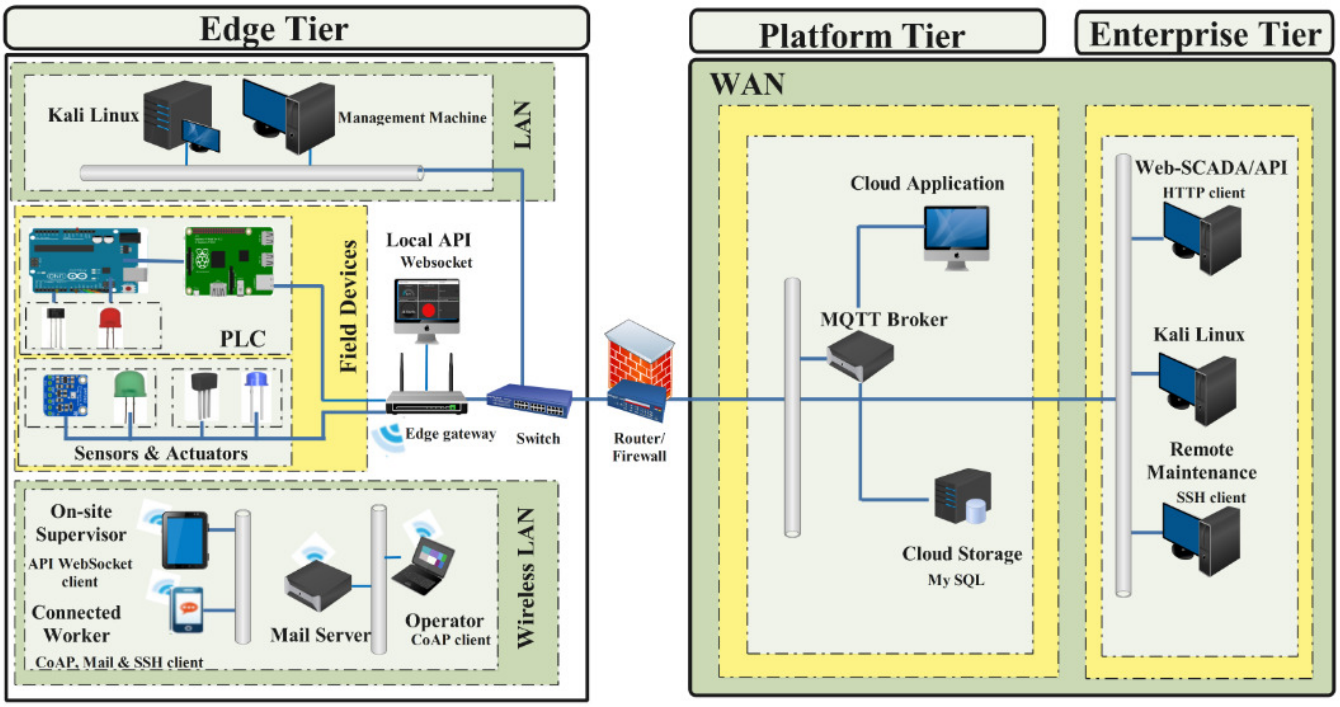

Figure 2: Entorno IIoT. Imagen adaptada de [18].

Además, estos entornos dependen de protocolos de comunicación industriales para asegurar la transmisión eficiente y segura de datos entre dispositivos y plataformas. La integración de métricas relevantes, como la latencia de la red, la disponibilidad del sistema y la seguridad de los datos, es esencial para medir el rendimiento y garantizar la sostenibilidad de las operaciones. Estas características hacen que los entornos IIoT sean fundamentales para la transformación digital en la industria, sentando las bases para la Industria 4.0.

En este sentido, la implementación de tecnologías de comunicación de vanguardia, como el 5G, cobra especial relevancia, ya que no solo reduce la latencia a niveles mínimos al facilitar respuestas casi en tiempo real, sino que también ofrece mayor ancho de banda y confiabilidad. Esto resulta fundamental para afianzar la coordinación y eficiencia de los procesos industriales en un entorno cada vez más interconectado.

2.1 Dispositivos IIoT

Los dispositivos del Internet Industrial de las Cosas (IIoT) se pueden clasificar en diversas categorías, cada una con funciones específicas que contribuyen a la automatización, el monitoreo y la optimización de procesos en entornos industriales. A continuación, se presentan algunas de las principales categorías y sus dispositivos más destacados:

2.1.1 Dispositivos de Adquisición de Datos

Sensores Industriales: Son dispositivos esenciales para recopilar datos en tiempo real de variables como temperatura, presión, vibración, humedad, entre otros. Su precisión y capacidad de resistencia a condiciones extremas los hacen ideales para aplicaciones críticas en plantas industriales.

Cámaras y Sensores de Visión: Utilizados para inspección visual y control de calidad, estos dispositivos incorporan capacidades de inteligencia artificial para identificar defectos, realizar mediciones y optimizar procesos. Las cámaras de visión infrarroja, por ejemplo, son fundamentales para detectar anomalías térmicas.

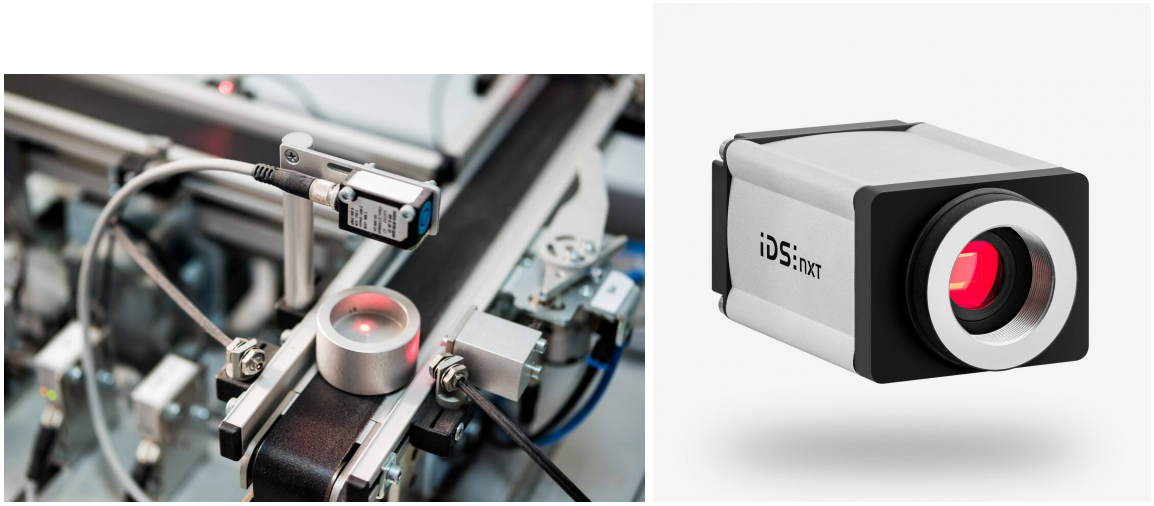

Figure 3: Izquierda: Sensor industrial. Derecha: Cámara de visión infrarroja.

2.1.2 Dispositivos de Control

Controladores Lógicos Programables (PLCs): Estos equipos gestionan procesos automatizados, tomando decisiones en función de datos recopilados por sensores. Su programación flexible permite adaptarlos a diversos procesos industriales, desde líneas de ensamblaje hasta sistemas de distribución.

Figure 4: Izquierda: Controlador Lógico Programable (PLC).

2.1.3 Dispositivos de Conexión y Gestión de Redes

Gateways Industriales: Actúan como intermediarios entre redes locales y servicios en la nube. Facilitan la transmisión de datos a plataformas de análisis, integrando dispositivos de campo con sistemas empresariales para monitoreo remoto y gestión centralizada.

Mail Servers y Redes LAN: En entornos IIoT, servidores locales y gateways aseguran la comunicación eficiente entre niveles del sistema. Esto incluye tanto conexiones a dispositivos como la transmisión segura de datos hacia servidores remotos o aplicaciones en la nube.

Figure 5: Gateway Industrial.

2.1.4 Sistemas de Automatización

Actuadores: Convierte señales electrónicas en acciones físicas, como abrir válvulas, mover piezas o accionar motores. Los actuadores pueden ser hidráulicos, neumáticos o eléctricos, dependiendo de las necesidades del entorno.

Robots Industriales: Diseñados para realizar tareas específicas como ensamblaje, soldadura o transporte de materiales. Los robots multiarticulados son altamente versátiles y mejoran significativamente la precisión y la eficiencia en entornos industriales.

Figure 6: Izquierda: Actuador hidráulico industrial. Derecha: Brazo robótico multiarticulado.

2.2 Arquitectura del Entorno

La arquitectura de un entorno IIoT puede ser tremendamente diversa. Cada sector industrial, cada conjunto de dispositivos y cada estrategia de negocio demandan requisitos específicos que pueden variar considerablemente. Elementos como el tamaño de la empresa o fábrica, o el presupuesto disponible para invertir en infraestructura IIoT, marcan factores diferenciales a la hora de moldear los entornos. Esto, a su vez, da lugar a la existencia de entornos "híbridos", en los que elementos de IIoT se combinan con máquinas y sistemas desfasados y obsoletos, lo que no hace sino añadir una capa más de complejidad a la defensa de estos entornos.

Sin embargo para para tener un modelo de referencia hemos seleccionado el fundamentado en el modelo de referencia *Industrial Internet Reference Architecture (IIRA)* [7], establecido por el *Industrial Internet Consortium (IIC)* [6]. . Este modelo proporciona un marco estandarizado para diseñar sistemas IIoT que integren de manera eficiente los flujos de datos, las interacciones entre dispositivos y las capas de control necesarias en entornos industriales críticos. La estructura propuesta comprende tres niveles principales, cada uno con funciones específicas para garantizar interoperabilidad, escalabilidad y seguridad:

- **Capa de Borde (*Edge Tier*):** Este nivel constituye la interfaz directa entre los procesos físicos y el sistema digital. Los **sensores y actuadores** son responsables de monitorear y controlar variables críticas, como temperatura, presión y vibración, en tiempo real. Los **controladores lógicos programables (PLCs)**, ampliamente utilizados en sistemas industriales, gestionan los procesos automatizados mediante lógica predefinida. Por último, los **gateways industriales** actúan como puntos de convergencia, conectando la red local de dispositivos (OT) con servicios en la nube o plataformas (IT), utilizando protocolos estándar como OPC UA y MQTT. Esta capa se diseña para garantizar confiabilidad, baja latencia y adaptabilidad a entornos dinámicos.
- **Capa de Plataforma (*Platform Tier*):** Este nivel opera como el núcleo del procesamiento y almacenamiento de datos, gestionando tanto información en tiempo real como datos históricos. Las **bases de datos y sistemas de almacenamiento** soportan grandes volúmenes de datos generados por los dispositivos de la capa de borde. Además, esta capa incluye **sistemas de análisis avanzados**, que permiten extraer patrones, detectar anomalías y ejecutar algoritmos de inteligencia artificial o aprendizaje automático. El diseño de esta capa sigue las recomendaciones del IIRA para garantizar interoperabilidad y soporte a aplicaciones de alto nivel.
- **Capa Empresarial (*Enterprise Tier*):** Diseñada para la interacción humana y la toma de decisiones estratégicas, esta capa incluye herramientas como **sistemas SCADA y aplicaciones API** para monitorear y controlar procesos en tiempo real. Además, integra **sistemas de gestión empresarial (ERP)** que facilitan la planificación, supervisión y optimización de operaciones. Según el IIRA, esta capa debe priorizar la seguridad y la accesibilidad, permitiendo que los datos y análisis de las capas inferiores respalden decisiones empresariales informadas.

Si bien la adopción de este estándar como estructura base de una arquitectura IIoT facilita la labor de estudio de entornos de esta clase, cabe recordar que los entornos IIoT puede ser tremendamente diversos. Sin embargo es útil para situarnos en un marco ampliamente aceptado de lo que debería ser un escenario de este estilo.

2.3 Protocolos y Comunicaciones

La arquitectura típica de un entorno **IIoT!**s (**IIoT!**s) integra distintos niveles o capas de comunicación: dispositivos (sensores, actuadores, cámaras), pasarelas (*gateways*), sistemas de gestión de datos y plataformas en la nube o *edge computing* [31]. Cada una de estas capas se apoya en diferentes protocolos de red, concebidos para satisfacer requisitos de baja latencia, escalabilidad, capacidad de transmisión en tiempo real y compatibilidad con dispositivos de recursos reducidos. Según el análisis realizado por Ramírez Delgado y Díaz-Piraquive [10] y el estudio de Mekala et al. [31], la adopción de protocolos de comunicación para entornos IIoT se concentra, principalmente, en los siguientes conjuntos:

- **Protocolos M2M (Machine-to-Machine).** Estos protocolos gestionan el intercambio directo de datos entre equipos industriales (p. ej., sensores, **PLC!**s (**PLC!**s), actuadores). Algunos ejemplos destacados incluyen:
  - **MQTT (Message Queue Telemetry Transport).** Protocolo ligero de mensajería basado en **TCP!**/**IP!**, con un modelo de suscripción y publicación (*publish–subscribe*). Empleado en múltiples sectores industriales gracias a su facilidad de configuración y bajo consumo de ancho de banda.
  - **CoAP (Constrained Application Protocol).** Diseñado para dispositivos con recursos limitados y enfocado en entornos **IoT!** (**IoT!**) basados en **IPv6!**. Ofrece modos de comunicación *request–response* y *publish–subscribe*, con un encabezado reducido que facilita la interacción en redes de baja potencia.

  - **DDS (Data Distribution Service).** Enfatiza un modelo de datos centrado en la comunicación entre nodos de *edge*. Es descentralizado y soporta el envío de datos tanto por **UDP!**/**IP!** como por **TCP!**/**IP!**. Se utiliza a menudo en sistemas de control distribuidos que requieren un bajo retardo y gran robustez (p. ej., gestión de redes eléctricas, tráfico aéreo o transporte).
  - **AMQP (Advanced Message Queuing Protocol).** Protocolizado en un modelo de *publish–subscribe* confiable y orientado a mensajería corporativa. Facilita el intercambio fiable de datos con acuses de recibo y es común en sistemas donde se requiere transaccionalidad y asincronía.
  - **MODBUS/TCP.** Utilizado profusamente en redes industriales para la comunicación entre dispositivos de supervisión (**SCADA!** (**SCADA!**)) y **PLC!**s. Emplea un esquema maestro–esclavo sobre **TCP!**/**IP!** y destaca por su facilidad de implementación y por su amplia adopción en la industria.
  - **CAN (Controller Area Network).** Orientado a entornos con requisitos de robustez y operación en tiempo real (por ejemplo, vehículos o maquinaria industrial). Opera sobre un bus de comunicaciones en serie, optimizado para escenarios de alta fiabilidad.
  - **WirelessHART.** Estándar abierto ideado para la comunicación inalámbrica en procesos industriales. Emplea topologías en malla (*mesh*) y habilita la conectividad entre sensores y actuadores en condiciones difíciles, aportando alta disponibilidad.
  - **NB-IoT (Narrowband IoT).** Tecnología **LPWAN!** (**LPWAN!**) celular de bajo consumo y gran cobertura, pensada para la conexión de una gran cantidad de dispositivos con un coste de mantenimiento reducido (por ejemplo, *smart buildings*, *smart cities*, etc.).

- **Protocolos H2M (Human-to-Machine).** Estos protocolos permiten la interacción con los operadores humanos para fines de monitorización y control:
  - **HTTP (HyperText Transfer Protocol).** Presente en interfaces web para la administración de dispositivos y la visualización de datos. En el ámbito IIoT, se utiliza a menudo en plataformas de supervisión remota y herramientas de diagnóstico.
  - **CoAP.** Además de su uso en M2M, sus modos de operación ligeros también pueden facilitar la comunicación con aplicaciones humanas, sobre todo en redes con recursos muy restringidos.

- **Protocolos de Red y Estructuras de Enlace.**
  - **TCP!/IP! y UDP!.** Forman la base del ecosistema IIoT al proporcionar transporte confiable o de baja latencia, respectivamente.
  - **Fieldbus (p. ej., PROFIBUS, DeviceNet, Foundation Fieldbus).** Agrupa diversos estándares para la automatización industrial, interconectando sensores, actuadores y **HMI!**s (**HMI!**s) en topologías como buses, anillos o mallas. Permite la digitalización de procesos críticos y la integración con capas de supervisión.
  - **LoRaWAN (Long Range Wide Area Network).** Aunque no se detalla profundamente en algunos estudios de IIoT industriales, es considerado un protocolo **LPWAN!** relevante para la monitorización de sensores distribuidos a gran distancia y con muy bajo consumo.
  - **ZigBee y 6LoWPAN.** Orientados a redes de baja potencia y bajo costo. Suelen utilizarse en escenarios de corto alcance (ZigBee) o para habilitar conectividad **IPv6!** en dispositivos con recursos muy limitados (6LoWPAN).

Como señalan Qiu et al. [35] y Boyes et al. [3], la adopción de estos protocolos permite a la industria abordar el reto de la interconexión masiva de equipos heterogéneos, habilitando la monitorización en tiempo real y la integración de datos para su análisis en la nube. Cada protocolo presenta capacidades específicas (estructura de mensajes, modelo de comunicación, escalabilidad), y su elección depende de factores como el número de dispositivos, los requerimientos de latencia o la disponibilidad de ancho de banda. La compatibilidad entre capas de red y la correcta configuración de los dispositivos resultan, por tanto, fundamentales para asegurar la fluidez y fiabilidad de las comunicaciones en un entorno industrial de nueva generación.

2.4 Controladores en el Entorno Industrial

Los sistemas de control son componentes esenciales en los entornos industriales, desempeñando un papel crítico en la operación, supervisión y optimización de infraestructuras clave como fábricas inteligentes, cadenas de suministro y procesos mineros. Estos sistemas permiten monitorear variables físicas, gestionar activos distribuidos y garantizar la eficiencia operativa mediante la interacción entre sensores, actuadores y controladores. Su función principal radica en recopilar datos en tiempo real, analizarlos y ejecutar acciones correctivas o preventivas para mantener los procesos dentro de los parámetros deseados. Los sistemas de control pueden adoptar diferentes arquitecturas dependiendo de las necesidades del entorno, destacando los sistemas centralizados, descentralizados y jerárquicos como los modelos más comunes [44]. A continuación, se describen las características principales de cada uno de estos enfoques.

- **Sistemas de Control Centralizado:** En los sistemas de control centralizado, un único controlador supervisa y gestiona múltiples subsistemas dentro de la arquitectura del sistema. Este controlador centralizado recibe datos de sensores que registran el estado operativo de los subsistemas y envía señales de comando a los actuadores correspondientes para ajustar su comportamiento. Un ejemplo clásico de este tipo de sistema es el *SCADA* (Sistema de Control Supervisado y Adquisición de Datos), ampliamente utilizado en redes eléctricas y sistemas de distribución de agua [26]. Aunque estos sistemas ofrecen ventajas como la centralización de datos y la facilidad de supervisión, también presentan vulnerabilidades significativas debido a su dependencia de plataformas heredadas y la falta de actualizaciones frecuentes, lo que los expone a amenazas cibernéticas [45].

- **Sistemas de Control Descentralizado:** Por otro lado, los sistemas de control descentralizado distribuyen la responsabilidad del control entre varios controladores individuales, cada uno dedicado a un subsistema específico. Esta arquitectura permite una mayor flexibilidad y capacidad de respuesta local, ya que los controladores no dependen de un único punto de control. Un ejemplo destacado es el *Sistema de Control Distribuido* (DCS), que combina múltiples controladores para coordinar procesos complejos de producción industrial [44]. Otro caso relevante son los *Controladores Lógicos Programables* (PLCs), que interpretan señales de sensores y generan respuestas automáticas a intervalos regulares. Estos sistemas son ampliamente utilizados en industrias manufactureras y pueden mejorarse con tecnologías inalámbricas como *RFID* para aumentar su agilidad operativa [41].

- **Sistemas de Control Jerárquico:** Finalmente, los sistemas de control jerárquico adoptan una estructura multinivel para manejar operaciones complejas y a gran escala. En este modelo, los controladores locales en el nivel inferior interactúan directamente con los subsistemas, mientras que los niveles superiores se encargan de la supervisión general y la coordinación estratégica. Esta arquitectura permite una gestión eficiente de sistemas industriales complejos, integrando funcionalidades de SCADA y DCS según sea necesario [41]. Además, los sistemas jerárquicos facilitan la escalabilidad y la segmentación de tareas, lo que los hace ideales para entornos donde la precisión y la adaptabilidad son prioritarias. Sin embargo, su complejidad puede introducir desafíos adicionales en términos de seguridad y mantenimiento [26].

3 Vulnerabilidades

Los entornos del Internet Industrial de las Cosas (IIoT) han revolucionado la forma en que las industrias operan, integrando dispositivos inteligentes, sistemas automatizados y plataformas avanzadas. Sin embargo, este crecimiento ha venido acompañado de un aumento exponencial en la cantidad de dispositivos interconectados, lo que implica una mayor exposición a la **red global**. Este nivel de conectividad ha incrementado significativamente la superficie de ataque, dejando a los sistemas industriales vulnerables frente a amenazas cibernéticas.

Una **vulnerabilidad** puede entenderse como cualquier debilidad inherente en el diseño, la implementación o la configuración de un sistema que puede ser explotada por un atacante para comprometer su integridad, disponibilidad o confidencialidad. En los entornos IIoT, estas vulnerabilidades pueden surgir tanto de los dispositivos individuales, como sensores y actuadores, como de las plataformas que los gestionan, los protocolos de comunicación empleados o las aplicaciones en la nube.

Para abordar este tema y poder presentar una exposición clara y organizada de las vulnerabilidades en entornos IIoT utilizaremos como punto de partida la taxonomía propuesta en **Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures** [34]

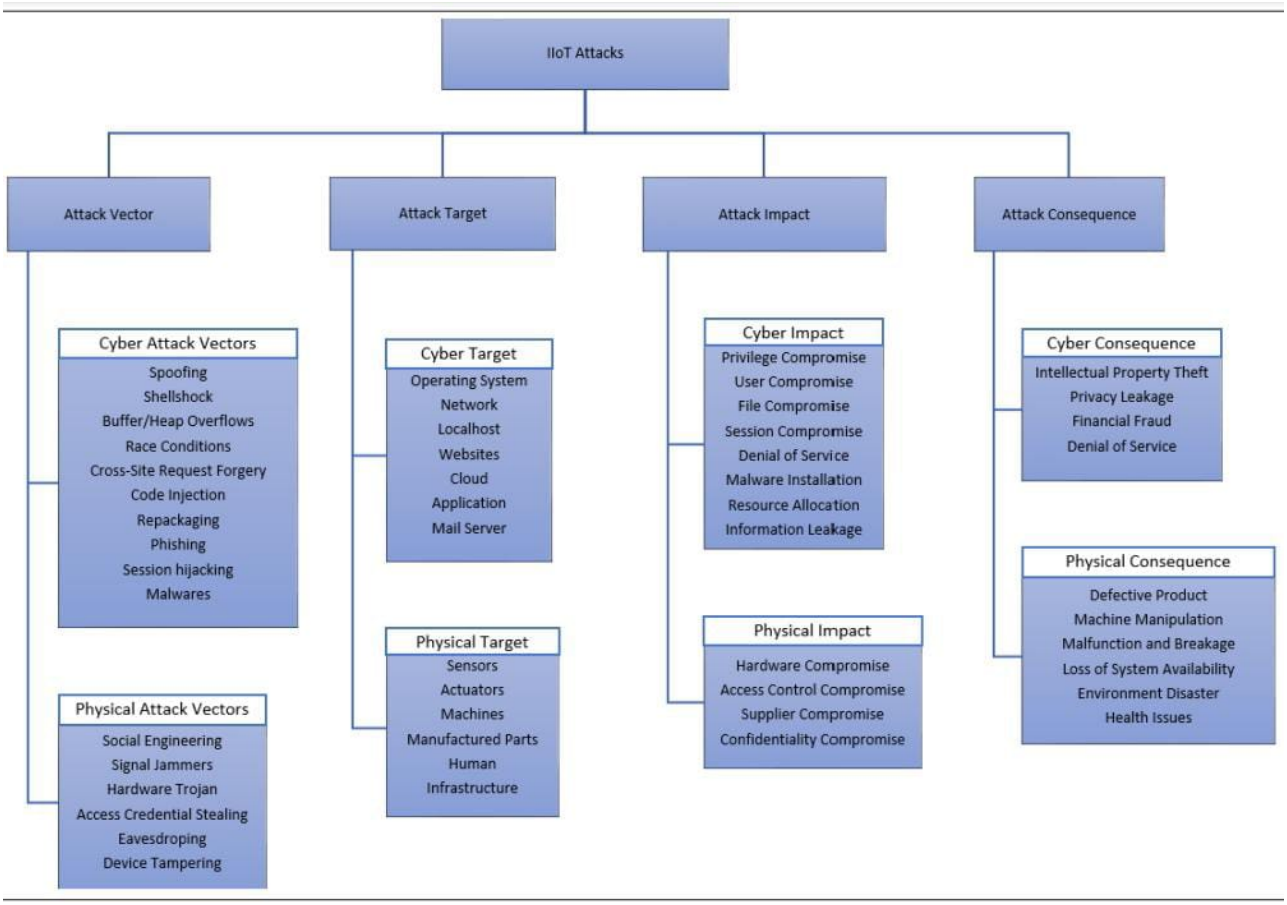

Figure 7: Taxonomia ataques en IIoT. Imagen adaptada de [34].

3.1 Vectores de Ataque

Un **vector de ataque** se define como la ruta o método que un adversario utiliza para explotar vulnerabilidades en un sistema, con el objetivo de comprometer su confidencialidad, integridad o disponibilidad. En entornos IIoT, estos vectores son particularmente críticos debido a la integración de sistemas operativos (OT) y tecnológicos (IT), así como a la exposición física de dispositivos en infraestructuras industriales. Según la taxonomía propuesta por Panchal et al. [34], los vectores de ataque en IIoT se clasifican en dos categorías principales: *cibernéticos* y *físicos*. A continuación, se detallan mas en profundiad.

Cibernéticos

Los vectores de ataque cibernéticos son aquellos que no requieren interacción física con los dispositivos o infraestructuras industriales, centrándose en vulnerabilidades en los sistemas de TI (Tecnología de la Información) y las redes de comunicación. Estos vectores incluyen:

- **Spoofing**: Suplantación de identidad en la que un atacante se hace pasar por un usuario o dispositivo legítimo.
- **Shellshock**: Ejecución remota de código mediante vulnerabilidades en intérpretes de comandos.
- **Buffer/Heap Overflow**: Desbordamiento de memoria que permite la ejecución de código malicioso.
- **Race Condition**: Condiciones de carrera donde múltiples procesos compiten por el acceso a un recurso compartido.
- **CSRF (Cross-Site Request Forgery)**: Envío de solicitudes maliciosas desde un usuario autenticado sin su conocimiento.
- **Inyección de Código (Code Injection)**: Introducción de código malicioso en aplicaciones vulnerables.
- **Reempaquetado (Repackaging)**: Alteración de aplicaciones legítimas para incluir código malicioso.
- **Phishing**: Engaños para obtener información confidencial haciéndose pasar por entidades confiables.
- **Secuestro de Sesión (Session Hijacking)**: Robo de cookies de sesión para tomar el control de una sesión activa.
- **Malware**: Software malicioso, como virus, gusanos, troyanos, rootkits, spyware, botnets y ransomware, diseñado para comprometer sistemas.

Físicos

Los vectores de ataque físicos requieren interacción directa con dispositivos o personas dentro del entorno industrial. Estos vectores incluyen:

- **Jamming de Señales**: Interrupción intencionada de las comunicaciones inalámbricas mediante la emisión de señales interferentes.
- **Troyanos de Hardware** : Modificaciones maliciosas en el hardware durante su diseño o fabricación, activadas bajo condiciones específicas.
- **Robo de Credenciales de Acceso**: Obtención de contraseñas, tarjetas de acceso u otros medios de autenticación legítimos, ya sea mediante espionaje físico (como *shoulder surfing*) o técnicas como el *tailgating*.
- **Escuchas Clandestinas** : Monitoreo no autorizado de comunicaciones privadas para recopilar información confidencial.
- **Manipulación de Dispositivos**: Alteración física de dispositivos, como desactivar mecanismos de seguridad o modificar configuraciones críticas.
- **Ingeniería Social** : Interacción social para engañar a personas y obtener información confidencial o realizar acciones que puedan desencadenar un ataque contra el sistema.

3.2 Objetivo del Ataque

En los entornos IIoT, los objetivos de los ataques pueden clasificarse en dos categorías principales: **Cyber Target (Objetivos Cibernéticos)** y **Physical Target (Objetivos Físicos)**. Cada uno de estos objetivos abarca componentes críticos dentro de la infraestructura industrial, cuya vulnerabilidad puede comprometer la seguridad, integridad y disponibilidad de los sistemas. A continuación, se detalla cada categoría:

Cibernéticos

Los objetivos cibernéticos incluyen componentes que forman parte de los sistemas de TI (Tecnología de la Información) y que son esenciales para la operación, gestión y comunicación en los entornos IIoT:

- **Operating System**: Los sistemas operativos en IIoT incluyen sistemas de propósito general y de propósito específico, como RTOS (Real Time Operating System) para dispositivos de baja latencia y sistemas basados en Windows o Linux utilizados en estaciones de trabajo y sistemas SCADA.

- **Network**: Las redes industriales son objetivos frecuentes debido a que muchos protocolos industriales carecen de mecanismos adecuados de autenticación y cifrado.
- **Localhost (Workstation)**: Las estaciones de trabajo pueden ser atacadas para engañar al operador, manipulando alarmas o induciendo acciones perjudiciales.
- **Websites (Web Server)**: Los servidores web se utilizan para alojar información sobre sistemas industriales y compartir datos con las partes interesadas, lo que los hace susceptibles a ataques.
- **Cloud**: La nube, que alberga aplicaciones y datos críticos de las plantas industriales, es un objetivo principal para atacar máquinas virtuales y comprometer la integridad de los datos.
- **Application**: Algunas aplicaciones industriales integradas en dispositivos se utilizan para configurar, probar y recopilar datos, siendo vulnerables a manipulaciones.
- **Mail Server**: Los servidores de correo en la DMZ pueden ser objetivos para obtener credenciales y enviar correos de phishing.

Físicos

Los objetivos físicos incluyen los dispositivos y componentes tangibles que son fundamentales para la operación de los sistemas industriales. Estos objetivos suelen estar expuestos a manipulaciones físicas y otras amenazas específicas:

- **Sensors**: Son esenciales para la monitorización en tiempo real de los procesos industriales.
- **Actuators**: Componentes responsables de convertir señales electrónicas en acciones físicas, como abrir válvulas o accionar motores.
- **Machines**: Equipos diseñados para realizar tareas específicas dentro de procesos industriales, como ensamblaje o transporte de materiales.
- **Manufactured Parts**: Los productos finales o piezas fabricadas pueden ser objetivos de ataques para introducir defectos o vulnerabilidades ocultas.
- **Human**: Los empleados pueden ser víctimas de ataques de ingeniería social, donde se les engaña para revelar información confidencial o realizar acciones perjudiciales.
- **Infrastructure**: Elementos como switches y controladores de energía son críticos para la operación industrial, siendo vulnerables a ataques como el envenenamiento de caché DNS para manipular el flujo de tráfico en la red.

3.3 Impacto del Ataque

El impacto de un ataque se define como el efecto o la consecuencia directa que provoca sobre el sistema comprometido. Los ataques en entornos IIoT pueden generar desde modificaciones no deseadas en el comportamiento de los sistemas hasta daños físicos significativos. Estos impactos se dividen en dos categorías principales: **Impacto Cibernético** e **Impacto Físico**. A continuación, se detallan los diferentes tipos de impacto dentro de cada categoría:

Cibernéticos

Los impactos cibernéticos afectan principalmente a los componentes digitales, alterando su funcionalidad, seguridad o disponibilidad. Estos incluyen:

- **Compromiso de Privilegios**: Bypass de las restricciones de privilegios que permite a usuarios o atacantes realizar tareas que pueden afectar el rendimiento o la disponibilidad del sistema.
- **Compromiso de Usuarios**: Acceso no autorizado a la cuenta de un usuario legítimo mediante el robo de credenciales o ataques de fuerza bruta.
- **Compromiso de Archivos**: Modificaciones maliciosas en archivos del sistema, ya sea mediante cambios directos o reempaquetado con certificados robados.
- **Compromiso de Sesiones**: Control de sesiones activas a través de ataques como CSRF o el robo de cookies de sesión.

- **Denegación de Servicio (DoS)**: Saturación de recursos del sistema, denegando el servicio a usuarios legítimos al consumir ancho de banda o capacidad de procesamiento.
- **Instalación de Malware**: Instalación de software malicioso, como troyanos de acceso remoto (RAT), para obtener control remoto sobre el sistema.
- **Bloqueo de Recursos**: Bloqueo de recursos críticos por procesos maliciosos, impidiendo su uso por parte de procesos legítimos.
- **Fuga de Información**: Exposición de datos confidenciales a través de ataques como Man-in-the-Middle (MitM), lo que puede causar pérdidas financieras significativas.

Físicos

Los impactos físicos afectan directamente a los componentes materiales del sistema, generando consecuencias que pueden comprometer la infraestructura o la seguridad industrial. Estos incluyen:

- **Compromiso de Hardware**: Malfuncionamiento de componentes de hardware, que puede provocar fallos en procesos críticos o daños materiales significativos.
- **Compromiso de Control de Acceso**: Violación de los mecanismos de control de acceso, permitiendo a atacantes manipular o desactivar dispositivos de manera no autorizada.
- **Compromiso de Proveedores**: Compromiso de la integridad del código fuente o de productos fabricados, lo que puede resultar en pérdida de propiedad intelectual o daños financieros para el proveedor.
- **Compromiso de la Confidencialidad**: Exposición de datos confidenciales, como credenciales o secretos comerciales, a través de canales de comunicación inseguros, comprometiendo la privacidad de la organización.

3.4 Consecuencias del Ataque

Las consecuencias de un ataque representan el resultado global que este genera tras su ejecución en un entorno IIoT. Estas consecuencias reflejan lo que el atacante logró tras comprometer el sistema y pueden variar desde la interrupción de servicios hasta daños físicos significativos. Según la taxonomía, las consecuencias de los ataques en IIoT se dividen en dos categorías principales: **Consecuencias Cibernéticas** y **Consecuencias Físicas**. A continuación, se detallan las subcategorías de cada una:

Cibernéticas

Las consecuencias cibernéticas son aquellas que afectan directamente los componentes digitales o virtuales del sistema industrial. Estas incluyen:

- **Robo de Propiedad Intelectual**: Robo de secretos comerciales y datos confidenciales que pueden ser utilizados por competidores para desarrollar estrategias comerciales o productos falsificados.
- **Fuga de Privacidad**: Exposición de información privada de clientes o personas involucradas en los procesos industriales, lo que puede dañar la reputación de la marca y causar grandes pérdidas económicas.
- **Fraude Financiero**: Uso de información financiera y registros de transacciones para cometer fraudes económicos.
- **Denegación de Servicio (DoS)**: Interrupción de servicios legítimos, que puede impedir a las partes interesadas acceder a datos o recursos necesarios.

Físicas

Las consecuencias físicas afectan directamente a los dispositivos, máquinas o infraestructura del entorno industrial, generando daños materiales o riesgos para las personas. Estas incluyen:

- **Producto Defectuoso**: Alteraciones maliciosas en herramientas de fabricación automatizada que conducen a la producción de productos defectuosos.
- **Manipulación de Máquinas**: Modificación del comportamiento de las máquinas sin el conocimiento de los operadores, como el uso de dispositivos IoT para actividades no autorizadas, como minería de criptomonedas.
- **Malfuncionamiento y Rotura**: Malfuncionamiento de dispositivos industriales que puede resultar en daños materiales, como ocurrió con el gusano Stuxnet, que destruyó centrifugadoras en instalaciones nucleares iraníes.
- **Pérdida de Disponibilidad del Sistema**: Ataques que provocan la pérdida de disponibilidad de sistemas o recursos, como el ataque cibernético a la planta de energía ucraniana que desconectó subestaciones durante tres horas.
- **Desastre Ambiental**: Fallos en sistemas de detección de fugas en plantas de petróleo y gas que pueden desencadenar desastres ambientales significativos.
- **Problemas de Salud**: Exposición a productos químicos, gases, radiaciones o malfuncionamientos de maquinaria que pueden poner en peligro la salud de las personas cercanas.

3.5 Vulnerabilidades en Protocolos

En este apartado se muestra a modo de resumen una tabla con las principales vulnerabilidades que presentan los protocolos mas ampliamente utilizados en IIoT mencionados en el apartado 2.3.

Table 1: Resumen de amenazas y vulnerabilidades en protocolos de comunicación

Protocolo	Amenazas/Vulnerabilidades
CAN	- Falta de autenticación [4] - Falta de cifrado - Ataques de denegación de servicio (DoS) - Inyección de datos maliciosos - Intercepción de comunicaciones (Eavesdropping) [4]
MQTT	- Autenticación y cifrado débiles - Oscuridad en el puerto - Ataques de denegación de servicio (DoS) [31] - Ataques Man-in-the-Middle (MITM) [32] - Ataques de fuerza bruta
CoAP	- Falta de autenticación y autorización [32] - Suplantación de identidad (IP spoofing) - Ataques Man-in-the-Middle (MITM) - Ataques de denegación de servicio (DoS)
DDS	- Cifrado y autorización deficientes - Ataques de denegación de servicio (DoS) - Ataques Man-in-the-Middle (MITM) [32]
AMQP	- Autenticación y cifrado deficientes - Ataques de denegación de servicio (DoS) [32] - Inyección de datos maliciosos - Ataques Man-in-the-Middle (MITM) - Secuestro de tráfico [31] - Ejecución remota de código
Fieldbus	- Cifrado y autenticación débiles [42] - Ataques de denegación de servicio (DoS) - Desbordamiento de búfer [31] - Inyección de comandos maliciosos - Ataques Man-in-the-Middle (MITM) - Intercepción de comunicaciones (Eavesdropping)
MODBUS/TCP	- Falta de autenticación, cifrado y control de acceso [36] - Falta de integridad de datos - Alteración de datos - Inyección de datos maliciosos - Ataques de denegación de servicio (DoS) - Ataques de repetición (Replay attack) - Ataques Man-in-the-Middle (MITM)
WirelessHART	- Autenticación y cifrado débiles [12] - Inyección de paquetes maliciosos - Ataques de denegación de servicio (DoS) - Ataques Man-in-the-Middle (MITM) - Ataques de interferencia (Jamming) - Suplantación de identidad y espionaje (Spoofing y Eavesdropping)
NB-IoT	- Inyección de paquetes maliciosos [31] - Desbordamiento de búfer - Ataques de denegación de servicio (DoS) [31] - Ataques de interferencia (Jamming) - Ataques de repetición (Replay)

4 Ataques

4.1 Fases de Ataque

A la hora de enfrentar los problemas de seguridad en un sistema es crucial comprender los patrones generales que suelen seguir los ataques a estos mismos, si lo que queremos es desarrollar herramientas verdaderamente capaces de hacerles frente. En el contexto de los ataques a infraestructuras de Internet de las Cosas Industrial (IIoT), los patrones de ataque suelen seguir una secuencia estructurada que puede variar ligeramente dependiendo del marco de referencia utilizado. Algunos de los marcos más conocidos son el Ciclo de Vida del Ataque de Lockheed Martin (CKC) [8], el Ciclo de Vida del Ataque de Mandiant (MALC) [30] y el marco ATT&CK de la MITRE Corporation [9]. Aunque estos marcos fueron originalmente diseñados para entornos de Tecnologías de la Información (IT), se han adaptado para abordar ataques en entornos de Sistemas de Control Industrial (ICS) y, en menor medida, en IIoT. Sin embargo, debido a la naturaleza híbrida de IIoT, que combina tanto tecnologías de Operaciones Tecnológicas (OT) como nuevas tecnologías de IT, es necesario adaptar estos marcos para capturar mejor la complejidad de los ataques en este tipo de infraestructuras [18].

- **Reconocimiento:** La fase de reconocimiento es el punto de partida de cualquier ataque. En esta fase, el atacante busca información sobre el objetivo, identifica vulnerabilidades y selecciona el método de ataque más adecuado. Las técnicas comunes incluyen el escaneo genérico para identificar puertos abiertos, sistema operativo y servicios disponibles en el objetivo utilizando herramientas como Nmap; el escaneo de vulnerabilidades para buscar vulnerabilidades conocidas y malas configuraciones en el sistema objetivo utilizando bases de datos como CVE; el fuzzing para enviar datos aleatorios o semiválidos a un sistema y detectar errores y excepciones; y el descubrimiento de recursos para identificar recursos disponibles en un sistema IIoT, como sensores y actuadores, mediante solicitudes específicas. Esta fase es crucial para el atacante, ya que proporciona la información necesaria para planificar el ataque. Detectar a tiempo actividades de reconocimiento puede ayudar a prevenir ataques incipientes.

- **Arma:** La fase de arma, también conocida como compromiso inicial, es donde el atacante obtiene acceso al sistema objetivo. Las técnicas comunes incluyen el ataque de fuerza bruta, que consiste en intentos repetidos de acceso utilizando combinaciones de nombre de usuario y contraseña; el ataque de diccionario, que utiliza listas de palabras para intentar adivinar contraseñas; y el insider malicioso, que es un empleado con acceso legítimo que actúa con intenciones maliciosas. Esta fase es crítica para el éxito del ataque.

- **Explotación:** En esta fase, el atacante explota una vulnerabilidad para obtener acceso más profundo al sistema. Las técnicas comunes incluyen el shell inverso, que crea una conexión inversa desde el sistema comprometido al sistema del atacante; y el ataque de hombre en el medio (MitM), que intercepta la comunicación entre dos puntos para inyectar datos maliciosos. La explotación puede ser rápida y difícil de detectar.

- **Movimiento Lateral:** El objetivo de esta fase es expandir el acceso dentro de la red y comprometer más sistemas. Las técnicas comunes incluyen la suscripción a broker MQTT para obtener información de dispositivos físicos; la lectura de registros Modbus para leer y descubrir registros en dispositivos PLC; y el ataque de retransmisión TCP, que utiliza técnicas de pivoteo para moverse entre segmentos de red. El movimiento lateral puede ser lento y discreto. La segmentación de la red y la monitorización de accesos internos pueden limitar la propagación del ataque.

- **Comando y Control (C&C):** Esta fase implica la creación de un canal de comunicación entre el sistema comprometido y el servidor del atacante para recibir comandos y enviar datos. Las técnicas comunes incluyen el uso de túnel DNS para establecer una comunicación discreta. El C&C es esencial para el control del ataque. La implementación de firewalls pueden interrumpir estos canales.

- **Exfiltración:** La exfiltración es el proceso de extraer información sensible del sistema comprometido. Las técnicas comunes incluyen la compresión y obfuscación de datos para evitar la detección durante la transferencia de datos. La exfiltración puede ser difícil de detectar. Encriptar los datos y monitorizar el tráfico saliente pueden ayudar a proteger la información.

- **Alteración:** Esta fase implica la manipulación de datos para afectar la integridad de la información. Las técnicas comunes incluyen la inyección de datos falsos en la nube para afectar análisis de datos y el envío de notificaciones falsas a operadores. La alteración puede tener consecuencias graves en la toma de decisiones.

- **Cripto-Ransomware:** En esta fase, el atacante inyecta malware para cifrar datos y exigir un rescate en criptomonedas. Las técnicas comunes incluyen el cifrado de archivos críticos hasta que se pague el rescate. El cripto-ransomware puede ser devastador. Crear copias de seguridad regulares pueden mitigar el impacto.

- **Denegación de Servicio Extorsivo (RDoS):** Esta fase implica amenazar con un ataque de denegación de servicio a menos que se pague un rescate.

4.2 Recopilacion Ataques

Para ilustrar todo lo expuesto anteriormente se va a elaborar una tabla con ataques reales que han afectado a infraestructura IIoT y clasificados en base a la taxonomia expuesta en el apartado anteriror.

Nombre	Vector	Objetivo	Impacto	Consecuencia
1. Stuxnet [11]	Cibernético (Malware)	*Machines / Actuators* (Controladores de centrifugadoras)	*Compromiso de Hardware* (Modificación de operaciones críticas)	*Malfuncionamiento y Rotura* (Daños físicos en centrifugadoras)
2. Troyano de Hardware [24]	Físico (Inserción de componentes maliciosos)	*Infrastructure / Machines* (Placa base de un dispositivo industrial)	*Compromiso de Hardware* (Dispositivo inseguro)	*Producto Defectuoso* (Fallos o puertas traseras)
3. Ataque DDoS a un SCADA [48]	Cibernético (DoS / DDoS)	*Network / SCADA*	*Denegación de Servicio* (Saturación de recursos)	*Pérdida de Disponibilidad* (Interrupción industrial)
4. Manipulación de Sensor [47]	Físico (Alteración directa)	*Sensors*	*Compromiso de Control de Acceso* (Acceso no autorizado)	*Producto Defectuoso* (Errores en la producción)
5. Ransomware en la Nube [25]	Cibernético (Malware)	*Cloud / Application*	*Instalación de Malware* (Cifrado de archivos)	*Denegación de Servicio* (Bloqueo de acceso a datos)
6. Desbordamiento de Búfer en un PLC [23]	Cibernético (Buffer Overflow)	*Actuators / Machines*	*Compromiso de Hardware* (Ejecución de código malicioso)	*Malfuncionamiento y Rotura* (Daños físicos)
7. Jamming de Señales	Físico (Jamming)	*Infrastructure (Antenas, APs)*	*Bloqueo de Recursos* (Red inalámbrica inutilizada)	*Pérdida de Disponibilidad* (Interrupción de comunicaciones)
8. Dispositivo USB Infectado	Físico (Interacción directa)	*Localhost (Workstation)*	*Instalación de Malware* (Troyano o keylogger)	*Fuga de Privacidad* (Exfiltración de datos)
9. Tailgating (Ingeniería Social)	Físico (Acceso físico no autorizado)	*Human / Infrastructure*	*Compromiso de Control de Acceso* (Ingreso sin permisos)	*Robo de Información* (Acceso a red interna)
10. Reempaquetado de Aplicaciones IIoT [23]	Cibernético (Repackaging)	*Application / OS*	*Instalación de Malware* (Código espía embebido)	*Fuga de Privacidad* (Exfiltración de datos)
11. Secuestro de Sesión Web SCADA [2]	Cibernético (Session Hijacking)	*Web Server*	*Compromiso de Sesiones* (Control de sesión de operador)	*Denegación de Servicio* (Cierre de procesos)
12. CSRF en Gestión IIoT [25]	Cibernético (CSRF)	*Websites / Application*	*Compromiso de Sesiones* (Acciones no autorizadas)	*Fraude Financiero* (Manipulación de parámetros)
13. Alteración de Firmware en IIoT [5]	Físico (Troyanos de Hardware)	*Sensors / Actuators*	*Compromiso de Hardware* (Modificación de firmware)	*Producto Defectuoso* (Resultados alterados)
14. Race Condition en OS Embebido [23]	Cibernético (Race Condition)	*Operating System*	*Compromiso de Archivos* (Corrupción de archivos)	*Denegación de Servicio* (Fallo masivo del sistema)

Continuará en la siguiente página

Table 2 – continuación de la página anterior

Nombre	Vector	Objetivo	Impacto	Consecuencia
15. Robo de Credenciales con *Shoulder Surfing* [40]	Físico (Robo de Credenciales de Acceso)	*Physical Target: Human*	*Compromiso de Usuarios* (Acceso posterior a la red con credenciales legítimas)	*Fraude Financiero / Fuga de Privacidad* (Uso indebido de cuentas con privilegios)
16. Falsificación de Certificados de Software IIoT [22]	Cibernético (Spoofing)	*Cyber Target: Application / Operating System*	*Compromiso de Archivos* (Ejecutables maliciosos parecen legítimos)	*Robo de Propiedad Intelectual o Fuga de Privacidad* (Distribución de software comprometido que filtra datos)
17. Ataque de Cadena de Suministro (SolarWinds-style en IIoT) [38]	Cibernético (Reempaquetado/Malware)	*Application/Cloud* (Actualizaciones de software legítimas comprometidas)	*Compromiso de Archivos* (Inserción de código malicioso en actualizaciones)	*Robo de Propiedad Intelectual* (Acceso a diseños industriales o datos sensibles)
18. Envenenamiento de Modelos de ML/AI [13]	Cibernético (Inyección de Código)	*Application* (Sistemas de mantenimiento predictivo basados en IA)	*Compromiso de Archivos* (Alteración de conjuntos de datos de entrenamiento)	*Producto Defectuoso* (Decisiones erróneas en líneas de producción)
19. Ataque de Canal Lateral (Side-Channel) [15]	Físico (Escuchas Clandestinas)	*Sensors/Actuators* (Dispositivos con emisiones electromagnéticas no protegidas)	*Fuga de Información* (Extracción de claves criptográficas mediante análisis de energía)	*Robo de Propiedad Intelectual* (Acceso a algoritmos propietarios de control)
20. Explotación de Firmware no Parcheado (Ej. VxWorks) [43]	Cibernético (Buffer Overflow)	*Operating System* (RTOS en dispositivos edge como PLCs)	*Compromiso de Privilegios* (Ejecución remota de código)	*Manipulación de Máquinas* (Parálisis de líneas de ensamblaje)
21. DNS Spoofing en Redes OT [14]	Cibernético (Spoofing)	*Network* (Servidores DNS internos en redes industriales)	*Fuga de Información* (Redirección de tráfico a servidores maliciosos)	*Robo de Propiedad Intelectual* (Interceptación de datos de procesos industriales)
22. Cryptojacking en Dispositivos Edge [37]	Cibernético (Malware)	*Machines* (Gateways IIoT con capacidad de procesamiento)	*Bloqueo de Recursos* (Consumo de CPU para minería de criptomonedas)	*Pérdida de Disponibilidad* (Retrasos críticos en tiempo real en líneas de producción)
23. Ataque de Falsa Inyección de Datos (False Data Injection) [19]	Cibernético (Spoofing)	*Sensors* (Sensores de temperatura/presión en oleoductos)	*Compromiso de Archivos* (Manipulación de lecturas enviadas al SCADA)	*Desastre Ambiental* (Sobrepresión no detectada en tuberías, causando fugas)
24. Ataque de Agotamiento de Batería (Battery Drain) [21]	Físico (Jamming de Señales)	*Infrastructure* (Dispositivos IIoT inalámbricos con batería limitada)	*Bloqueo de Recursos* (Interrupción de comunicaciones por agotamiento energético)	*Pérdida de Disponibilidad* (Caída de redes de sensores en plantas remotas)
25. Exploit de Protocolos Legacy (Ej. Modbus) [5]	Cibernético (Inyección de Código)	*Network* (Protocolos sin autenticación como Modbus TCP)	*Compromiso de Control de Acceso* (Comandos no autorizados a PLCs)	*Malfuncionamiento y Rotura* (Parada abrupta de motores industriales)

Continuará en la siguiente página

Table 2 – continuación de la página anterior

Nombre	Vector	Objetivo	Impacto	Consecuencia
26. Ataque a Sistemas de Edge Computing [16]	Cibernético (Race Condition)	*Cloud/Edge Nodes* (Nodos de procesamiento local en fábricas)	*Compromiso de Archivos* (Corrupción de datos en tiempo real)	*Producto Defectuoso* (Errores en inspecciones visuales automatizadas)

Cada uno de estos ataques ilustra cómo se pueden combinar diferentes tipos de vectores (cibernéticos o físicos) con objetivos tanto cibernéticos (p.ej. sistemas operativos, redes, servidores de aplicaciones) como físicos (sensores, actuadores, máquinas), generando impactos que abarcan desde la simple alteración de archivos o sesiones hasta la destrucción de hardware industrial o la producción de bienes defectuosos, con consecuencias igualmente diversas (desde el robo de información confidencial hasta daños materiales y riesgos para la salud y el medioambiente).

5 Contramedidas de Seguridad

Los desafíos de ciberseguridad en el entorno industrial (IIoT) son significativamente diferentes y más complejos en comparación con los del IoT orientado al consumidor. Mientras que en el IoT convencional los dispositivos suelen conectarse directamente a Internet para proporcionar o ejecutar sus funciones, en el IIoT existe una fuerte interconexión entre dispositivos de campo, controladores y servidores centralizados, donde una gran parte del procesamiento de datos ocurre dentro de redes locales.

La conexión a Internet y los servicios en la nube en el entorno IIoT se utiliza principalmente para mejorar las capacidades de procesamiento local mediante la monitorización avanzada y la optimización de procesos. En este contexto, los requisitos de seguridad más críticos en el IIoT son la disponibilidad y la integridad, aspectos que marcan una clara diferencia con otros dominios.

Además, el modelo de atacante en el ámbito del IIoT es un componente vital para clasificar y determinar las amenazas y riesgos asociados. Dado el entorno único del IIoT, caracterizado por procesos críticos, componentes operativos de larga duración, altas demandas de conectividad, un gran número de dispositivos, confidencialidad de datos, errores humanos y posibles sabotajes , se requieren soluciones robustas y específicas para mitigar las amenazas cibernéticas y sus vulnerabilidades asociadas.

A continuación, se presentan las principales contramedidas de seguridad propuestas para abordar estos desafíos en el ámbito del IIoT.

5.1 IDS para IIoT

Los Sistemas de Detección de Intrusos (IDS) son esenciales para detectar tráfico malicioso en entornos IIoT, actuando como una capa de defensa secundaria más allá de los firewalls tradicionales. Las soluciones IDS suelen dividirse en dos categorías: basadas en firmas (coincidencia de patrones contra amenazas conocidas) y basadas en anomalías (detección de desviaciones del comportamiento normal). Los enfoques híbridos que combinan ambos métodos son cada vez más populares debido a su capacidad para identificar tanto ataques conocidos como desconocidos.

Por ejemplo, en [27] se propuso un IDS híbrido liviano que utiliza nodos basados en agentes, aprovechando metadatos del sistema y parámetros de contexto para monitorear las pasarelas IIoT. Sin embargo, este enfoque puede volverse computacionalmente costoso. De manera similar, en [46] se introdujo un IDS híbrido basado en aprendizaje automático (ML) para IIoT en el borde de la red, utilizando gradient boosting para los nodos de borde y aprendizaje profundo para los nodos maestros. Aunque es eficaz para dispositivos con recursos limitados, presenta limitaciones con conjuntos de datos pequeños. Finalmente, en [33] se presentó un IDS basado en inspección profunda de paquetes para detectar vulnerabilidades en Modbus/TCP; no obstante, su enfoque en un solo protocolo limita su aplicabilidad general.

5.2 Aprendizaje Automático

Las técnicas de Aprendizaje Automático (ML) son fundamentales para la detección de ataques en entornos IIoT debido a la naturaleza dinámica de estos sistemas y las limitaciones de los IDS tradicionales. Métodos convencionales, como los IDS basados en firmas o reglas, tienen dificultades para adaptarse a amenazas emergentes y cambios en el sistema. En cambio, los IDS basados en ML pueden identificar patrones complejos de anomalías y adaptarse a intrusiones desconocidas.

Por ejemplo, en [1] se introdujo un modelo de aprendizaje profundo llamado Deep-IFS, que combinó unidades recurrentes cerradas y capas de atención múltiple para detectar intrusiones en entornos de computación en la niebla, demostrando un rendimiento superior en los conjuntos de datos BotIoT y UNSW-NB15. Estos enfoques destacan el potencial del ML para mejorar la precisión de detección y la escalabilidad en entornos IIoT con recursos limitados.

Sin embargo, persisten desafíos, como la dependencia de grandes conjuntos de datos etiquetados y el costo computacional. Por ejemplo, en [28] se propuso un marco basado en optimización de enjambre de partículas para ajustar hiperparámetros de redes neuronales profundas, alcanzando una precisión del 99.90% en Bot-IoT pero requiriendo recursos computacionales significativos. Otro estudio en [28] desarrolló un sistema de detección de anomalías utilizando autoencoders y análisis de componentes principales, el cual enfrentó limitaciones en el manejo de relaciones no lineales entre características. Estos ejemplos subrayan la necesidad de modelos de ML ligeros y adaptativos diseñados para las restricciones del IIoT.

Los enfoques híbridos, como la combinación de ML con inspección profunda de paquetes (DPI), muestran potencial para abordar vulnerabilidades específicas de protocolos. Por ejemplo, en [33] se propuso un IDS con DPI habilitado para Modbus/TCP, aunque su aplicabilidad se limitó a un solo protocolo. Trabajos futuros deberían centrarse en desarrollar marcos de ML robustos y multimodales que integren datos de sensores y protocolos diversos para garantizar una detección integral de amenazas en entornos IIoT.

Dataset	CNSC	HDS						RNT	DAT	DDD	FS	IIoT-CP			RA	AF	IIoT-T	LD	MD	PA
		NT	HR	L	PP	AL	CC					MQTT	CoAP	WS						
KDD CUP 99 [13]	YES	YES	NO	YES	NO	NO	YES	NO	YES	N/A	YES	NO	NO	NO	NO	YES	NO	YES	NO	YES
CAIDA [15]	YES	YES	NO	NO	NO	NO	NO	YES	NO	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
NSL-KDD [14]	YES	YES	NO	YES	NO	NO	YES	NO	YES	N/A	YES	NO	NO	NO	NO	YES	NO	YES	NO	YES
ISCX [18]	YES	YES	NO	NO	NO	NO	YES	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO	YES	YES	YES
Morris et al. [26]	YES	YES	NO	NO	YES	NO	YES	YES	YES	YES	YES	NO	NO	NO	NO	NO	NO	YES	YES	YES
UNSW-NB15 [16]	YES	YES	NO	NO	NO	NO	NO	NO	YES	NO	YES	NO	NO	NO	NO	NO	NO	YES	YES	YES
TUIDS [25]	YES	YES	NO	NO	NO	NO	YES	YES	NO	YES	YES	NO	NO	NO	NO	YES	NO	YES	YES	NO
Pan et al [27]	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES	NO	NO	NO	NO	NO	NO	YES	YES	YES
SWaT [28]	YES	YES	NO	YES	NO	NO	NO	YES	YES	NO	YES	NO	NO	NO	NO	NO	NO	YES	YES	NO
NGIDS-DS [24]	YES	YES	NO	YES	NO	NO	NO	NO	YES	NO	YES	NO	NO	NO	NO	NO	NO	YES	YES	YES
Rodofile et al [29]	YES	YES	NO	NO	NO	NO	YES	YES	YES	N/A	NO	NO	NO	NO	NO	NO	NO	NO	YES	NO
Myers et al [30]	YES	YES	NO	YES	NO	NO	YES	YES	N/A	NO	NO	NO	NO	NO	NO	NO	NO	NO	YES	NO
CICIDS [17]	YES	YES	YES	NO	NO	NO	YES	YES	YES	NO	YES	NO	NO	NO	NO	NO	NO	YES	YES	NO
N-BaIoT [19]	NO	YES	NO	NO	NO	NO	YES	YES	NO	YES	YES	NO	NO	NO	YES	YES	NO	YES	YES	YES
Bezerra et al [22]	NO	YES	YES	NO	NO	NO	NO	YES	NO	NO	YES	NO	NO	NO	YES	YES	NO	YES	YES	NO
BoT-IoT [21]	NO	YES	NO	NO	NO	NO	YES	NO	NO	N/A	YES	YES	NO	NO	YES	YES	NO	YES	YES	YES
Kang et al [20]	NO	YES	NO	NO	NO	NO	YES	NO	NO	N/A	NO	NO	NO	NO	YES	NO	NO	NO	NO	NO
Al-Hadhrami and Hussian [12]	NO	YES	NO	NO	NO	NO	YES	NO	NO	NO	YES	NO	NO	NO	NO	NO	NO	YES	YES	YES
X-IIoTID	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES

CNSC: Complete Network and System Configuration — **NT:** Network Traffic — **L:** Logs — **AL:** Alerts — **RNT:** Realistic Network Traffic
DDD: Diverse Data Duration — **IIoT-CP:** IIoT Connectivity Protocols — **AF:** Agnostic-Features — **LD:** Labeled Dataset — **PA:** Public Availability
HDS: Heterogeneous Data Sources — **HR:** Host Resources — **PP:** Physical Process — **CC:** Complete Capture — **MD:** Metadata
DAT: Divers Attacks Scenario and Types — **FS:** Feature Set — **RA:** Recent Attacks — **IIoT-T:** IIoT Traces

Figure 8: Tabla de comparación de datasets de intrusiones en IIoT [34].

5.3 Protección de redes SCADA

Las redes SCADA (*Supervisory Control and Data Acquisition*) son esenciales para controlar y monitorear procesos industriales, pero su arquitectura tradicional las hace vulnerables a ciberataques. Una red SCADA típica incluye una red de control (con RTUs, PLCs y sensores), una infraestructura de comunicación (como *fieldbus* o Modbus) y una red de procesos (con servidores y HMI). Cada componente expone riesgos: la infraestructura de comunicación puede sufrir ataques DoS o *jamming*, mientras que las redes inalámbricas de sensores enfrentan amenazas como inyección de datos falsos o replicación de nodos.

Para proteger estas redes, se han desarrollado soluciones como *middlewares* resistentes, sistemas de detección de intrusiones (IDS) y técnicas de *machine learning* (ML). Un ejemplo es el IDS basado en ML propuesto en [49], que utiliza

algoritmos como *random forest* para detectar comportamientos anormales y alertar a los operadores a través de una interfaz gráfica. Otra aproximación es el modelo de detección de ataques basado en aprendizaje *ensemble* (como *random subspace-random tree*) presentado en [17], que combina múltiples clasificadores para mejorar la precisión y reducir el sobreajuste. Estos sistemas permiten identificar amenazas sin comprometer el rendimiento de la red.

Además, se han propuesto *middlewares* basados en multiagentes para monitorear y coordinar la comunicación entre componentes, como el *framework* resiliente en [20]. Estos sistemas adaptativos ayudan a mitigar amenazas mediante mecanismos de resiliencia y conciencia contextual. En resumen, la seguridad de las redes SCADA requiere soluciones integradas que combinen ML, IDS y arquitecturas flexibles para enfrentar amenazas en tiempo real.

5.4 Otras

Las tecnologías emergentes, como el cifrado adaptativo y los contratos inteligentes, son cruciales para proteger datos en entornos heterogéneos, como se discute en [39], donde se proponen soluciones como re-cifrado y cifrado parcial para garantizar confidencialidad de extremo a extremo.El blockchain emerge como una solución para asegurar la integridad y trazabilidad en IIoT. En [29], se presenta un marco blockchain-edge que aborda amenazas en capas locales (sensores), de borde (procesamiento) y globales (almacenamiento en la nube).

En la capa local, se mitigan ataques como inyección de datos mediante firmas criptográficas. En la capa de borde, se abordan amenazas de virtualización mediante aislamiento de políticas de seguridad. En la capa global, se enfrentan ataques API y DoS/DDoS con cifrado homomorfo y encriptación basada en atributos. Finalmente, en la capa de ledger, se protege contra ataques Sybil y de claves privadas mediante cadenas híbridas y cierre de código. Estos enfoques integran blockchain y cifrado para fortalecer la seguridad en todo el ecosistema IIoT.

References

[1] M. Abdel-Basset et al. "DeepIFS: Intrusion detection approach for industrial internet of things traffic in fog environment". In: *IEEE Transactions on Industrial Informatics* 17.11 (2020), pp. 7704–7715.

[2] KeepCoding Bootcamps. *¿Qué es el secuestro de sesión? [2025]*. 2021. URL: https://keepcoding.io/blog/que-es-el-secuestro-de-sesion/.

[3] H. Boyes et al. "The Industrial Internet of Things (IIoT): An analysis framework". In: *Computers in Industry* 101 (2018). Disponible en: https://doi.org/10.1016/j.compind.2018.04.015, pp. 1–12.

[4] M. Bozdal et al. "Evaluation of CAN bus security challenges". In: *Sensors* 20.8 (2020). Disponible en: https://doi.org/10.3390/s20082364, p. 2364.

[5] S. Chaudhary and P. K. Mishra. "DDoS attacks in Industrial IoT: A survey". In: *Computer Networks* 236 (2023), p. 110015. DOI: 10.1016/j.comnet.2023.110015.

[6] Industrial Internet Consortium. *Industrial Internet Consortium*. Disponible en: https://www.iiconsortium.org/. 2023.

[7] Industrial Internet Consortium. *The Industrial Internet Reference Architecture (IIRA)*. Disponible en: https://www.iiconsortium.org/IIRA.htm. 2023.

[8] Lockheed Martin Corporation. *Cyber Kill Chain®*. Disponible en: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. 2025.

[9] MITRE Corporation. *MITRE ATT&CK® Framework*. Disponible en: https://attack.mitre.org/. 2025.

[10] Manuel Andrés Ramírez Delgado and Flor Nancy Díaz-Piraquive. "Análisis a la utilización de protocolos de interconexión para internet de las cosas: Una revisión sistemática". In: *Universidad Católica de Colombia* (2020). Disponible en: https://www.ucatolica.edu.co/.

[11] D. D. Denning. "Stuxnet: What Has Changed?" In: *Future Internet* (2012). DOI: 10.3390/fi4040681.

[12] P.A.M. Devan et al. "A survey on the application of WirelessHART for industrial process monitoring and control". In: *Sensors* 21.15 (2021). Disponible en: https://doi.org/10.3390/s21154951, p. 4951.

[13] D. Dunn, N. Moustafa, and B. Turnbull. "Robustness evaluations of sustainable machine learning models against data poisoning attacks in the internet of things". In: *Sustainability* 12.16 (2020), p. 6434. DOI: 10.3390/su12166434.

[14] E. M. de Elias et al. "A hybrid CNN-LSTM model for IIoT edge privacy-aware intrusion detection". In: *2022 IEEE Latin-American Conference on Communications (LATINCOM)*. IEEE, 2022. DOI: 10.1109/LATINCOM55665.2022.9964214.

[15] M. A. Ferrag et al. "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning". In: *IEEE Access* 10 (2022), pp. 40281–40306. DOI: 10.1109/ACCESS.2022.3179871.

[16] M. A. Ferrag et al. "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning". In: *IEEE Access* 10 (2022), pp. 40281–40306. DOI: 10.1109/ACCESS.2022.3179871.

[17] M. M. Hassan et al. "Increasing the trustworthiness in the industrial IoT networks through a reliable cyberattack detection model". In: *IEEE Transactions on Industrial Informatics* 16.9 (2020), pp. 6154–6162.

[18] Muna Al-Hawawreh, Elena Sitnikova, and Neda Aboutorab. "X-IIoTID: A Connectivity- and Device-agnostic Intrusion Dataset for Industrial Internet of Things". In: *IEEE Internet of Things Journal* (2021).

[19] Y. Himeur et al. "Federated learning for computer vision". In: *arXiv preprint* (2023). DOI: 2308.13558.

[20] F. Januário et al. "Security challenges in SCADA systems over wireless sensor and actuator networks". In: *2016 8th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. IEEE, 2016, pp. 363–368.

[21] D. Javeed et al. "An intrusion detection system for edge-envisioned smart agriculture in extreme environment". In: *IEEE Internet of Things Journal* (2023). DOI: 10.1109/JIOT.2023.3279314.

[22] Keyfactor. *Establecimiento de la confianza en entornos IoT, IIoT y OT*. 2024. URL: https://www.keyfactor.com/es/blog/establishing-trust-in-iot-iiot-and-ot-environments/.

[23] A. A. Al-Khalifa and M. A. Al-Khalifa. "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions". In: *Electronics* (2023). DOI: 10.3390/electronics12061333.

[24] A. A. Al-Khalifa and M. A. Al-Khalifa. "Trojan Horses: A Review". In: *2nd International Workshop on Materials Engineering and Computer Sciences (IWMECS 2015)*. Atlantis Press, 2015. DOI: 10.2991/iwmecs-15.2015.33.

[25] A. S. Al-Khalifa and A. A. Al-Khalifa. "Artificial Intelligence-Based Malware Detection, Analysis, and Mitigation". In: *Mathematics* (2022). DOI: 10.3390/math10151461.

[26] H. Khujamatov et al. "IoT, IIoT, and cyber-physical systems integration". In: *Advances in Green Synthesis*. 2021, pp. 31–50. DOI: 10.1007/978-3-030-66222-6_3.

[27] J. Kirupakar and S. M. Shalinie. "Situation aware intrusion detection system design for industrial IoT gateways". In: *2019 International Conference on Computational Intelligence in Data Science (ICCIDS)*. IEEE, 2019, pp. 1–6.

[28] N. Koroniotis, N. Moustafa, and E. Sitnikova. "A new network forensic framework based on deep learning for internet of things networks: A particle deep framework". In: *Future Generation Computer Systems* 110 (2020), pp. 91–106.

[29] T. Kumar et al. "SECBlockEdge: Security threats in blockchain-edge based industrial IoT networks". In: *2019 11th International Workshop on Resilient Networks Design and Modeling (RNDM)*. IEEE, 2019, pp. 1–7.

[30] Mandiant. *Soluciones de defensa cibernética de Mandiant*. Disponible en: https://cloud.google.com/security/mandiant?hl=es-419. 2025.

[31] Sri Harsha Mekala et al. "Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions". In: *Review* (2025). Disponible en: [https://www.sciencedirect.com/science/article/pii/S0140366423002189].

[32] G. Nebbione and M.C. Calzarossa. "Security of IoT application layer protocols: Challenges and findings". In: *Future Internet* 12.3 (2020). Disponible en: https://doi.org/10.3390/fi12030055, p. 55.

[33] O. N. Nyasore et al. "Deep packet inspection in industrial automation control system to mitigate attacks exploiting modbus/TCP vulnerabilities". In: *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*. IEEE, 2020, pp. 241–245.

[34] Abhijeet C. Panchal, Vijay M. Khadse, and Parikshit N. Mahalle. "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures". In: *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*. IEEE. Pune, India, 2018.

[35] T. Qiu et al. "Edge computing in industrial internet of things: Architecture, advances and challenges". In: *IEEE Communications Surveys & Tutorials* 22.4 (2020). Disponible en: https://doi.org/10.1109/COMST.2020.3009103, pp. 2462–2488.

[36] A. Rahman et al. "Launch of denial of service attacks on the MODBUS/TCP protocol and development of its protection mechanisms". In: *International Journal of Critical Infrastructure Protection* 39 (2022). Disponible en: https://doi.org/10.1016/j.ijcip.2022.100568, p. 100568.

[37] R. Saadouni et al. "Secure IIoT networks with hybrid CNN-GRU model using edge-IIoTset". In: *2023 15th International Conference on Innovations in Information Technology (IIT)*. IEEE, 2023. DOI: 10.1109/IIT57066.2023.10229924.

[38] A. Sánchez-Zumba and D. Avila-Pesantez. "Cybersecurity for Industrial IoT, Threats, Vulnerabilities, and Solutions: A Brief Review". In: *Proceedings of Eighth International Congress on Information and Communication Technology (ICICT 2023)*. Springer, Singapore, 2023. DOI: 10.1007/978-981-99-3243-6_90.

[39] M. Serror et al. "Challenges and opportunities in securing the industrial internet of things". In: *IEEE Transactions on Industrial Informatics* 17.5 (2020), pp. 2985–2996.

[40] La Sexta. *Shoulder Surfing: Mucho cuidado, podrías caer en este ataque cibernético*. 2022. URL: https://www.lasexta.com/tecnologia-tecnoxplora/internet/shoulder-surfing-mucho-cuidado-podrias-caer-ataque-cibernetico_202202236216372fcfdb0c0001f267f4.html.

[41] K. Stouffer, J. Falco, and K. Scarfone et al. *Guide to industrial control systems (ICS) security*. Tech. rep. 82. NIST Special Publication, 2011, p. 16.

[42] J.-P. Thomesse. "Fieldbus technology in industrial automation". In: *Proceedings of the IEEE* 93.6 (2005). Disponible en: https://doi.org/10.1109/JPROC.2005.849724, pp. 1073–1101.

[43] S. Ullah et al. "MAGRU-IDS: A multi-head attention-based gated recurrent unit for intrusion detection in IIoT networks". In: *IEEE Access* (2023). DOI: 10.1109/ACCESS.2023.3277812.

[44] H. Xu et al. "A survey on industrial internet of things: A cyber-physical systems perspective". In: *IEEE Access* 6 (2018), pp. 78238–78259.

[45] G. Yadav and K. Paul. "Architecture and security of SCADA systems: A review". In: *International Journal of Critical Infrastructure Protection* 34 (2021), p. 100433. DOI: 10.1016/j.ijcip.2021.100433.

[46] H. Yao et al. "Hybrid intrusion detection system for edge-based IIoT relying on machine-learning-aided detection". In: *IEEE Network* 33.5 (2019), pp. 75–81.

[47] Y. Zhang et al. "Sensor Attack Detection Based on Active Excitation Response with Uncertain Delays". In: *Journal of Systems Architecture* (2024). DOI: 10.1016/j.sysarc.2024.05.004.

[48] T. Zhukabayeva et al. "Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions". In: *Sensors* (2024). DOI: 10.3390/s25010213.

[49] M. Zolanvari et al. "Machine learning-based network vulnerability analysis of industrial internet of things". In: *IEEE Internet of Things Journal* 6.4 (2019), pp. 6822–6834. DOI: 10.1109/JIOT.2019.2912022.