Universidad de Alcalá
Escuela Politécnica Superior

Máster Universitario en Ingeniería Industrial

Trabajo Fin de Máster

Ciberseguridad en Smart Grids: Estudio y Aplicación Real sobre una Microrred Inteligente

Autor: Pablo José Hueros Barrios

Tutor/es: Francisco Javier Rodríguez Sánchez

Julio de 2021

Escuela Politécnica Superior

Máster Universitario en Ingeniería Industrial

Trabajo Fin de Máster

Ciberseguridad en Smart Grids: Estudio y Aplicación Real sobre una Microrred Inteligente

Pablo José Hueros Barrios

Alcalá de Henares, Julio 2021

UNIVERSIDAD DE ALCALÁ

Escuela Politécnica Superior

Máster Universitario en Ingeniería Industrial

Trabajo Fin de Máster

Ciberseguridad en Smart Grids: Estudio y Aplicación Real sobre una Microrred Inteligente

Autor: Pablo José Hueros Barrios

Tutor: Francisco Javier Rodríguez Sánchez

TRIBUNAL:

Presidente: Emilio José Bueno Peña.

Vocal 1º: Iván Marsá Maestre.

Vocal 2º: Francisco Javier Rodríguez Sánchez.

FECHA: Julio, 2021.

Resumen

Las redes eléctricas inteligentes o *Smart Grids* se implantan, cada vez con más frecuencia, en el sistema de distribución eléctrica. Y es que, a medida que el cambio climático se agudiza, el mundo se está viendo obligado a realizar cambios en el modelo convencional de generación, gestión y consumo de energía.

Aunque son muchos los beneficios asociados a las *Smart Grids*, dicha evolución implica serios riesgos de ciberseguridad en tanto que el número de dispositivos conectados aumenta.

El presente documento pretende constituir un acercamiento a la materia para los profesionales del sector eléctrico que estén dando sus primeros pasos en el mundo de la ciberseguridad aplicada a las Smart Grids, ofreciendo un modelo a seguir para la identificación de activos, la evaluación de amenazas, la cuantificación de riesgos y la implementación de mecanismos de protección.

Con el fin de resaltar la gravedad de los ciberataques en este campo, se realizará una breve demostración de la facilidad con la que es posible penetrar en las comunicaciones de un sistema inteligente de gestión de una microrred eléctrica que no tenga como lema el diseño por seguridad y la seguridad mediante confianza cero.

Palabras clave: Smart Grids, ciberseguridad, IoT, ciberataque, evaluación de riesgos, evaluación de amenazas, MQTT, microrred.

Abstract

Smart grids are increasingly being implemented in the electric distribution system. As climate change worsens, the world is being forced to make changes to the conventional model of energy generation, management and consumption.

While there are many benefits associated with *Smart Grids*, this evolution entails serious cybersecurity risks as the number of connected devices increases.

This document aims to provide an approach to the subject for professionals in the electric sector who are taking their first steps in the world of cybersecurity applied to Smart Grids, offering a model to follow for asset identification, threat assessment, risk quantification and implementation of protection mechanisms.

In order to highlight the seriousness of cyber-attacks in this field, a brief demonstration will be given of the ease with which it is possible to penetrate the communications of a microgrid management system that does not have security design and zero trust security as its motto.

Keywords: Smart Grids, cybersecurity, IoT, cyberattack, risk assessment, threat assessment, MQTT, microgrid.

Índice general

Índice de Figuras

Índice de Tablas

Lista de acrónimos

AMI: Advanced Metering Infraestructure.

CA: Autoridad Certificadora.

CEN: European Committee for Standardization.

CENELEC: European Committee for Electrotechnical Standardization.

DER: Distribution Energy Resources.

DGM: Distribution Grid Management.

DMS: Distribution Management System.

DoS: Denial of Service.

DR: Demand Response.

DRAS: Demand Response Automation Server.

EMS: Energy Management System.

EPS: Escuela Politécnica Superior.

ETSI: European Telecommunications Standards Institute.

EV: Electric Vehicle.

EVSE: Electric Vehicle Supply Equipment.

FDI: False Data Injection.

HAN: Home Area Network.

HMI: Human Machine Interface.

IDS: Intrusion Detection System.

IoT: Internet of Things.

IPS: Intrusion Protection System.

MiTM: Man in The Middle.

MQTT: Message Queue Telemetry Transport.

NESCOR: National Electric Sector Cybersecurity Organization Resource.

OCCP: Open Charge Point Protocol.

OpenADR: Open Automated Demand Response.

PMU: Phasor Measurement Unit.

RBAC: Role-Based Access Control.

ROS: Robot Operating System.

SCADA: Supervisory Control And Data Acquisition.

TICs: Tecnologías de la información y de la comunicación.

WAMPAC: Wide Area Monitoring, Protection and Control.

QoS: Quality of Service.

RSA: Rivest Shamir Adleman.

TLS: Transport Layer Security.

PKI: Public Key Infraestructure.

VPP: Virtual Power Plant.

Capítulo 1

Introducción

La electricidad es muy importante en nuestro día a día ya que permite el uso de numerosos aparatos electrónicos que se encuentran en viviendas, oficinas, industrias y un largo etcétera de lugares.

Hay países en desarrollo que no tienen la habilidad de generar y proveer de energía eléctrica de un modo continuo a sus ciudades para su actividad diaria debido a un uso y gestión deficiente de los recursos energéticos disponibles.

Para, entre otros aspectos, integrar diversas fuentes de generación distribuida que permitan paliar este problema, la red eléctrica tradicional ha experimentado una evolución tecnológica utilizando los servicios ofrecidos por las tecnologías de la información y comunicación (TICs), dando paso, por tanto, a las *Smart Grids*.

Las *Smart Grids* necesitan de la infraestructura necesaria para permitir la interacción bidireccional en tiempo real entre los consumidores y las empresas de servicios públicos, consiguiendo, a su vez, una electricidad más eficiente, fiable y segura.

Aunque las *Smart Grids* ofrecen mejoras notables frente a la red eléctrica convencional, también generan serios retos de ciberseguridad al introducir elementos de comunicación como redes de sensores inalámbricos y otros dispositivos industriales. Ejemplo de ello fue el apagón que sufrió una región al suroeste de Ucrania a finales de 2015 debido a un ciberataque coordinado que afectó a tres de las principales compañías energéticas de la región.

Por ende, resulta necesario introducir soluciones para evitar la interrupción del funcionamiento de alguno de los componentes anteriormente mencionados, impidiendo así daños a una escala mayor.

Un sistema de detección de intrusiones (IDS) o prevención de intrusiones (IPS) puede informar o realizar una contramedida si un ciberataque lograse eludir los mecanismos de encriptación y autorización. Con el fin de integrar correctamente estos recursos, es necesario realizar un estudio de los ciberataques que son plausibles en la comunicación de las *Smart Grids*.

Un caso particular de *Smart Grids* son las microrredes eléctricas, las cuales está previsto que se desplieguen de manera intensa en un futuro próximo gracias a las soluciones de autoconsumo

energético (solar, principalmente) y de almacenamiento de energía, que han alcanzado costes competitivos.

Este proyecto se centrará en analizar los problemas de ciberseguridad en el ámbito de estas microrredes, primero desde un punto de vista general y, posteriormente, particularizando la metodología de análisis a un caso real existente en la Escuela Politécnica Superior (EPS) de la Universidad de Alcalá.

1.1. Contexto del trabajo

Este TFM se encuentra estrechamente vinculado al proyecto de investigación Helios Sharing [1], desarrollado por el grupo de Ingeniería Electrónica aplicada a Sistemas de Energías Renovables (GEISER) de la Escuela Politécnica Superior de la Universidad de Alcalá, coordinado por la empresa CLYSEMA S.A. e incluido en la convocatoria Retos-Colaboración de 2017 (enmarcada dentro del Programa Estatal de Investigación, Desarrollo e Innovación Orientada a los Retos de la Sociedad del Ministerio de Ciencia, Innovación y Universidades).

El objetivo de dicho proyecto hacía referencia al diseño y despliegue de una planta de generación virtual (VPP sus siglas del inglés, Virtual Power Plant) empleando las estaciones base de telefonía que se encuentran desplegadas en el territorio nacional. Para poder poner a disposición de la red eléctrica estas estaciones, fue necesario reconvertirlas en unidades DER con capacidad de almacenamiento distribuido, disposición de bus de continua y generación fotovoltaica, con el fin de alimentar a las cargas, recargar baterías o inyectar energía a la red.

Con todo lo anterior, se perseguía obtener eficiencia energética y rentabilidad económica a la par que ofrecer soporte a la red eléctrica.

Sin embargo, el proyecto no contemplaba específicamente el diseño de la seguridad en las comunicaciones. Es decir, el sistema de gestión inteligente desarrollado para controlar el DER basado en las estaciones de telefonía no tuvo en cuenta las diferentes amenazas de ciberseguridad presentes en las *Smart Grids*.

El trabajo que nos ocupa nace con el fin de atender y cubrir las necesidades en el ámbito de la ciberseguridad que presenta el sistema mencionado.

1.2. Objetivos del trabajo

Los objetivos que comprende el trabajo son los siguientes:

1. Estudiar las principales amenazas de ciberseguridad que pueden afectar a las microrredes inteligentes.
2. Realizar un análisis de ciberseguridad de la microrred del proyecto HELIOS, que cuenta con una instalación fotovoltaica, electrónica de control y sistema de gestión energética (EMS). Este estudio se realizará mediante:
   - Comparativa con casos documentados.
   - Análisis STRIDE [2] del sistema en cuestión para obtener amenazas que no estén documentadas. Para poder realizar un análisis más completo y eficaz se realizará, a su vez, un C4 Model [3] del sistema bajo estudio.

     El análisis STRIDE contribuye a la búsqueda de nuevas amenazas para el sistema:
     - *Spoofing*: Suplantación de Identidad de un usuario del sistema.
     - *Tampering*: Modificación malintencionada de los datos del sistema.
     - *Repudiation*: Denegación de la ejecución de una acción (firma de un contrato inteligente).
     - *Information Disclosure*: Acceso a información del sistema a usuarios que no deberían tenerlo (bases de datos).
     - *Denial of service*: Denegación de un servicio del sistema.
     - *Elevation of privilege*: Usuario que obtiene acceso con privilegios y puede realizar acciones que dañen o destruyan el sistema.
3. Ordenar y categorizar los posibles riesgos que pueda presentar la microrred. En función de la categorización, se obtendrán las amenazas que puedan explotar las vulnerabilidades causando los riesgos más relevantes.

   Esta clasificación se realizará mediante la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT[1]) [4] y con ayuda de la información obtenida del NIST [5].
4. Finalmente, se seleccionarán los riesgos más representativos y se les aplicará una salvaguarda o sistema de protección.

   La salvaguarda será diferente en función del riesgo escogido como ejemplo, pudiendo llegar a utilizarse técnicas como *blockchain*, detección de intrusiones o control de acceso a

[1] MAGERIT está desarrollada por el Consejo Superior de Administración Electrónica del Gobierno de España y dispone de tablas para ordenar y categorizar los riesgos en función de la intensidad de los daños que puedan generar en el sistema.

la información. De esta forma, se logrará la protección parcial del sistema de control y gestión de la microrred inteligente del proyecto Helios Sharing [1].

1.3. Estructura de la memoria

El desarrollo de esta memoria se dividirá en diferentes capítulos interrelacionados entre sí. Dichos capítulos, que estarán subdivididos en apartados (incluyendo una pequeña introducción y su desarrollo), se exponen a continuación:

- ***Capítulo 1:*** Introducción.
- ***Capítulo 2:*** Estado del arte.
- ***Capítulo 3:*** *Smart Grids*.
- ***Capítulo 4:*** Amenazas en *Smart Grids*.
- ***Capítulo 5*:** Evaluación de riesgos en una microrred inteligente.
- ***Capítulo 6*:** Seguridad en la comunicación MQTT.
- ***Capítulo 7:*** Presupuesto.
- ***Capítulo 8:*** Conclusiones y futuras líneas.
- ***Apéndices:***
    - Apéndice A - C4 Model de bajo nivel.
    - Apéndice B - Tablas de evaluación de riesgos.
    - Apéndice C - Código.
    - Apéndice D – Manual de Instalación.

Capítulo 2

Estado del arte

Las amenazas de ciberseguridad relativas a las *Smart Grids* constituyen un campo a explorar que requiere de una mayor contribución por parte de la comunidad científica para implementar un sistema más seguro y fiable. Y es que la digitalización invade, cada vez con más fuerza, el sector eléctrico.

Con el fin de analizar las iniciativas surgidas hasta el momento en respuesta al escenario planteado, se ha llevado a cabo una profunda revisión bibliográfica de las fuentes.

Entre las aportaciones llevadas a cabo por organismos institucionales, destaca el trabajo desarrollado por el National Institute of Standards Technology (NIST) [5], una entidad muy avanzada en el estudio de la ciberseguridad en *Smart Grids* que redactó en 2010 una colección de tres volúmenes con directrices orientadas a la ciber protección de estas (*"Guidelines for Smart Grid Cybersecurity"*). La publicación proporciona una serie de recomendaciones que las organizaciones pueden utilizar para desarrollar estrategias efectivas de ciberseguridad adaptadas a sus características particulares, riesgos y vulnerabilidades.

Posteriormente, en el año 2014, el NIST llevó a cabo una revisión del documento con el fin de adaptarse a los constantes cambios que experimenta la red eléctrica (resulta lógico pensar que en un futuro próximo se hará necesaria una nueva actualización).

- En el primer volumen, "Smart Grid Cybersecurity Strategy, Architecture and High-Level Requirements" [6], concretamente en el capítulo 3, se exponen los requerimientos de ciberseguridad para las *Smart Grids* con el fin de asegurar el cumplimiento de los objetivos de integridad, confidencialidad y disponibilidad.
- En el segundo volumen, "Privacy and the Smart Grid" [7], se tratan diferentes cuestiones relacionadas con la privacidad de los usuarios en las *Smart Grids*, así como algunos ejemplos de casos de uso (contenidos en el apéndice E del propio tomo).
- El tercer volumen, "Supportive Analyses and References" [8], dedica su sexto capítulo a los diferentes tipos de vulnerabilidades que pueden presentar las *Smart Grids.*

Continuando con la literatura institucional, destaca el documento elaborado por el National Electric Sector Cybersecurity Organization Resource (NESCOR): *"Electric Sector Failure Scenarios and Impact Analyses - Version 3.0"* [9]. En él, se describen diferentes escenarios y se realiza un repaso de las vulnerabilidades de algunos dispositivos desplegados en las diferentes

secciones que componen una *Smart Grid,* así como de las posibles mitigaciones frente a las amenazas.

Para la redacción de este documento, el NESCOR se basó en el informe del NIST ya mencionado (*"Guidelines for Smart Grid Cybersecurity"*).

Antes de concluir con la aportación institucional, resulta necesario hablar de la metodología MAGERIT y sus tres libros: "Método" [10], "Catálogo de elementos" [11] y "Guía de técnicas" [12].

- En el primero de ellos, es posible encontrar una introducción, así como los procedimientos necesarios (recomendación de buenas prácticas de seguridad) para realizar una correcta evaluación de riesgos en los sistemas de información.
- El segundo libro sirve de guía para realizar un análisis a través de unas bases genéricas comunes ofreciendo tipos de activos, dimensiones de valoración, criterios de valoración, tipos de amenazas y salvaguardas que se podrían implementar.
- Por último, el tercer ejemplar, ofrece al lector diferentes posibilidades para cuantificar y representar los riesgos.

Los tres volúmenes del NIST, el informe facilitado por el NESCOR y los libros de la metodología MAGERIT elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España han servido para sentar las bases teóricas del presente documento.

Tras repasar la literatura institucional, es importante examinar las publicaciones científicas en tanto que constituyen el principal motor de investigación orientado a la adaptación de las redes inteligentes a las nuevas amenazas que puedan surgir.

Por su parte, el artículo *"Microgrid resilience: A holistic approach for assesing threats, identifying vulnerabilities, and designing corresponding mitigation strategies"* [13] proporciona una revisión completa de amenazas, vulnerabilidades y estrategias para la mitigación de estas en las microrredes eléctricas. Además, expone una metodología de diseño de microrredes resilientes considerando el diseño por seguridad desde cero (evaluando las amenazas, las vulnerabilidades y los riesgos asociados). De esta forma, es posible obtener microrredes eléctricas con las características necesarias para abordar estas amenazas en diferentes situaciones.

Como se expondrá en próximos capítulos, la metodología seguida en el presente trabajo para obtener una evaluación de riesgos será MAGERIT; sin embargo, en el artículo mencionado, la evaluación de riesgos se llevó a cabo con un procedimiento diferente: la metodología DREAD

(Damage, Reproducibility, Exploitability, Affected users and Discoverability). Esta metodología atribuye una puntuación del 1 al 10 a cada uno de los elementos anteriores y realiza la media de valores para obtener el riesgo final.

Prosiguiendo con la línea teórica del proyecto que nos ocupa (evaluación de amenazas en una microrred inteligente), en *"A review on microgrid architecture, cyber security threats and standards"* [14], frente al aumento de los ciberataques, exponen que el desafío clave es crear una microrred robusta y estable. También manifiestan la importancia de la seguridad de los datos del cliente.

En definitiva, el estudio proporciona una descripción completa de todos los requisitos que deben presentar las microrredes inteligentes para ser robustas frente a los problemas de ciberseguridad que pudiesen aparecer. Además, presenta otro modo de obtener los riesgos de ciberseguridad en las microrredes inteligentes, así como una clasificación de los estándares presentes en la literatura institucional en función de su aplicación en la ciberseguridad de las *Smart Grids*.

En *"Cyber-security on smart grid: Threats and potential solutions"* [15], se analizan las amenazas y las posibles soluciones de las *Smart Grids* basada en IoT. El artículo se centra en examinar las vulnerabilidades de la red, las contramedidas frente a los ciberataques y los requisitos de seguridad que deben reunir las redes inteligentes.

Siguiendo con la literatura científica, en *"Cybersecurity in smart grids, challenges and solutions"* [16], se procede a enumerar las diferentes amenazas que afectan a la integridad, la confidencialidad y la disponibilidad de las redes inteligentes. Finalmente, se realiza una clasificación de los diferentes ataques en cada estrato de la red, distinguiendo entre el impacto que causa cada uno de ellos sobre los tres pilares básicos (confidencialidad, integridad y disponibilidad).

Por otro lado, en *"Security Challenges in Control Network Protocols: A survey"* [17], se realiza un análisis de ciberseguridad de los protocolos de comunicación más importantes en el ámbito de los sistemas de control industrial: Modbus, OPC UA, TASE.2, DNP3, IEC 60870-5-101, IEC 60870-5-104 e IEC 61850. En el artículo, se utiliza la misma metodología de prueba basada en ataques de explotación para poder llevar a cabo una comparación mejorada entre ellos. Además, se analiza la eficacia del estándar de seguridad IEC 62351 sobre los diferentes protocolos anteriormente mencionados.

Otros organismos como el European Committee for Standardization (CEN), el European Committee for Electrotechnical Standardization (CENELEC) y el European Telecommunications

Standards Institute (ETSI) se agruparon para realizar el proyecto europeo Smart Grids Information Security (SGIS) y publicaron "*Smart Grid Cibersecurity Risk Assesment (Experiences with the SGIS Toolbox)"* [18], en el que se describe una herramienta y un método (SGIS toolbox). En la investigación, se particulariza en los ataques sobre el control de voltaje para la optimización de los flujos de potencia en un DER. A su vez, presenta un análisis de los mecanismos de protección utilizados y el impacto de seguridad que se podría obtener sobre diferentes activos involucrados a nivel de confidencialidad, integridad y disponibilidad.

Respecto a la temática tratada en el Capítulo 6, Seguridad en la comunicación MQTT, se han encontrado investigaciones similares al presente proyecto, pero sin llevar a cabo una evaluación de amenazas mediante STRIDE, una cuantificación de riesgos con MAGERIT y la realización de pruebas con dispositivos físicos reales.

El artículo *"Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol"* [19] presenta el modelo de amenazas MQTT y sus posibles mitigaciones. Asimismo, efectúa pruebas de ataque de denegación de servicio (DoS) que tienen como objetivo al *broker* de MQTT.

Por último, en *"A Novel MQTT Security framework In Generic IoT Model"* [20], se analizan los avances recientes que se han realizado sobre MQTT para lograr un protocolo de comunicación robusto frente a los problemas de ciberseguridad y se enumeran los desafíos más importantes.

En suma, el presente capítulo constituye una revisión de la literatura institucional, destacando su importancia para sentar las bases teóricas de la ciberseguridad en las redes inteligentes, y de la literatura científica relacionada con la materia que vertebra el presente proyecto: la evaluación de amenazas y riesgos en microrredes eléctricas (incluyendo estudios exhaustivos sobre la ciberseguridad del protocolo MQTT).

Capítulo 3

Smart Grids

La red eléctrica tradicional Figura 1 se ha visto forzada a evolucionar tecnológicamente utilizando los servicios ofrecidos por las tecnologías de la información y comunicación (TICs), dando paso a las *Smart Grids* Figura 2.

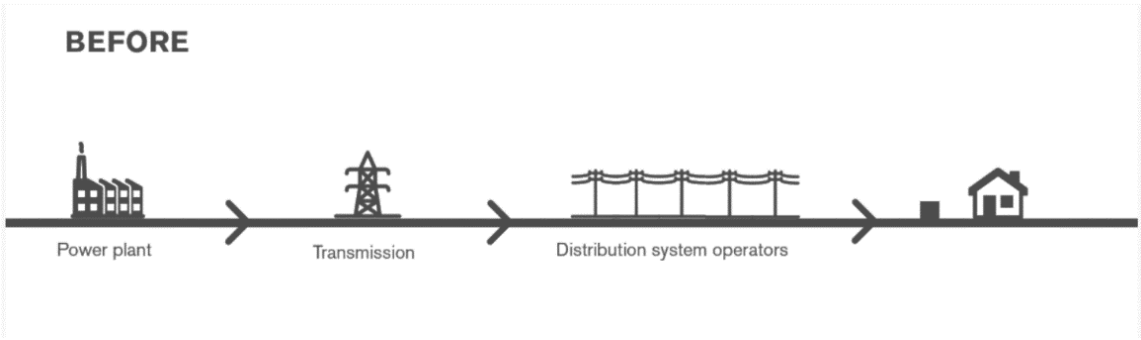

Figura 1. Red Eléctrica Convencional [21].

En la Figura 2 se puede observar cómo las *Smart Grids* dotan de la infraestructura necesaria para permitir la interacción bidireccional en tiempo real entre los consumidores y las empresas de servicios públicos, consiguiendo una electricidad más eficiente, fiable y segura.

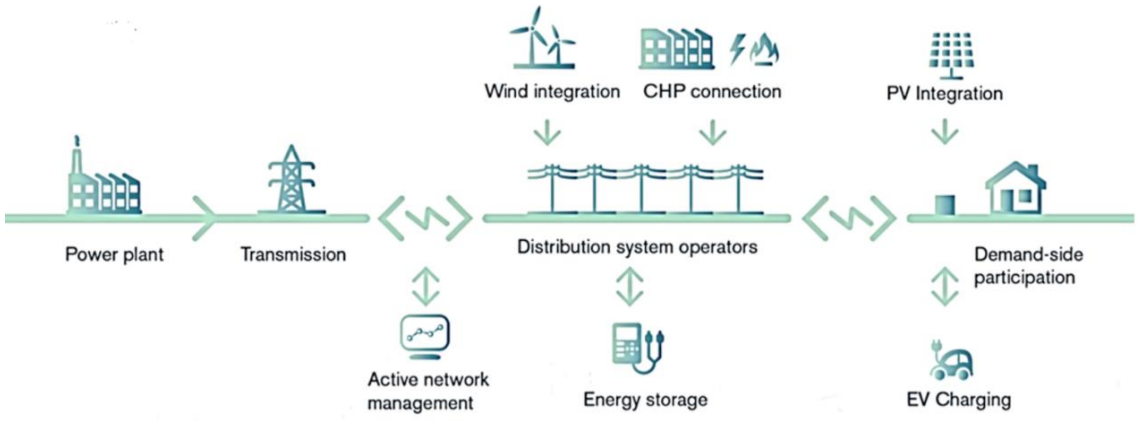

Figura 2. Red Eléctrica Inteligente [21].

Normalmente, las redes inteligentes son una combinación de:

1. Infraestructura inteligente, siendo subyacentes a esta:

- El subsistema inteligente de energía: es el encargado de la generación inteligente de electricidad, transporte y consumo.
- El subsistema inteligente de información: es el responsable de la medición, monitorización y gestión de datos de las *Smart Grids*.

- El subsistema inteligente de comunicación: se encarga de favorecer la comunicación y el intercambio de información entre los diferentes sistemas y dispositivos en las *Smart Grids*.

Cabe destacar que esta infraestructura permite el intercambio bidireccional de energía, lo que supone una evolución con respecto a las redes de energía tradicionales. Actualmente, los usuarios son capaces de generar electricidad para su autoconsumo utilizando paneles solares instalados en sus hogares y devolver a la red la energía sobrante.

2. Sistemas de gestión inteligentes: Son los responsables de proveer servicios de control y gestión de la energía, teniendo como objetivo la mejora de la eficiencia energética, el balance de la oferta y la demanda o reducción de los costes de operación.

En este subsistema se ubica la tecnología *blockchain*. Empresas como Iberdrola han comenzado a incluirla en sus modelos de negocio relacionados con las energías renovables, puesto que permite asignar con rapidez y eficiencia los activos de generación al punto de consumo, estableciendo una jerarquía de prioridades en la fuente de origen.

3. Sistemas de protección inteligentes: Estos sistemas se encargan de proporcionar protección contra fallos físicos y ciberataques, así como servicios de protección de la privacidad en los intercambios de energía.

En cuanto a la infraestructura de las *Smart Grids,* como se puede observar en la Figura 3, esta se puede dividir en 6 subsistemas: sistemas de medición avanzados, fuentes de generación distribuida, transporte, usuario final, distribución y generación a gran escala.

Dichos subsistemas deben colaborar entre ellos de un modo inteligente y, a su vez, tienen que ser resistentes frente a ciberataques y ataques físicos.

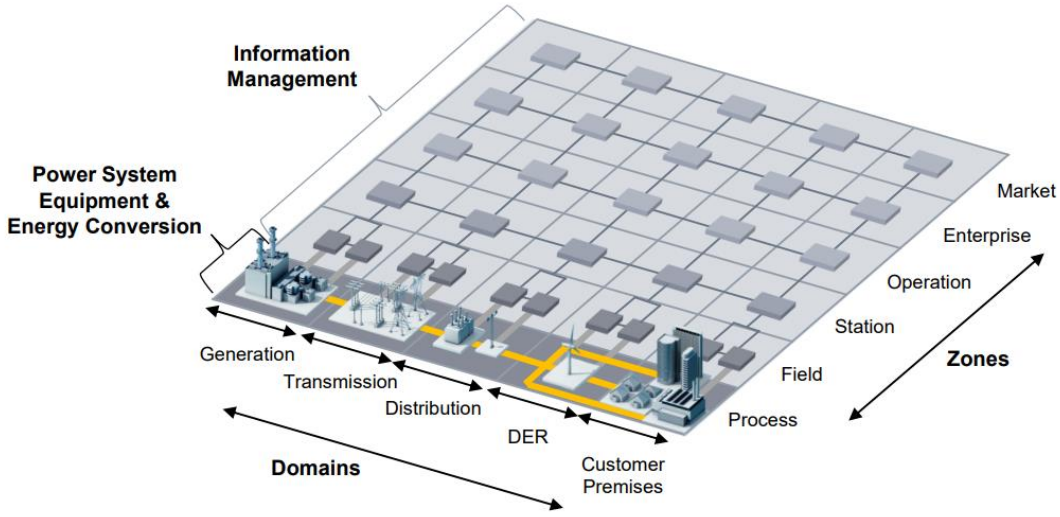

Figura 3. Smart Grid dividida por dominios y zonas [22].

Medición Avanzada

Estos equipos se encuentran desplegados en la infraestructura inteligente, proporcionando información sobre el estado de la red y realizando las mediciones necesarias. Asimismo, se encarga de conectar y desconectar remotamente protecciones, sensores, etc.

Normalmente, este subsistema se divide en los sensores de usuario *submetering*, una red de comunicaciones y una infraestructura avanzada de medición (AMI).

Fuentes de Generación Distribuida (DER)

Se encuentran conectadas a la red de distribución, en el rango de 3 kW a 10.000 kW. En este bloque ha irrumpido con fuerza la generación distribuida mediante energías renovables.

El seguimiento de los DER puede realizarse directamente desde el centro de control por los operadores de red, mediante comunicación con estándares como el IEC 61850.

Transporte de energía

Está compuesto por subestaciones para monitorizar, controlar y automatizar el proceso de transporte de energía de largo recorrido.

Las subestaciones se comunican en tiempo real con la oficina central de control, donde se encuentran los sistemas SCADAS.

Los centros de datos se encargan de monitorizar, balancear las cargas y gestionar la energía en tiempo real, así como responder a los cortes de energía que se puedan registrar. A su vez, es necesario nombrar los sistemas de monitorización, protección y control de área amplia (WAMPAC).

Usuario final

Los usuarios finales pueden pertenecer a diferentes ámbitos, véase el industrial, el comercial o el doméstico.

Dentro de este dominio se pueden encontrar fuentes de generación renovable a menor escala, baterías, vehículos eléctricos o dispositivos inteligentes que se puedan comunicar dentro de los diferentes ámbitos anteriormente descritos.

A su vez, en este apartado es necesario tener en cuenta los sistemas de respuesta a la demanda que ya están implantados en algunos países y que ayudan a optimizar el uso de la energía, logrando una comunicación bidireccional entre empresa y cliente. Esto permite, por ejemplo, un menor uso de las cargas del cliente en horas pico de consumo y, por ende, el suavizamiento de la curva de demanda de energía.

Distribución de energía

Dispone de los mecanismos necesarios para transmitir la energía desde los puntos de distribución hasta el consumidor final (entendiendo como punto final el contador correspondiente de cada usuario).

Generación a gran escala

Generación de energía eléctrica a gran escala mediante combustibles fósiles (carbón, ciclo combinado), centrales nucleares, centrales hidroeléctricas, parques eólicos *offshore* y *onshore y* energía fotovoltaica, estando todas estas tecnologías normalmente conectadas al sistema de transporte.

En la Figura 4 es posible observar un diagrama de flujos de información de las Smart Grids:

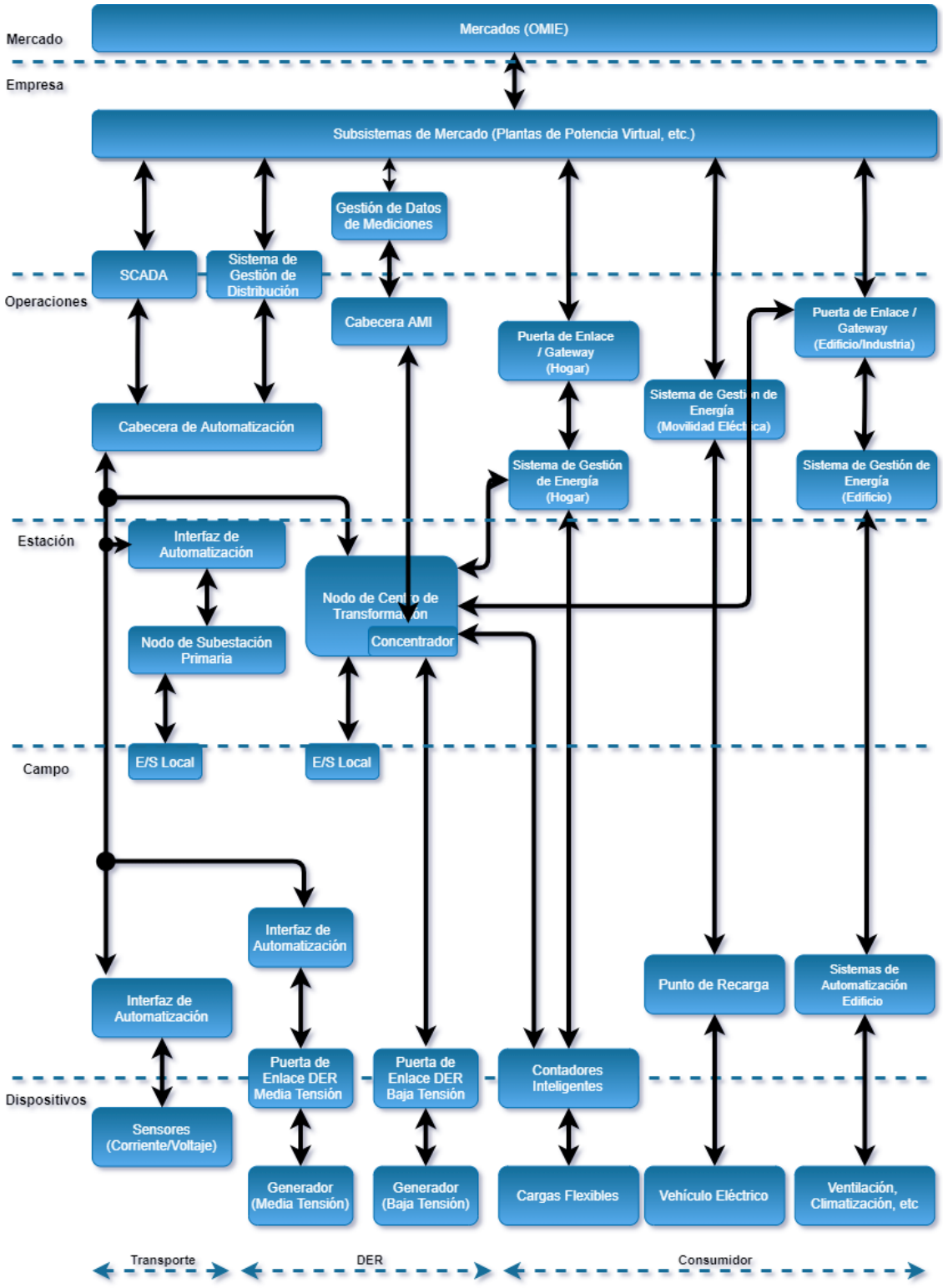

Figura 4. Diagrama de flujo de información *Smart Grid* (Fuente propia).

3.1. Comunicaciones en las *Smart Grids*

El papel que juegan las redes de comunicaciones en las *Smart Grids* es crucial, pues tienen como objetivo fundamental conseguir que esta sea fiable y resistente frente a ciberataques. En este contexto, se distinguen dos retos a batir para conseguir dicho fin:

- Proveer de una plataforma de comunicaciones capaz de llegar a todos los rincones del sistema eléctrico acarrea ciertas consecuencias como los ciberataques contra el funcionamiento normal del sistema físico de energía y los sistemas de control que permiten la operación de los sistemas de potencia.
- Los dispositivos que operan en la red de comunicaciones y los diferentes protocolos mediante los que realizan la comunicación, ofrecen una zona de ataque adicional, pudiendo afectar al funcionamiento normal de los controles de las *Smart Grids*.

3.1.1 Infraestructura de medición avanzada

La infraestructura de medición avanzada (AMI) permite a las *Smart Grids* la comunicación entre los contadores inteligentes ubicados en las instalaciones del cliente y las subestaciones de distribución, siendo este el entorno en el que se localizan las microrredes eléctricas.

Dichos medidores se conectan entre sí por medio de la red disponible en la casa[2], pudiendo leer la información de los dispositivos (ej.: el consumo de los diferentes equipos electrónicos del hogar), así como las incidencias que estos puedan presentar. Así, gracias a los AMI, los centros de monitorización y control pueden lograr una mayor fiabilidad, además de conseguir lecturas en tiempo real para equiparar de un modo más preciso la distribución de cargas del consumidor.

Para la implementación de la red de comunicación HAN se podría utilizar Zigbee o MQTT (cada uno en sus respectivas capas de red), unos de los protocolos más usados y con mayor soporte para este tipo de redes.

[2] La red a la que se conectan los medidores domésticos recibe la denominación de HAN (Home Area Network).

3.1.2 Comunicaciones entre dispositivos de campo y subestaciones eléctricas

Dispositivos de campo

Los dispositivos de campo presentan diversas aplicaciones y, entre ellas, se encuentra la recopilación de datos de medición por concentradores de información. Por ende, la integridad y la disponibilidad de los datos constituyen uno de los requisitos más importantes.

Hay dispositivos de campo, como las Unidades de Medida Fasorial (PMU), que dependen de una buena sincronización de tiempos en todas las unidades desplegadas en la red.

Además, en los dispositivos de campo, se suelen utilizar protocolos de bajo nivel (como el protocolo Modbus) y están controlados por las subestaciones eléctricas mediante una red creada para comunicarse con ellos.

Subestaciones eléctricas

La red anteriormente mencionada puede ser también utilizada en las subestaciones eléctricas. Estas comunicaciones se basan en facilitar el intercambio de datos de los medidores, así como en ordenar el disparo protecciones en caso de faltas.

Las comunicaciones entre las subestaciones eléctricas pueden considerarse críticas o no en lo que a tiempo se refiere:

- Las comunicaciones críticas hacen referencia a aquellas que se encargan de coordinar los esquemas de protección para que, por ejemplo, se produzca el disparo de una protección en un corto periodo de tiempo.
- Las comunicaciones que no son críticas hacen referencia a aquellas que se encargan de realizar una actualización de las configuraciones del sistema o a realizar un post procesamiento de fallas para el desarrollo de nuevas tecnologías.

En este caso, se pueden utilizar protocolos parecidos a los del apartado anterior, pero se añaden otros nuevos más complejos como el IEC-61850, DNP3 o el IEC-104.

3.1.3 Comunicaciones con el centro de control

Este tipo de comunicaciones son las que se realizan entre las subestaciones y los centros de monitorización y control, pero también entre los propios centros de control para poder coordinarse.

De la misma forma que en el apartado anterior, es posible diferenciar entre comunicaciones críticas y no críticas, siendo las críticas las más relevantes para el punto que nos ocupa.

Estas comunicaciones están relacionadas con el control y la monitorización de la automatización de la subestación eléctrica, así como con la gestión de la configuración y el procesamiento de fallas.

Además, las restricciones para el tiempo de transmisión son altas ya que la comunicación de las acciones que se pretenden ejecutar desde el centro de control deben de ser inmediatas para que los equipos, en caso de emergencia, no sufran daños.

Los diferentes centros de control se comunican entre sí con el fin de intercambiar información sobre fallos o datos de alarmas que hayan surgido en las subestaciones y poder realizar un posterior análisis de contingencias u activar protocolos internos de emergencia.

Los protocolos aplicados son semejantes a los que utilizan las subestaciones eléctricas para comunicarse, siendo el IEC-61850 uno de los más utilizados a nivel europeo.

Al igual que en los otros apartados, la integridad y la confidencialidad son muy importantes. En este caso, se añade el hecho de que las transacciones entre los centros de control implican decisiones financieras importantes para la compañía.

Esta comunicación es de vital importancia en tanto que se pueden tomar decisiones sobre precios en base a una información incorrecta e, incluso, dicha transacción podría llegar a ser manipulada por medio de un ciberataque, derivando en graves consecuencias financieras para las compañías eléctricas.

3.2. Microrredes eléctricas inteligentes [23]

Las microrredes eléctricas pueden definirse como un grupo de fuentes de generación de energía, cargas y almacenamiento, pudiéndose encontrar estas en modo isla o integradas con la red eléctrica. La puesta o no en modo isla de la microrred se llevará a cabo en función de los requisitos técnicos y económicos que presente la aplicación.

Una microrred está compuesta por numerosas fuentes de generación de energía controladas independientemente para constituir una infraestructura de red fiable y flexible.

El principal objetivo de la creación de las microrredes eléctricas es la disminución del uso de los combustibles fósiles, además de resolver problemas de calidad de la energía, de resiliencia y flexibilidad de la infraestructura de red existente.

En la Figura 5 se puede observar un ejemplo de arquitectura de una microrred eléctrica:

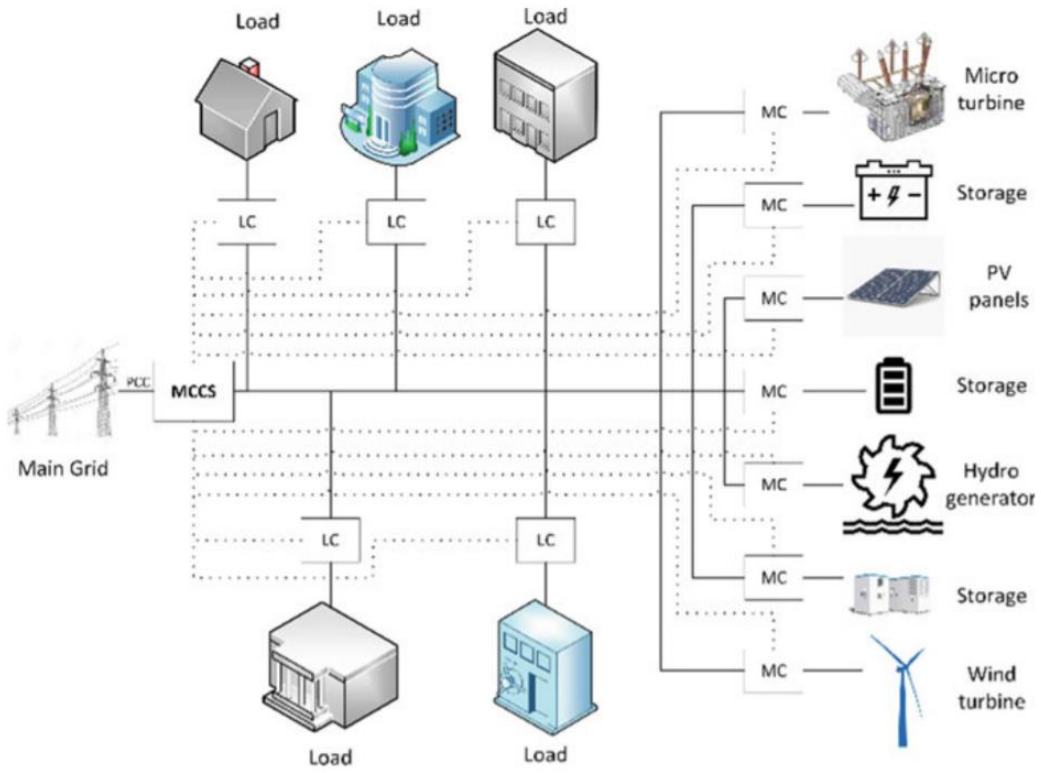

Figura 5. Ejemplo de arquitectura de microrred eléctrica.

Existen diferentes tipologías de microrredes eléctricas, como la radial, de anillo o de malla. Asimismo, es posible encontrar los siguientes tipos de microrred:

- Microrredes de consumidor doméstico.
- Microrredes institucionales.
- Microrredes comunitarias.
- Microrredes remotas aisladas de la red debido a inconvenientes geográficos y económicos.
- Microrredes de bases militares.
- Microrredes comerciales e industriales.

Estas microrredes eléctricas inteligentes necesitan el apoyo del IoT para poder realizar la comunicación entre todos los equipos desplegados en esta. Pero existen diferentes problemas de ciberseguridad debido a los motivos que ya se han expuesto con anterioridad en el presente documento.

La información que se intercambien los equipos inteligentes de las microrredes eléctricas será un elemento clave para las *Smart Grids*. El IoT aplicado a las microrredes inteligentes producirá una gran cantidad de datos en tiempo real y los sistemas de inteligencia artificial analizarán, procesarán y filtrarán estos datos para cada cliente final.

Por ello, es necesario destacar cuatro puntos que debe abordar el sistema inteligente de gestión de las microrredes eléctricas:

- Resiliencia.
- Seguridad frente a ciberataques.
- Robustez.
- Estabilidad de precios.

Las microrredes eléctricas basadas en IoT tendrán un gran impacto en el control de las redes inteligentes, dado que se tendrán que plantear nuevas formas de producir, distribuir y gestionar la energía de estas, ya sea en modo isla o conectadas a la red.

Las cuestiones de ciberseguridad que se deben abordar para conseguir microrredes inteligentes seguras y fiables se desarrollan en el siguiente capítulo Amenazas en *Smart Grids*.

Capítulo 4

Amenazas en *Smart Grids*

La evolución hacia una red eléctrica inteligente está causando y causará la aparición de nuevas amenazas que puedan explotar las vulnerabilidades de las *Smart Grids*. En la Figura 6 se puede observar cómo dichas amenazas pueden surgir en todo el entorno referente a las *Smart Grids*.

Es necesario avanzar en el campo de la ciberseguridad aplicada a las *Smart Grids pu*esto que la red eléctrica es susceptible de verse afectada por ciberatacantes. Por ello, es importante hacer un estudio de los riesgos que puedan afectar al funcionamiento normal de las redes inteligentes.

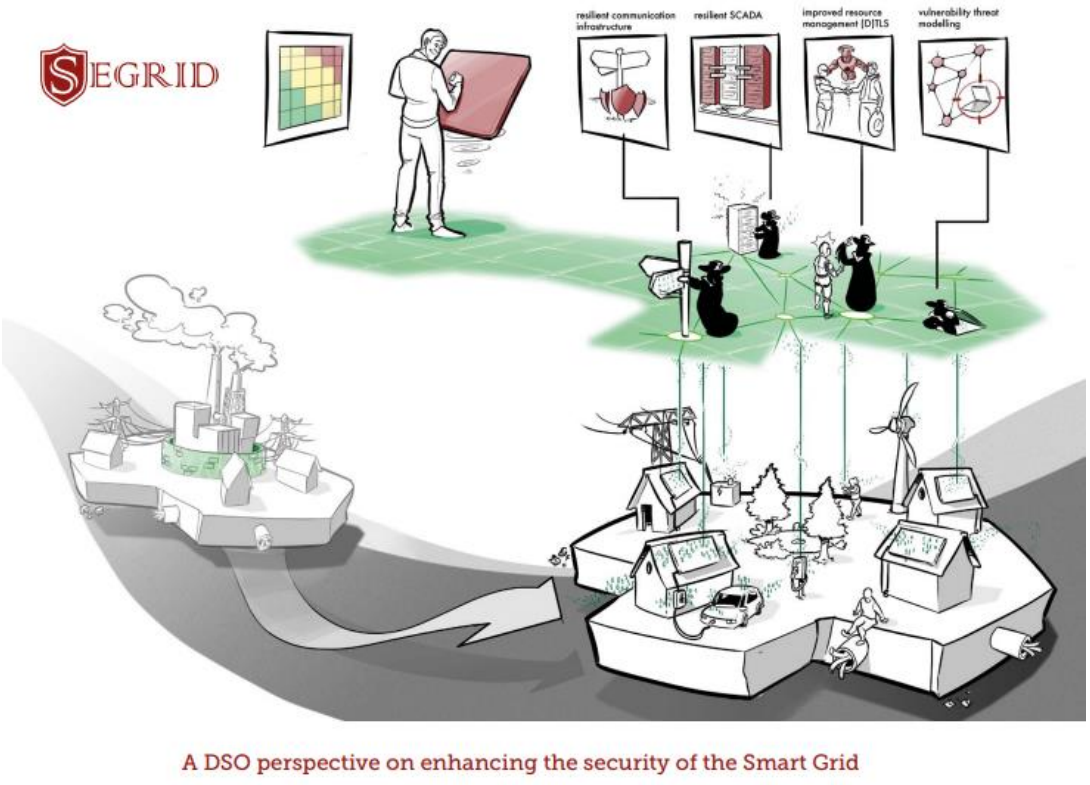

Figura 6. Amenazas en *Smart Grids* [24].

Antes de evaluar las amenazas que pueden dañar las *Smart Grids*, es necesario atender a los tres pilares fundamentales de la ciberseguridad, que serán los objetivos de estas a corto y largo plazo:

Confidencialidad

Se define como la propiedad que verifica que la información del sistema no sea revelada a terceros con mala intencionalidad, así como que empresas realicen espionaje.

La confidencialidad en el contexto doméstico es fundamental ya que, si se filtran datos sobre el usuario con el objetivo de hacer un uso fraudulento de estos por parte de las empresas, este querrá desinstalar el equipo de su vivienda y perderá la confianza en la empresa que ofrece el servicio.

Por esta razón, se debe asegurar:

- La privacidad de la información del cliente.
- La información del mercado eléctrico.

Integridad

La integridad es otro requisito de seguridad crítico para los sistemas de energía ya que evita que tengan lugar las siguientes acciones:

- La modificación de datos sin autorización.
- La ausencia de autentificación de la fuente de datos y sus tiempos asociados.
- El desconocimiento de la calidad de los datos.

Disponibilidad

La disponibilidad se considera generalmente el requisito de seguridad más relevante en contextos como el industrial, dado que, si se consiguiese bloquear el funcionamiento de la red eléctrica en alguno de sus niveles, supondría grandes pérdidas monetarias y de imagen empresarial.

Se deben asegurar los siguientes tiempos de respuesta:

- Milisegundos, para sistemas de protección físicos.
- Décimas de segundos, para la monitorización de la transmisión.
- Segundos, para el control de supervisión de subestaciones, *feeders* y adquisición de datos (SCADA).
- Minutos, para la monitorización equipos no críticos y obtención de información relacionada con los precios de mercado.
- Horas, para la lectura de medidores e información de precios de mercado a largo plazo.
- Días, semanas o meses, para recopilar datos a largo plazo, como información sobre la calidad de la energía.

El objetivo de este análisis es conseguir que los sistemas que se encuentran operando en las *Smart Grids* sean resilientes en los tres pilares básicos de la ciberseguridad. En definitiva, proteger la confidencialidad, la integridad y la disponibilidad del sistema.

4.1. Amenazas listadas por NESCOR

A continuación, se expondrá una selección de las amenazas más representativas del documento redactado por el NESCOR: "Electric Sector Failure Scenarios and Impact Analyses – Version 3.0" [9].

*Los códigos referidos en el título de cada uno de los casos hacen referencia a su localización en el índice de la publicación.

4.1.1 Infraestructura de medición avanzada

Caso 1: Empleados autorizados realizan una desconexión remota no autorizada (AMI.1).

- **Descripción:** Un empleado descontento, extorsionado o sobornado que tenga autorización para realizar acciones de control, manda un comando de control para desconectar un gran número de medidores.
- **Vulnerabilidades:**
  - El sistema permite secuencias de comandos potencialmente dañinas, como una gran cantidad de desconexiones que pueden amenazar el equilibrio del sistema.
- **Impactos:**
  - Una desconexión/conexión masiva instantánea a través de múltiples concentradores podría causar apagones temporales debido a la desconexión de los interruptores eléctricos o *circuit breakers*, hasta que la energía en la red pudiera ser balanceada.
  - Una pequeña cantidad de desconexiones podría afectar en la confianza del consumidor hacia las *Smart Grids* y hacer a su vez que se pierda confianza en la empresa que ofrece el servicio de suministro eléctrico.
- **Posibles mitigaciones:**
  - Detectar comandos anormales.
  - Usar un control de acceso basado en roles (RBAC).
  - Validar los datos para admitir solo cambios razonables.
  - Generar alarmas si hay cambios en datos críticos.
  - Crear un sistema de auditoría para registrar quien ha realizado cambios sobre el sistema.
  - Requerir la autorización de dos personas para este tipo de acciones de control sobre elementos críticos de la red.
  - Limitar el número de elementos que se pueden desconectar a la vez en un periodo de tiempo concreto.

Caso 2: Dispositivos no autorizados realizan un ataque de Denegación de Servicio (DoS) y bloquean mensajes válidos para la respuesta a la demanda (DR) (AMI.18).

- **Descripción:** Dispositivos no autorizados acceden a una red doméstica HAN. Estos pueden ser utilizados para realizar un ataque DoS con el fin de que los mensajes de DR no puedan llegar al cliente final.
- **Vulnerabilidades:**
  - El sistema está basado en credenciales que son fáciles de obtener mediante un ataque de fuerza bruta, consiguiendo acceso a la HAN.
  - Las interfaces de red permiten flujos innecesarios de información hacia puntos que no sean el *router* o la puerta de enlace de confianza de la HAN.
- **Impactos:**
  - La imposibilidad de recibir mensajes de DR puede hacer que el cliente final se vea afectado pagando más por la energía o sufriendo la desconexión de un dispositivo.
  - La empresa que ofrece el servicio tendrá costes asociados a la solución de los problemas presentados al cliente final.
  - Si se realiza el mismo ataque a gran escala, podrían producirse cortes de energía debido a la incapacidad de la empresa que ofrece el servicio para realizar acciones de DR.
- **Posibles mitigaciones:**
  - Restringir el acceso de dispositivos a la red HAN.
  - Solicitar autentificación para el acceso de dispositivos a la red HAN.

Caso 3: Sistema de encriptación débil en las comunicaciones de los dispositivos AMI (AMI.24).

- **Descripción:** Un proveedor de dispositivos AMI implementa un sistema criptográfico débil fácilmente descifrable, permitiendo el acceso y la modificación de la configuración del dispositivo.
- **Vulnerabilidades:**
  - Se usa un sistema criptográfico, el cual puede llegar a romperse en un corto periodo de tiempo, consiguiendo el acceso a la información importante del dispositivo AMI.
- **Impactos:**
  - Costes por la actualización o el reemplazamiento del dispositivo AMI.
  - Pérdida de información privada del cliente y sus costes asociados.
  - Desconexión en masa de medidores de campo, causando la intervención del *circuit breaker* y resultando en cortes de energía temporales.

- **Posibles mitigaciones:**
  - Implantar algoritmos criptográficos verificados.
  - Definir procedimientos en las políticas de gestión de configuraciones y cambios para introducir nuevos algoritmos criptográficos.
  - Realizar pruebas de los controles de seguridad en el periodo de verificación del sistema.

Caso 4: Dispositivo no autorizado obtiene acceso a la red HAN y roba información privada (AMI.29).

- **Descripción:** Un dispositivo no autorizado obtiene acceso a la HAN y usa la interfaz web para obtener información privada como, por ejemplo, patrones de uso de energía u obtención de información acerca del tipo de dispositivos instalados en el domicilio.
- **Vulnerabilidades:**
  - El sistema se basa en credenciales que son fáciles de obtener para acceder a la HAN.
- **Impactos:**
  - Violación de la privacidad del cliente final.
  - Pérdida de confianza en la AMI, incluso si la empresa que ofrece el servicio no es responsable de la privacidad del cliente.
  - Costes asociados a la violación de la privacidad.
- **Posibles mitigaciones:**
  - Implantar algoritmos criptográficos verificados para la protección de la HAN.
  - Requerir autentificación mediante múltiples factores para el acceso a la red.
  - Minimizar la cantidad de información privada recogida en cada sistema y dispositivo de la red.

4.1.2 Recursos energéticos distribuidos (DER)

Caso 1: Control de acceso inadecuado del DER causa fallo del sistema (DER.1).

- **Descripción:** Cuando el propietario no puede cambiar la contraseña por defecto o no se ha establecido una clave para la interfaz del sistema, el ciberatacante puede llevar a cabo una suplantación y obtener acceso a la interfaz.
- **Vulnerabilidades:**
  - Personas no autorizadas pueden acceder al DER.
  - La contraseña por defecto no se modifica o establece por el usuario.
  - El sistema permite cambios o monitorización por actores no autorizados en la red, provocando fallos en partes críticas del DER.

- **Impactos:**
  - El sistema sufre daños físicos, provocando la parada parcial o completa de su funcionamiento.
  - El usuario puede perder confianza en el sistema tras comprobar que es propenso a sufrir ataques.
  - El operario de mantenimiento o el usuario puede sufrir un accidente de electrocución si las protecciones pertinentes no saltan debido al mal funcionamiento del DER.
- **Posibles mitigaciones:**
  - Solicitar la autentificación del usuario u operario para las interacciones que se realicen con la interfaz.
  - Sugerir al usuario el cambio de la información de acceso una vez se haya instalado el equipo.
  - Asegurar el hardware con las protecciones pertinentes para proteger frente a un fallo del sistema.
  - Formar a los operarios para que enseñen a los usuarios, en el momento de la instalación, los beneficios o desventajas asociados a la presencia en sus equipos de mecanismos de seguridad.
  - En caso de que el usuario u operario realizase modificaciones críticas, crear un aviso para informar de que esa acción podría causar alteraciones en el sistema.
  - Incluir diferentes roles para limitar privilegios en las acciones que se consideren críticas.

Caso 2: El DER dispone de conexión inalámbrica a Internet, exponiéndose a diferentes amenazas (DER.2).

- **Descripción:** Al tener conexión inalámbrica a internet con requisitos de seguridad limitados, la microrred basada en DER es interceptada por un ciberatacante que obtiene el control del sistema.
- **Vulnerabilidades:**
  - El sistema está basado en credenciales de acceso que son fáciles de obtener a través de la conexión a internet.
  - La red inalámbrica permite el acceso de ciberatacantes no autorizados, provocando fallos y cambios en el funcionamiento.
- **Impacto:**
  - El usuario pierde confianza en el equipo y en la empresa instaladora.

- Se podría producir un desequilibrio del sistema si el DER fuese de mayor potencia, pudiendo provocar sobrecargas en los transformadores de la subestación que realice la distribución hacia ese DER.

- **Posibles mitigaciones:**
  - Autentificar los diferentes dispositivos por si se produjesen nuevas conexiones no autorizadas.
  - Detectar cambios no autorizados en el sistema.
  - Si el usuario u operario realizase modificaciones críticas, crear un aviso informando de que esa acción podría causar algún tipo de fallo o parada del sistema.
  - Limitar las modificaciones funcionales y de seguridad remotas del sistema.
  - Incluir diferentes roles para limitar privilegios en las acciones que se consideren críticas.
  - Autentificar e incluir mensajes de error en las comunicaciones en los protocolos de comunicación utilizados.

Caso 3: Información confidencial de consumo y generación del DER es sustraída para diferentes usos (DER.4).

- **Descripción:** El *Energy Management System* (EMS) monitoriza y gestiona la demanda y la generación de energía de la microrred basada en DER del cliente. El ciberatacante intercepta las comunicaciones del EMS obteniendo información relevante sobre el funcionamiento del sistema.
- **Vulnerabilidades:**
  - El sistema permite el acceso a las comunicaciones de ciberatacantes (agentes externos).
  - Los ciberatacantes obtienen información privada del usuario.
- **Impacto:**
  - El equipo y la empresa instaladora tienen pérdida de confianza por parte del cliente al no ofrecer la seguridad de la información privada/personal.
  - La empresa es demandada por el cliente por no haber conseguido ofrecer un servicio seguro, comprometiendo su privacidad.
- **Posibles mitigaciones:**
  - Encriptar las comunicaciones utilizadas para evitar la sustracción de información confidencial de la empresa o privada para el usuario.
  - Autentificar los dispositivos desplegados en la instalación.

Caso 4: Los datos meteorológicos comprometidos de DERMS modifican los pronósticos de salida de DER (DER.20).

- **Descripción:** Un agente de amenazas accede al sistema DERMS y modifica los datos medidos por la estación meteorológica que son utilizados para pronosticar cargas, así como para la generación/almacenamiento de DER.
- **Vulnerabilidades:**
  - El sistema se basa en credenciales que son fáciles de obtener para acceder a DERMS.
  - Los usuarios no tienen visibilidad sobre los cambios realizados por lo que no pueden actuar en consecuencia.
  - Los mensajes modificados por ciberatacantes resultan complejos de distinguir de un mensaje válido para el acceso a los datos de las predicciones.
- **Impacto:**
  - Impacto financiero para el usuario, ya que el DERMS puede llegar a establecer un precio o una cantidad de energía a generar que no coincida con las predicciones.
  - Costes legales para la empresa, relacionados con una posible demanda del usuario del DER por prácticas desleales.
- **Posibles mitigaciones:**
  - Usar RBAC en el sistema DERMS de la empresa.
  - Autentificar los mensajes en el protocolo de comunicación utilizado.
  - Verificar la integridad del mensaje de comandos de control del DERMS.

Caso 5: La información de registro del sistema DER es robada (DER.21).

- **Descripción:** Un ciberatacante accede al sistema DERMS y sustrae la información de registro del DER.
- **Vulnerabilidades:**
  - El sistema permite acceso a funciones innecesarias del DERMS.
  - Los usuarios no tienen visibilidad sobre los cambios realizados por lo que no pueden actuar en consecuencia.
  - Los mensajes modificados por ciberatacantes son complicados de distinguir de un mensaje válido para el acceso a datos de las predicciones.
- **Impacto:**
  - Brecha de seguridad en la información confidencial del usuario.
  - Pérdidas financieras debido a la brecha de seguridad.
- **Posibles mitigaciones:**
  - Usar RBAC en el sistema DERMS.

- Introducir un IDS e IPS como parte de la red DERMS.
- Proteger las credenciales que permiten el acceso a los datos de registro del DER del usuario.
- Crear registros de auditoría para guardar los accesos a los datos de registro.

4.1.3 Transporte de energía

Monitorización, Protección y Control de Área Amplia (WAMPAC: *Wide Area Monitoring Protection and Control*).

Caso 1: Comunicaciones comprometidas entre las Unidades de Medida Fasorial (PMU) y el centro de control (WAMPAC.6).

- **Descripción:** Las comunicaciones WAMPAC se ralentizan o se detienen al atacar las comunicaciones entre las PMU y el centro de control. Esto se podría realizar atacando componentes que forman la red, como *routers*, u obteniendo acceso a dicha red ejecutando posteriormente un ataque de inundación SYN.
- **Vulnerabilidades:**
  - Los usuarios carecen de visibilidad de la actividad sobre amenazas, como el acceso de un intruso a la red.
  - Las credenciales de acceso a la red WAMPAC son fáciles de obtener.
- **Impactos:**
  - Retraso en la reconfiguración de la red.
  - Retraso en el disparo de las protecciones eléctricas.
  - Generación innecesaria debido a la optimización deficiente de los flujos de potencia.
  - Fallo en cascada debido a la sobrecarga de la línea.
- **Posibles mitigaciones:**
  - Detección y bloqueo de accesos no autorizados a la red de comunicaciones.
  - Restringir el acceso a la red empleando listas de control de acceso en el *router* y firewalls.
  - Introducir un IDS o IPS y comprobar que no bloquea el funcionamiento normal del sistema.

Caso 2: Base de datos comprometida tiene impacto en la estabilidad de red (WAMPAC.7).

- **Descripción:** Un ciberatacante con información privilegiada puede obtener acceso no autorizado a la red a la que el histórico de mediciones de WAMPAC está conectada, así como al software de la base de datos.

  El ciberatacante corrompe o elimina datos de medición de la base de datos.

- **Vulnerabilidades:**
  - Las interfaces de red permiten acceso innecesario al histórico.
  - Los usuarios carecen de visibilidad sobre la realización de cambios no autorizados en la base de datos del histórico de mediciones de WAMPAC.
  - Individuos no autorizados pueden acceder de forma remota al histórico desde redes externas.
  - El sistema está basado en credenciales fácilmente obtenibles para acceder a la configuración y actualizaciones de software del histórico.
- **Impactos:**
  - Generación innecesaria debido a la optimización deficiente de los flujos de potencia.
  - Retraso en el disparo de las protecciones eléctricas.
  - Fallo en cascada debido a la sobrecarga de la línea.
- **Posibles mitigaciones:**
  - Restringir el acceso remoto al histórico.
  - Permitir únicamente el acceso mediante lectura a los datos del histórico.
  - Generar alertas de actividad maliciosa en la base de datos del histórico de mediciones.
  - Usar RBAC con el fin de limitar los privilegios para la modificación de los datos gestionados por el histórico.
  - Asegurar la integridad del mensaje usando encriptación en las comunicaciones de la red WAMPAC.

Gestión de la distribución (DGM).

Caso 1: Los dispositivos de campo de la subestación son suplantados influyendo en las respuestas automatizadas (DGM.6).

- **Descripción:** El ciberatacante suplanta las entradas de datos de los dispositivos de campo en las subestaciones para conseguir que el Sistema de Gestión de la Distribución (DMS) informe, por ejemplo, de un estado crítico del sistema. Esto podría llevar a que el operador o el sistema automático tomen medidas inapropiadas.
- **Vulnerabilidades:**
  - Se permite que los mensajes sean modificados por personas no autorizadas en las comunicaciones entre los dispositivos de campo y el DMS.
  - Es complicado distinguir entre el mensaje modificado por un ciberatacante y uno válido en las comunicaciones entre los dispositivos de campo y el DMS.

- **Impactos:**
  - Las acciones inapropiadas de despeje de faltas y un uso excesivo de actuaciones de reparación y reconfiguración de línea conducen a la pérdida de energía para los clientes finales.
  - Los controles de tensión se aplican o ajustan incorrectamente en función de datos erróneos, posiblemente desencadenando disparos por huecos o picos de tensión.
  - Los datos recopilados por el medidor son incorrectos debido a la influencia del ciberatacante, obteniéndose una posible pérdida de ingresos para la empresa que ofrece el servicio o un mayor consumo para el cliente.
- **Posibles mitigaciones:**
  - Autentificación de los mensajes en la comunicación entre los dispositivos de campo y los centros de control.
  - Detección de patrones inusuales de entradas que pudiesen indicar acciones o datos erróneos mediante la comparación de las entradas entre sí y con sus respectivas entradas anteriores.
  - Limitar el acceso a las comunicaciones.
  - Realizar una encriptación de las comunicaciones.

Caso 2: Bancos de condensadores conmutados son manipulados para empeorar la calidad de la red (DGM.10).

- **Descripción:** Los bancos de condensadores conmutados pueden crear grandes transitorios de conmutación cuando están conectados a un *feeder* de la empresa que ofrece el servicio, generando picos de tensión de hasta el doble del voltaje nominal. Esto puede agravarse cuando se conectan varios bancos a la vez, uno al lado del otro.

  Un ciberatacante obtiene la contraseña de la interfaz hombre-máquina (HMI) para obtener el control de los relés que realizan la conexión/desconexión del banco de condensadores para encender y apagar, generando picos de voltaje en cascada y retardos en el disparo de los dispositivos de protección.

- **Vulnerabilidades:**
  - Se permite acceso físico a personas no autorizadas.
  - Un ciberatacante obtiene las credenciales de acceso al HMI.
  - Un ciberatacante obtiene la IP para el acceso remoto al DMS.
  - Un empleado puede abrir un correo de phishing introduciendo las credenciales de acceso al HMI.

- **Impactos:**
  - La repetición de picos de tensión puede dañar a los equipos del cliente o de la empresa que ofrece el servicio.
  - Mal funcionamiento de los dispositivos de protección pudiendo provocar pérdida de energía del cliente.
  - No disponibilidad del banco de condensadores en situaciones en las que sea necesario.
- **Posibles mitigaciones:**
  - Formar al personal sobre las amenazas de ataques de ingeniería social y realizar ejercicios de ingeniería (como correos electrónicos de phishing generados por la propia empresa o mediante unidades USB) para involucrar a los empleados.
  - Restringir el acceso físico a las consolas y HMI.
  - Introducir RBAC para el acceso al HMI, de modo que se limite el acceso a las funciones críticas del DMS.
  - Auditar los accesos a las funciones críticas del DMS.

4.1.4 Vehículo eléctrico

Caso 1: Muchas recargas rápidas simultáneas provocan una sobrecarga del centro de transformación de media/baja tensión (ET.2).

- **Descripción:** Un ciberatacante puede comprometer la gestión de la recarga rápida cuando haya una gran cantidad de vehículos conectados a las estaciones de recarga.

  El ciberatacante puede modificar el algoritmo de distribución de carga, de modo que la carga rápida sea simultánea para todos los vehículos, provocando una interrupción en la red de la zona y dejando sin suministro eléctrico a los puntos de recarga y a los emplazamientos cercanos.

- **Vulnerabilidades:**
  - El sistema permite cambios no autorizados en la gestión de la estación de recarga.
  - Un diseño, implementación y mantenimiento pobres posibilitan que el sistema entre en un estado crítico, permitiendo que los circuitos se sobrecarguen en el transformador de distribución.
- **Impacto:**
  - Cortes de energía en los vehículos eléctricos y la estación de recarga.
  - Daño o desconexión del transformador de distribución.

- **Posibles mitigaciones:**
  - Autentificar a los usuarios para acceder a los archivos de software y configuración del sistema de gestión de la estación de carga rápida.
  - Verificar la integridad del firmware del software de administración de la estación de carga rápida y sus archivos de configuración.
  - Generar alarmas sobre cambios en la configuración, como el número de vehículos eléctricos que se pueden cargar simultáneamente.
  - Instalar un interruptor eléctrico o *circuit breaker* para evitar la sobrecarga del transformador de distribución.

Caso 2: Información intercambiada entre el vehículo eléctrico (EV) y el punto de recarga (EVSE) (ET.7).

- **Descripción:** Información privada intercambiada entre el EV y el punto de recarga es capturada por un ciberatacante (información acerca del dueño del vehículo eléctrico, localización del vehículo eléctrico, localización del domicilio, etc.).
- **Vulnerabilidades:**
  - El sistema permite que los datos intercambiados sean fácilmente accesibles para individuos no autorizados.
- **Impacto:**
  - Pérdida de datos privados del cliente final.
  - Pérdida de confianza en el modelo de gestión del vehículo eléctrico y en el vehículo eléctrico (indirectamente, la empresa que ofrezca el servicio también experimentará pérdida de confianza por parte del cliente final).
- **Posibles mitigaciones:**
  - Encriptar las comunicaciones entre el vehículo eléctrico y el punto de recarga.

Caso 3: Registro de vehículo eléctrico con preferencia usado con malas intenciones para obtener una recarga más rápida (ET.10).

- **Descripción:** Si en un futuro se introdujese el transporte eléctrico en los vehículos oficiales (tales como ambulancias o coches de policías), estos deberían poseer una identidad especial para obtener preferencia en los puntos de recarga ante emergencias.

  Un ciberatacante podría obtener dicha credencial y utilizarla o compartirla para que otros usuarios se beneficiasen de estas ventajas.

- **Vulnerabilidades:**
  - El sistema no comprueba correctamente la credencial de acceso.

- **Impacto:**
  - Carga más lenta de otros vehículos especiales o de usuarios ordinarios.
  - Desequilibrios en la distribución al ser utilizada este tipo de recarga por usuarios convencionales que no presentan ningún tipo de emergencia.
- **Posibles mitigaciones:**
  - Requerir un PIN o certificado junto con la identidad del vehículo eléctrico en el momento de realizar el registro.
  - Utilizar el mecanismo *Rivest Shamir Adleman* (RSA) o infraestructura de clave pública (PKI) para los vehículos oficiales.

Caso 4: Ciberatacante causa la descarga del vehículo eléctrico hacia la red (ET.15).

- **Descripción:** Un ciberatacante compromete el protocolo *Open Charge Point Protocol* (OCPP) [25] que permite comunicaciones con el sistema de gestión de los puntos de recarga.

  El ciberatacante puede interceptar las comunicaciones e incluso inyectar un *malware*, consiguiendo que los vehículos se descarguen parcial o completamente sin el consentimiento del propietario.
- **Vulnerabilidades:**
  - El sistema permite cambios no autorizados.
  - El protocolo de comunicación empleado no dispone de mecanismos de ciberseguridad.
- **Impacto:**
  - Pérdida de confianza del usuario final sobre el sistema de recarga del vehículo eléctrico.
  - Costes asociados a la demanda interpuesta por dicho usuario ante las pérdidas causadas.
- **Posibles mitigaciones:**
  - Requerir un PIN o certificado junto con la identidad del vehículo eléctrico en el momento de realizar el registro.
  - Utilizar el mecanismo RSA o PKI para los vehículos oficiales.

4.1.5 Respuesta a la demanda (DR)

La respuesta a la demanda o DR hace referencia a un método de gestión de la energía que ha sido implantado en países como Estados Unidos, donde los consumidores son capaces de ajustar su patrón de consumo ante un desequilibrio del sistema eléctrico.

Caso 1: Suplantación o modificación de información en las comunicaciones con el servidor automático de respuesta a la demanda (DRAS) (DR.3).

- **Descripción:** Un ciberatacante obtiene acceso a las comunicaciones entre el DRAS y el sistema de respuesta de demanda del cliente, modificando los mensajes y enviando avisos falsos.

  El mensaje puede causar comportamientos involuntarios y desfavorables en el sistema.

- **Vulnerabilidades:**
  - El sistema permite la modificación de los mensajes sin autorización.
  - El atacante puede obtener acceso físico al sistema de comunicaciones.
  - Los usuarios carecen de visibilidad de las alarmas que se activen debido a amenazas, por ejemplo, las debidas a la presencia de entidades desconocidas con acceso a las comunicaciones.
- **Impacto:**
  - Un mensaje falso puede solicitar al DRAS que reduzca el suministro de energía o que active una acción de respuesta a la demanda errónea.
  - Información falsa puede indicar precios más bajos de energía a los consumidores, pudiendo alentarles a aumentar el consumo de energía durante las horas de alta demanda u horas pico.
  - La empresa y el cliente sufrirán un impacto financiero.
- **Posibles mitigaciones:**
  - Detectar accesos no autorizados a las comunicaciones.
  - Restringir el acceso físico a los componentes de la red de comunicación.
  - Detectar y prevenir intrusiones en las comunicaciones.
  - Verificar los mensajes desde el sistema de respuesta a la demanda del consumidor.
  - Asegurar la integridad de los mensajes mediante firmas digitales para poder verificar la integridad y autenticidad de los mensajes de respuesta a la demanda por parte del consumidor.

Caso 2: Malware personalizado es inyectado en el DRAS (DR.6).

- **Descripción:** Un ciberatacante inyecta un *malware* diseñado especialmente para el sistema automático de respuesta a la demanda y obtiene el control de este, enviando mensajes de respuesta a la demanda para horas valle en horas pico y viceversa.
- **Vulnerabilidades:**
  - El sistema permite cambios no autorizados en el software del DRAS.
  - El sistema no tiene capacidad de detectar cambios no autorizados en el software.

- Acceso innecesario de dispositivos externos a la red de la que el DRAS forma parte.

- **Impacto:**
  - El cliente obtiene carga adicional en horas pico y reducción de carga en horas valle. Como consecuencia, se producen cortes de energía y daños físicos en sistema de energía.
  - El cliente final pierde su confianza en el programa de respuesta a la demanda.
- **Posibles mitigaciones:**
  - Restringir el acceso remoto a los sistemas del DRAS.
  - Restringir el acceso remoto a la red del DRAS.
  - Usar RBAC para limitar el acceso a las partes críticas del DRAS.
  - Realizar una configuración con las funcionalidades y puertos necesarios para que no haya ninguno de ellos sin utilizar, pudiendo constituir una puerta de entrada para ciberatacantes.

Caso 3: Malware personalizado es inyectado en el sistema de respuesta a la demanda del cliente (DR.7).

- **Descripción:** Un ciberatacante inyecta un *malware* en el sistema de respuesta a la demanda de un cliente que ejecuta *Open Automated Demand Response* (OpenADR) [26]. Una vez realizado el ataque, el sistema puede ser controlado de forma remota por el ciberatacante, así como ver modificado su comportamiento. Como consecuencia, el sistema DR comprometido envía mensajes DR incorrectos al DRAS.

  Ejemplo: se envía un mensaje de registro de DR falso al DRAS informando que el cliente puede reducir 500kW, sin ser esto cierto. Alternativamente, el sistema DR comprometido envía un mensaje de informe de DR falso al DRAS. Una vez finalizado el evento de DR, el mensaje falso enviado al DRAS informa sobre la reducción de 500kW por parte del cliente, aunque realmente la reducción fue de 100kW.

- **Vulnerabilidades:**
  - Los parches de software no se comprueban con regularidad para garantizar que estén actualizados, resultando en vulnerabilidades que soportan la inyección de malware personalizado.
  - Acceso innecesario a las funciones del sistema DR del cliente.
  - El sistema asume que las entradas de datos y los cálculos resultantes son precisos con respecto al uso de energía del cliente.
  - Se permiten cambios no autorizados en el software del sistema de DR.

- El usuario tiene poca visibilidad ante cambios no autorizados en el sistema de DR del cliente.

- **Impacto:**
  - Estimación de consumo incorrecta
  - Cortes de suministro potenciales para el operador de red.
  - Impactos financieros en la empresa que ofrece el servicio.
  - Pérdida de confianza en el programa de DR.
- **Posibles mitigaciones:**
  - Restringir el acceso remoto a los sistemas del DRAS.
  - Instalar antivirus en el sistema DR del cliente.
  - Restringir el acceso remoto a la red del cliente.
  - Realizar una configuración con las funcionalidades y puertos necesarios para que no haya ninguno de ellos sin utilizar, pudiendo constituir una puerta de entrada para ciberatacantes.

4.1.6 Generación eléctrica "*Bulk Generation*"

Caso 1: El sistema de gestión de combustible es bloqueado debido a tramas erróneas enviadas por el PLC.

- **Descripción:** Un empleado que tiene acceso a un ordenador portátil con los archivos de configuración de los Controladores Lógicos Programables (PLC) de manejo de combustible, realiza cambios accidentales o intencionados en parámetros que afectan a la lógica de control para deshabilitar el funcionamiento de la bomba del oleoducto.
- **Vulnerabilidades:**
  - No se verifica la modificación de los cambios de configuración, ya que el usuario es capaz de modificar la configuración de puntos críticos.
- **Impacto:**
  - Costes asociados a los recursos necesarios para diagnosticar y reparar la lógica de control.
  - La empresa suministradora obtiene pérdidas debido al bloqueo del combustible.
  - El cliente final sufre una subida de precio del combustible debido a la escasez de producto.
- **Posibles mitigaciones:**
  - Auditar todos los cambios realizados sobre los PLC.
  - Implementar un plan de gestión de los archivos de configuración para reducir la probabilidad de que un ciberatacante pueda comprometer alguna parte del sistema.

- Usar RBAC con el fin de limitar el número de usuarios que pueden actuar sobre los archivos de configuración de los PLC.
- Implantar la obligación de que los cambios de configuración deban ser autorizados, como mínimo, por dos personas.
- Verificar la integridad del archivo de configuración mediante firmas digitales para validar las actualizaciones de software o firmware antes de la instalación o en pleno funcionamiento.

Caso 2: La interfaz HMI del precipitador se deshabilita debido a la introducción de malware a través de una actualización (GEN.6).

- **Descripción:** Un proveedor de servicios de automatización actualiza un HMI para un precipitador electroestático[3] e instala un software mediante una unidad USB que está infectada con *malware*. El *malware* produce el bloqueo del HMI para el precipitador, logrando deshabilitar las capacidades de control del mismo.

  La pérdida de control puede resultar en una violación de las políticas medioambientales. Como consecuencia, el precipitador puede ser retirado de la línea hasta la restauración del sistema.

- **Vulnerabilidades:**
  - Mano de obra no especializada ni capacitada en procedimientos de ciberseguridad puede utilizar una unidad USB con *malware* para conectarse a un recurso de red.
  - El sistema permite la instalación de *malware*.
- **Impacto:**
  - Costes asociados al diagnóstico, reconfiguración y prueba del sistema.
  - Potencial propagación del *malware* hacia otros sistemas de la planta.
- **Posibles mitigaciones:**
  - Entrenar al personal sobre uso de unidades USB y técnicas adecuadas de protección contra *malware*.
  - Comprobación de *malware* antes de realizar la actualización de software.
  - Auditar las conexiones para la realización de cambios en configuración.

[3] El precipitador electroestático es el encargado de reducir la contaminación atmosférica producida por las emisiones de gases de la planta industrial.

4.2. Cuestiones de privacidad en una microrred inteligente

Las *Smart Grids* en el contexto doméstico presentan dos inconvenientes principales:

1. La información personal disponible puede ser sustraída en cualquier momento por un ciberatacante.
2. Los ciberatacantes pueden utilizar mecanismos para la obtención de información no registrada.

Por ello, uno de los puntos más importantes vinculados a la ciberseguridad en este ámbito hace referencia a la información obtenida acerca del usuario, pudiendo identificarse a modo general las actuaciones descritas en la Tabla 1:

Cuestiones de Privacidad	Descripción
Fraude	Atribuir el consumo eléctrico a otra vivienda o localización
Patrones de uso personal	Equipos domésticos instalados en la casa, tiempo que pasa el usuario en casa, tipo de equipos que consumen energía, etc
Vigilancia remota en tiempo real	Similar al anterior punto, con la diferencia de que en este caso se obtiene la información en tiempo real
Usos comerciales	Campañas de marketing y ventas específicas de productos que se detecten que usan los usuarios

Tabla 1. Cuestiones de privacidad en una microrred inteligente.

4.3. Información potencial disponible en una microrred inteligente

Los datos de la microrred inteligente (mediciones de uso de energía, datos de generación e informes sobre el consumo de los equipos del domicilio) proporcionan nuevas fuentes de información personal.

La información personal recopilada tradicionalmente por las empresas de suministro eléctrico es capaz de identificar a un usuario en concreto con sus datos de facturación: nombre, fecha de nacimiento, cuenta bancaria, DNI, etc.

Sin embargo, los equipos de medición de las *Smart Grids* que reflejan el tiempo y la cantidad de energía utilizada, unidos a los elementos tradicionales, proporcionan información adicional sobre el estilo de vida de los consumidores domésticos.

La tecnología integrada por medio de las *Smart Grids* permite a las empresas que proporcionan el servicio un mayor control sobre el uso de energía en el hogar, ayudando a suavizar los aumentos repentinos de la demanda.

Los medidores domésticos muestran el uso de energía por parte de los consumidores y permiten la comunicación inalámbrica bidireccional con las empresas que ofrecen los servicios, pudiendo estas pronosticar la demanda o aumentar el precio de la energía en hora punta. Es por esta razón que los medidores están continuamente asociados al tópico del espionaje dentro de los hogares.

Existen determinados elementos de información dentro de la microrred inteligente que podrían llegar a afectar a la privacidad de los usuarios si no se protegen adecuadamente. Dichos elementos se pueden observar en la Tabla 2:

Elementos de Información	Descripción
Nombre	Parte Responsable de la cuenta
Dirección	Localización del servicio
Número de cuenta	Identificador único e intransferible para el usuario
Datos de Facturación	Factura actual asociada a la cuenta
Histórico de Datos	Lecturas de medidores pasadas, antiguas facturas
Red Local Doméstica	Red usada por los dispositivos que forman parte de la microrred
Hábitos	Obtención de datos sobre el usuario de su vida personal: cuando la casa está ocupada o desocupada, cuando está durmiendo
Lectura de Equipos de Medición	Consumo de energía expresado en kWh
IP de los Equipos de Medición	La dirección IP del equipo
Proveedor	Identificar la parte que proporciona la energía al usuario
Otras soluciones de Generación	Obtener información sobre la presencia de dispositivos de generación y dispositivos de almacenamiento, estado actual de la instalación, patrones de uso

Tabla 2. Información disponible en una microrred inteligente.

4.4. Ejemplos de ataques comunes

Denegación de servicio (DoS)

Los ataques DoS son un conjunto de ofensivas que tienen como objetivo el bloqueo de recursos (como la memoria, la cantidad de procesos o el ancho de banda disponible). Se pueden iniciar desde el interior de una red tras la intrusión inicial por medio de un nodo vulnerable.

ARP spoofing y desbordamiento de MAC

El protocolo de resolución de direcciones (ARP) se utiliza asiduamente para proporcionar un mapeo entre la capa de red y la capa de enlace de datos.

Las tramas de datos del paquete IP solo se pueden enviar si las direcciones físicas de los host destinatarios son conocidas. Para recibir este mensaje, se emite una solicitud ARP en la red que debe ser respondida por el equipo con la dirección IP solicitada.

En ARP, la identidad del remitente no se puede autentificar y, por lo tanto, el mapeo que se realiza es susceptible de alteraciones intencionadas. Por ende, los paquetes pueden ser transmitidos al host incorrecto y utilizarse para recopilar o alterar sus datos, así como efectuar ataques DoS.

Ataque *Man in the Middle* (MiTM)

En un ataque MiTM, el ciberatacante se sitúa entre dos nodos que se comunican, haciéndoles creer que están hablando directamente entre sí. Por tanto, el ciberatacante podría mantener una comunicación cifrada o no con ambas partes con la capacidad añadida de inyectar o descartar paquetes e, incluso, alterar otros nuevos.

Réplica

Al usar ataques MiTM, un atacante puede grabar la comunicación entre los nodos y reproducirla para ocultar el comportamiento real del sistema. Estos paquetes reproducidos pueden ocasionar errores o un comportamiento indefinido en el extremo receptor.

Inyección

Usando el ataque MiTM, el atacante puede inyectar o alterar lecturas y comandos en las comunicaciones en tiempo real. Este ataque es muy problemático si lo ejecuta un usuario experimentado, ya que es difícil de detectar y puede tener un efecto potencialmente significativo sobre el sistema.

Un ciberatacante puede manipular la medición de equipos localizados en lugares remotos, así como suprimir o inyectar comandos de control entre dos nodos.

Secuestro de sesión

En el secuestro de sesiones, el atacante se hace cargo de una sesión válida.

El ciberatacante, al no tener los medios para establecer una sesión válida, intercepta y toma el control de un nodo autorizado que ha establecido una conexión legítima, utilizando esta sesión para realizar comunicaciones con la víctima.

4.5. Histórico de ataques

Si bien a lo largo del documento se han expuesto los riesgos asociados a las *Smart Grids*, con el fin de demostrar la realidad acerca de las amenazas de ciberseguridad presentes en el sector eléctrico, a continuación, en la Figura 7 se muestran los ciberataques más relevantes ocurridos en este ámbito entre 2015 y 2021:

Figura 7. Histórico de Ataques más relevantes en el sector eléctrico [27], [28], [29].

Capítulo 5

Evaluación de riesgos en una microrred inteligente

Para realizar un análisis de amenazas completo es necesario estudiar un caso concreto, puesto que los patrones de ataque pueden ser muy diferentes en función de los objetivos que se quieran conseguir con el ciberataque.

En la metodología del presente proyecto se lleva a cabo la evaluación de riesgos conforme al siguiente diagrama, representado en la Figura 8:

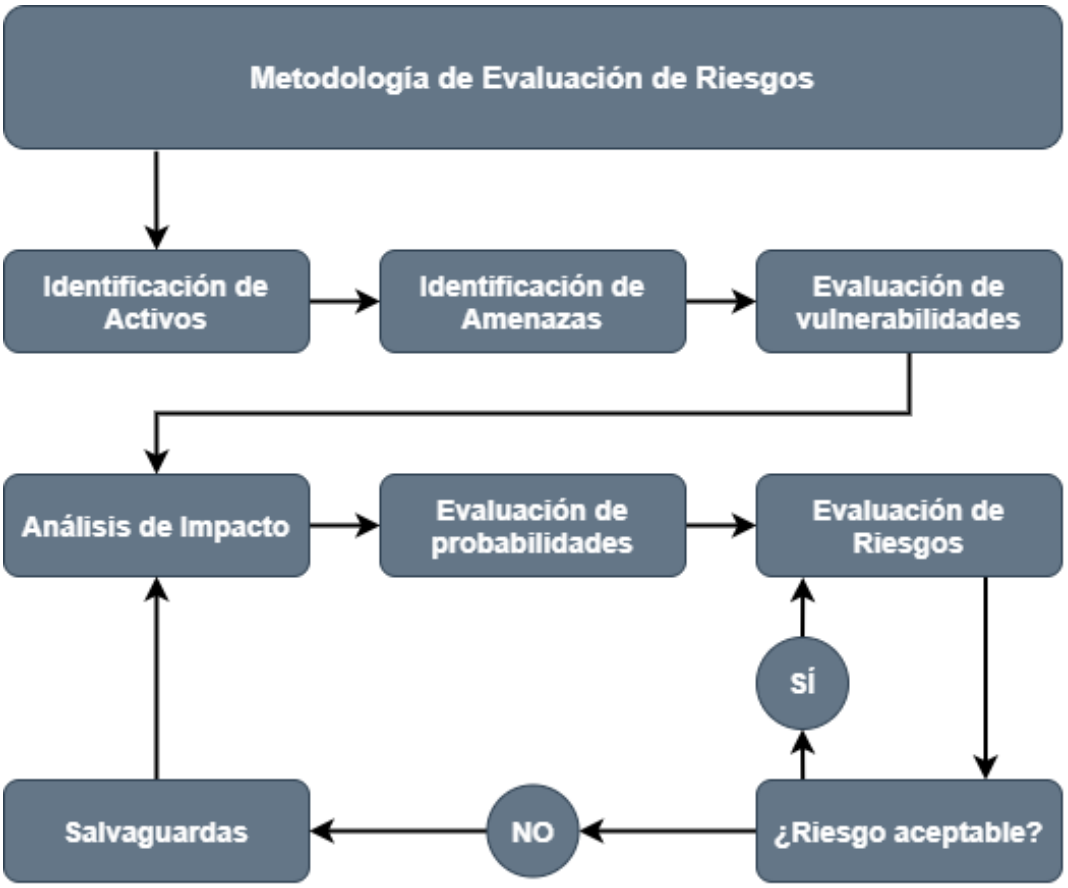

Figura 8. Metodología de Evaluación de riesgos (Fase Inicial).

- Identificación de activos: Es necesario conocer los activos del sistema y las interacciones con agentes externos y entre ellos.
- Identificación de las amenazas que puedan afectar a los activos.
- Evaluación de vulnerabilidades que podrían verse explotadas por las amenazas identificadas en el paso anterior.

- Análisis del impacto que podría producirse si la amenaza afectara al activo (impacto sobre la confidencialidad, la integridad y la disponibilidad).
- Evaluación de las probabilidades de que las diferentes amenazas pudieran llegar a explotar las vulnerabilidades de los activos.
- Evaluación de los riesgos que podría conllevar que el activo se viera afectado, teniendo en cuenta la probabilidad y el impacto.
- ¿Es el riesgo aceptable? Es necesario determinar qué nivel de riesgo residual es aceptable.
- En caso de que el riesgo no fuera aceptable, será necesario introducir un mecanismo de protección o salvaguarda.

La evaluación de riesgos es un proceso continuo que debe actualizarse atendiendo a las nuevas amenazas que puedan aparecer. Por ello, el proceso descrito en el diagrama de Figura 8 constituye la primera fase de la evaluación de riesgos.

La siguiente fase es la de implementación y evaluación de las salvaguardas, representada en la Figura 9:

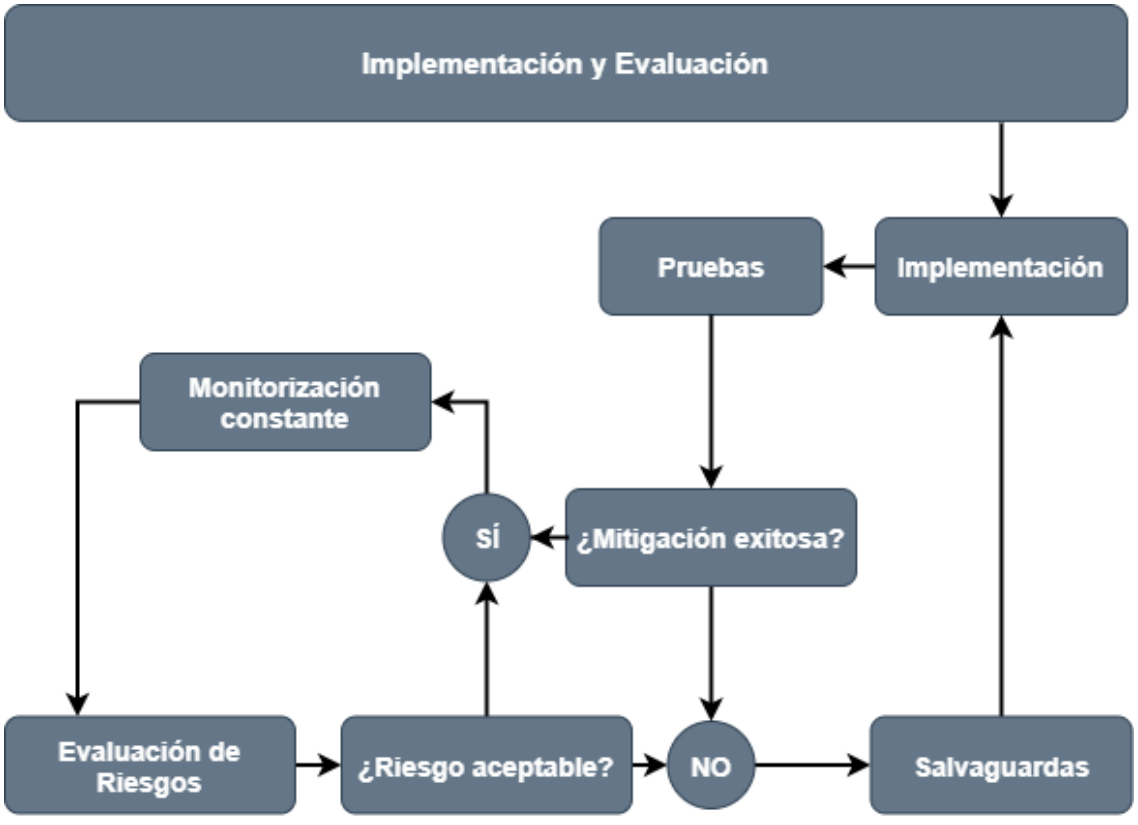

Figura 9. Proceso de implementación de salvaguardas.

- Implementación inicial del mecanismo de protección o salvaguarda en el sistema bajo análisis.

- Realización de pruebas del sistema junto con el mecanismo de protección para asegurar que el funcionamiento es el correcto. Dependiendo de la aplicación, los requerimientos del sistema serán distintos; por ejemplo, la latencia de las comunicaciones podría verse afectada por el propio sistema de protección.
- ¿Mitigación exitosa? Es necesario determinar si la mitigación ha sido exitosa.
- En caso de que la mitigación haya sido exitosa:
  - Monitorización constante
  - Evaluación de riesgos
  - ¿Riesgo aceptable?
    - Si el riesgo es aceptable, se continúa monitorizando y evaluando riesgos hasta que el riesgo, en algún momento, deje de ser aceptable.
    - Si el riesgo no es aceptable, hay que introducir o modificar un mecanismo de protección o salvaguarda.
- Si la mitigación no ha sido exitosa, se debe introducir o modificar un mecanismo de protección o salvaguarda.

5.1. Contexto

En este caso, el contexto bajo estudio es el siguiente:

1. Instalación renovable para una industria con una potencia instalada mayor de 100 kW.
2. La instalación consigue cubrir todo el gasto energético durante el horario de operación de la industria.
3. Trabajador encargado de la gestión y control de la instalación.
4. Instalación del equipo de control de la microrred en el interior de la industria.
5. Instalación de paneles fotovoltaicos en el tejado de la industria, con una compleja accesibilidad.
6. Equipo de control de la microrred conectado a la red inalámbrica de la industria.
7. Grandes pérdidas monetarias debido a parada del sistema.

5.2. Modelo de Amenaza

En la microrred inteligente objeto de estudio es de gran importancia especificar qué actores participan, cuáles son sus motivaciones y qué comportamiento malicioso se puede esperar de estos. Hay que destacar que, cuanto más estricto sea el modelo de amenazas, más seguro será el sistema.

Puesto que la mayor parte de los ciberataques que están sufriendo las empresas en los últimos años provienen de los propios empleados (ingeniería social) [30], se ha decidido partir de este hecho para especificar el presente modelo de amenaza.

En este modelo de amenaza intervienen tres tipos de actores:

- **Trabajador descontento con la empresa que gestiona la microrred:** Operario encargado de la gestión de la microrred mediante el HMI que busque conocer más elementos del sistema inteligente realizando escaneos de red y otros tipos de ataque, con el fin de obtener información crítica e inaccesible desde el HMI.
- **Trabajador descontento con la empresa externa que ha realizado la instalación del sistema inteligente de gestión de la microrred:** En este caso, existen dos perfiles. En primer lugar, el ingeniero de software que dispone de mecanismos para realizar actualizaciones de firmware del sistema inteligente de gestión de la microrred y, en segundo lugar, el ingeniero de control que realiza comunicaciones mediante el estándar IEC61850.
- **Prosumidor:** Ingeniero de operaciones de la industria donde se encuentra instalada la microrred inteligente que puede realizar transacciones de compra/venta de energía y, posteriormente, denegar dichas transacciones, lo que implicaría pérdidas para la empresa.

5.3. Identificación de activos y amenazas con C4 Model + STRIDE

Para poder identificar los diferentes activos involucrados en la microrred inteligente anteriormente descrita, ha sido necesaria la realización de un C4 Model [3] que describa el sistema que se encuentra realizando la gestión de la microrred. De este modo, se puede obtener una visión completa de cada parte de este y de cómo interactúan los diferentes elementos externos, ya sean personas físicas u otros sistemas.

El sistema objeto de estudio está compuesto por:

- El controlador de la microrred, que se encuentra instalado en una Raspberry Pi 4 de 8 GB RAM.
- El controlador de la estación meteorológica, que se encuentra instalado en un ESP32.

En la Figura 10 se pueden observar los agentes externos que interactúan con el sistema:

- **Cliente IEC 61850 (Empresa Externa)**: Este agente externo pertenecerá a la empresa que ofrece el servicio de gestión de la microrred, realizando comunicaciones cuando sea necesario llevar a cabo algún mantenimiento mediante el estándar de comunicación IEC 61850.
- **Prosumidor:** Este agente externo pertenece a la empresa que acoge la instalación y se encarga de realizar ofertas de compra/venta de energía.
- **Operario Industrial (Mantenimiento de Microrred**): Este agente externo pertenece a la industria que acoge la instalación. Es el encargado de monitorizar el funcionamiento del sistema mediante el HMI y actuar sobre este si hubiese alguna situación fuera de lo normal.
- **Desarrollador (Empresa Externa):** Este agente externo pertenece a la empresa que ofrece el servicio y es el encargado de realizar las actualizaciones pertinentes sobre el firmware instalado en el equipo de gestión de la microrred.

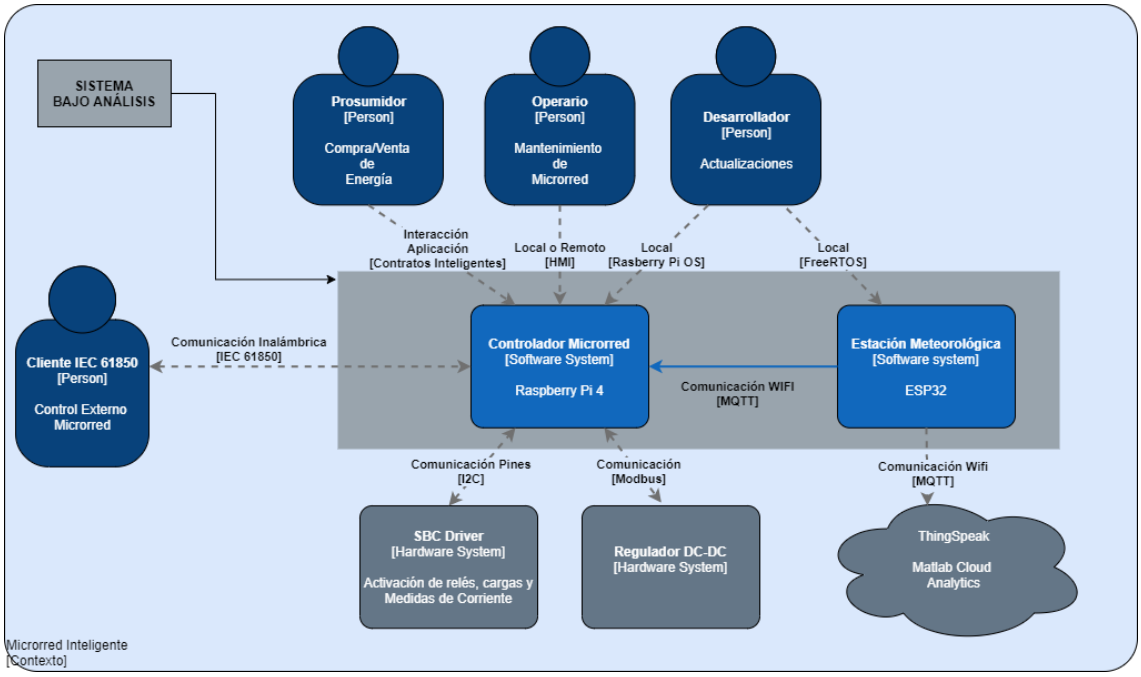

Figura 10. C4 Model General de sistema inteligente de control de Microrred.

Sobre el C4 Model de la Figura 11 se han situado las diferentes amenazas, realizando el análisis STRIDE:

- Spoofing: Suplantación de identidad de un usuario del sistema.
- Tampering: Modificación malintencionada de los datos del sistema.
- Repudiation: Denegación de la ejecución de una acción.
- Information Disclosure: Acceso a información del sistema a usuarios que no deberían tenerlo.
- Denial of Service: Denegación de un servicio del sistema.
- Elevation of privilege: Usuario que obtiene acceso con privilegios y puede realizar acciones que dañen o destruyan el sistema.

En prácticamente todas las interacciones, la comunicación entre las partes es bidireccional, por lo que se han modelado las amenazas en la misma interacción, pero en diferentes direcciones.

Por otro lado, es necesario destacar que las amenazas que se han tenido en cuenta son únicamente las que se producen en las interacciones entre agentes externos y los diferentes activos del controlador de la microrred. Por ello, en la presente evaluación de amenazas, no se profundiza más en el análisis. No obstante, en el Apéndice A - C4 Model de bajo nivel se adjuntan los C4 Model de bajo nivel del sistema.

Además, con el fin de poder relacionar mejor las amenazas del C4 Model con la tabla Excel incluida en el siguiente apartado (5.4. Cuantificación de riesgo con Magerit), se ha situado un número o código de amenaza al lado de cada una de ellas.

El controlador de la microrred es el encargado de gestionar las distintas mediciones obtenidas por los sensores desplegados en la instalación. Sobre el controlador se ejecuta *Robot Operating System* (ROS) [31], actuando de punto central en el flujo de información.

Como se puede observar en la Figura 11, ROS interactúa con:

- **Hardware desplegado en la instalación**, con el objetivo de activar/desactivar interruptores físicos para, por ejemplo, realizar una gestión de las cargas como método para dar respuesta a la demanda.
- **Estación meteorológica**: Adquiere datos meteorológicos como presión, humedad, temperatura, velocidad del viento, irradiancia de los paneles fotovoltaicos, etc.
- **Node-RED** [32]: Envía las consignas activadas en el HMI por el operario de mantenimiento hacia ROS. Node-RED es un software de programación visual que se utiliza para comunicar dispositivos hardware, aplicaciones gráficas y servidores de internet.

- **Cliente IEC 61850**: Envía comunicaciones hacia ROS mediante el estándar IEC 61850, con consignas de actuación por parte de la empresa utilitaria.
- **Servidor IEC 61850**: Una vez recibe las comunicaciones, el servidor IEC 61850 realiza la traducción de los comandos de control al lenguaje utilizado por ROS. De igual modo, si el cliente IEC 61850 pide información sobre el estado de la microrred, ROS utiliza este servidor para traducir los datos y enviárselos en formato IEC 61850.
- **Hyperledger Fabric** [33]**:** Interactúa internamente con ROS para informarle de las actuaciones de compra/venta de energía que quiere efectuar el gestor de la instalación. Es un blockchain diseñado e implementado en la microrred con el fin de realizar transacciones de energía seguras velando por la integridad, la confidencialidad y el no repudio de las operaciones.

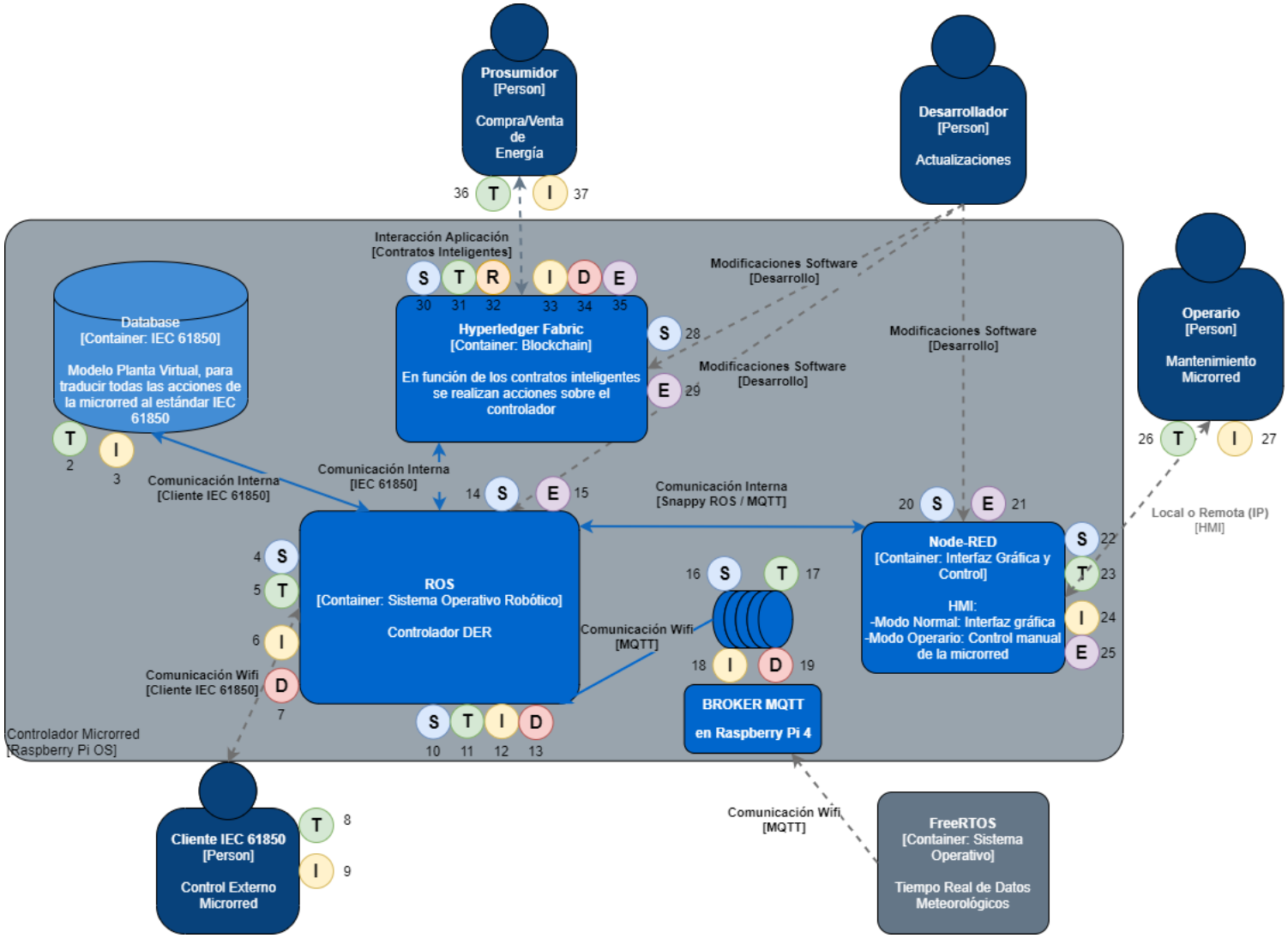

Figura 11. C4 Model + STRIDE de controlador de microrred.

A continuación, se adjunta la Figura 12, donde se puede observar el funcionamiento del sistema de un modo más profundo:

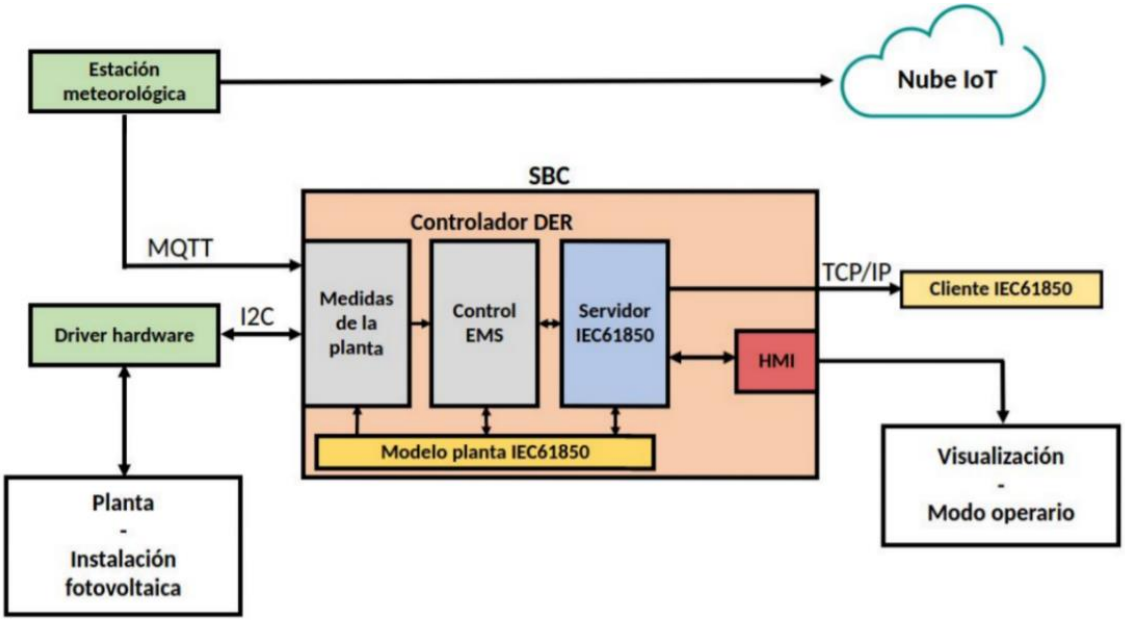

Figura 12. Sistema inteligente de gestión de la microrred [33].

Por otro lado, se encuentra la estación meteorológica, la cual obtiene medidas de irradiancia, presión, temperatura, humedad, velocidad y dirección del viento. Estos datos son enviados mediante el protocolo *Message Queue Telemetry Transport* (MQTT), del que se hablará con mayor detalle en el siguiente capítulo.

Este protocolo está basado en la pila TCP/IP para establecer la comunicación y ofrece un servicio de mensajería de publicador/suscriptor conectados a un *broker* que se encarga de transferir la información entre los partícipes.

En la Figura 13 se puede observar cómo el sistema de tiempo real FreeRTOS [35] instalado en la estación meteorológica envía datos al *broker* MQTT localizado en la Raspberry Pi 4. Una vez que el *broker* recibe la información, se encarga de distribuirla a los suscriptores del *topic* creado por el publicador (estación meteorológica).

En este caso, hay dos suscriptores: ROS y ThingSpeak [36]. Los datos enviados a ROS sirven para realizar actuaciones directas sobre el EMS del controlador de la microrred mientras que los enviados a ThingSpeak se procesan por medio de inteligencia artificial para obtener predicciones meteorológicas. Por ello, es importante conseguir que la integridad, la confidencialidad y la disponibilidad se cumplan, ya que, de lo contrario, las predicciones meteorológicas podrían verse afectadas, obteniendo como consecuencia una mala decisión (por ejemplo, en la compra/venta de energía en el blockchain de Hyperledger Fabric [33]).

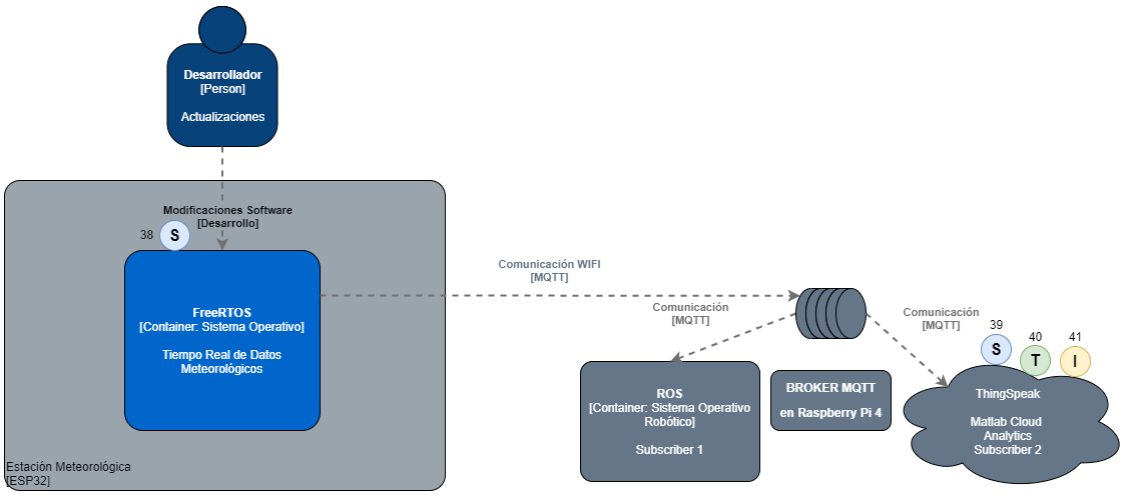

Figura 13. C4 Model + STRIDE de Estación Meteorológica.

5.4. Cuantificación de riesgo con Magerit

Magerit [4] es una metodología de análisis y gestión de riesgos de sistemas de información elaborada por el Consejo Superior de Administración Electrónica de España. Ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para, posteriormente, utilizar mecanismos de protección que permitan minimizar dichos riesgos.

Se ha utilizado esta metodología para poder obtener el nivel de riesgo de las amenazas planteadas en el punto 5.3. Identificación de activos y amenazas con C4 Model + STRIDE.

En el presente apartado, se detallará el proceso que se ha seguido para obtener el nivel de riesgo. Si se requiere, en el Apéndice B - Tablas de evaluación de riesgos se adjuntan las tablas completas correspondientes a la obtención de los niveles de riesgo del análisis.

A continuación, en la Tabla 3, se detallan las escalas utilizadas para medir el impacto, la probabilidad y el riesgo:

ESCALAS		
impacto	**probabilidad**	**riesgo**
5: muy alto	5: prácticamente seguro	5: crítico
4: alto	4: probable	4: importante
3: medio	3: posible	3: apreciable
2: bajo	2: poco probable	2: bajo
1: muy bajo	1: muy raro	1: despreciable

Tabla 3. Escalas de impacto, probabilidad y riesgo.

Se puede observar cómo las escalas van desde el 1 [impacto (muy bajo), probabilidad (muy baja o prácticamente imposible) y riesgo (despreciable)] hasta el 5 [impacto (muy alto), probabilidad (muy alta o prácticamente seguro que ocurra el acto) y riesgo (muy crítico)].

Una vez se han especificado las distintas escalas que se van a utilizar en el análisis, se pueden comenzar a realizar los cálculos del impacto y del riesgo.

El cálculo del impacto se obtiene de la siguiente forma:

$$Impacto = \frac{Impacto\ (Integridad) + Impacto\ (Confidencialidad) + Impacto\ (DoS)}{3}$$

Posteriormente, se debe realizar la media de los impactos que pudiera causar la amenaza sobre la integridad, la confidencialidad y la denegación de servicio del activo en cuestión.

La Tabla 4 recoge la siguiente información:

- **Código de Amenaza:** Especifica el número que aparece junto a cada amenaza sobre el C4 Model.
- **Activo:** Se refiere al componente del sistema que se está analizando.
- **Amenazas STRIDE:** *Spoofing*, *Tampering*, *Repudiation*, *Information Disclosure* y *Denial of Service*.
- **Código MAGERIT:** Código de amenaza del Libro II: Catálogo de elementos [4].
- **I:** Impacto sobre la integridad del activo.
- **C:** Impacto sobre la confidencialidad del activo.
- **D:** Impacto sobre la denegación de servicio que se le pueda realizar al activo.
- **Impacto:** Columna que especifica la media de los impactos anteriores y presenta un color determinado. El código de colores utilizado se expone en la Tabla 5.

Código Amenaza	Activo	Amenazas STRIDE	Código MAGERIT	I	C	D	Impacto
16	Comunicación Wifi MQTT de FreeRTOS hacia Broker MQTT	Spoofing	[A.5]	5	5	5	**5**
17	Comunicación Wifi MQTT de FreeRTOS hacia Broker MQTT	Tampering	[A.15]	5	3	1	**3**
18	Comunicación Wifi MQTT de FreeRTOS hacia Broker MQTT	Information Disclosure	[A.14]	3	5	1	**3**
19	Comunicación Wifi MQTT de FreeRTOS hacia Broker MQTT	Denial of Service	[A.24]	1	1	5	**3**

Tabla 4. Ejemplo de obtención de impacto total.

En la Tabla 5 se puede observar la matriz utilizada para la cuantificación de riesgos así como el código de colores empleado.

riesgo		***Impacto***				
		1	2	3	4	5
Probabilidad	5	M (5)	A (10)	A (15)	MA (20)	MA (25)
	4	B (4)	M (6)	A (12)	A (16)	MA (20)
	3	B (3)	M (7)	M (9)	A (12)	A (15)
	2	B (2)	B (4)	M (6)	M (8)	A (10)
	1	B (1)	B (2)	B (3)	B (4)	M (5)

Tabla 5. Matriz de riesgos.

Por último, una vez obtenido el impacto total, es necesario precisar la probabilidad de que esa amenaza pueda llegar a producirse.

Con la probabilidad y el impacto, puede obtenerse el riesgo:

$$Riesgo = Impacto \cdot Probabilidad$$

En la Tabla 6 se puede observar la siguiente información:

- **Código de Amenaza:** Especifica el número que aparece junto a cada amenaza sobre el C4 Model.
- **Activo:** Se refiere al componente del sistema que se está analizando.
- **Amenazas STRIDE:** Spoofing, Tampering, Repudiation, Information Disclosure y Denial of Service.
- **Código MAGERIT:** Código de amenaza correspondiente al Libro II: Catálogo de elementos [4].
- **I:** Impacto total sobre el activo.
- **P:** Probabilidad de que pueda llegar a producirse el ataque.
- **Riesgo:** Columna que especifica el nivel de riesgo conforme al código de colores utilizado en la Tabla 5.
- **Posible mitigación:** Indica el mecanismo de protección o salvaguarda principal para mitigar esa amenaza.
- **Riesgo final:** Columna que especifica el nivel de riesgo conforme al código de colores utilizado en la Tabla 5 una vez se ha implementado el mecanismo de protección.

Código Amenaza	Activo	Amenazas STRIDE	Código MAGERIT	I	P	Riesgo	Posibles Mitigación	Riesgo Residual
16	Comunicación Wifi MQTT de FreeRTOS hacia Broker MQTT	Spoofing	[A.5]	5	3	**15**	Control de acceso con roles	**4**
17	Comunicación Wifi MQTT de FreeRTOS hacia Broker MQTT	Tampering	[A.15]	3	4	**12**	Encriptar comunicación	**2**
18	Comunicación Wifi MQTT de FreeRTOS hacia Broker MQTT	Information Disclosure	[A.14]	3	4	**12**	Encriptar comunicación	**2**
19	Comunicación Wifi MQTT de FreeRTOS hacia Broker MQTT	Denial of Service	[A.24]	3	4	**12**	Detectar comandos anómalos	**3**

Tabla 6. Ejemplo de obtención de nivel de riesgo.

En el presente capítulo se ha expuesto una metodología de identificación de activos, evaluación de amenazas y cuantificación de riesgos. La valoración del impacto sobre la confidencialidad, la integridad y la disponibilidad de los activos, al igual que la cuantificación de sus respectivos riesgos, es una tarea que debe perfeccionarse conforme el profesional que realice este análisis obtenga un mayor grado de experiencia en este campo.

Los resultados obtenidos indican la necesidad de introducir mecanismos de seguridad en los diferentes apartados del EMS de la microrred eléctrica. Esto es debido a que el diseño que se ha realizado del EMS no ha tenido en cuenta los riesgos de ciberseguridad. El único elemento de la microrred que permite reducir la probabilidad de que se efectúen ciertas amenazas es el blockchain desarrollado en Hyperledger Fabric.

Capítulo 6

Seguridad en la comunicación MQTT

El protocolo MQTT fue desarrollado por Andy Stanford-Clark, de IBM, y Arlen Nipper, de Arcom. Aunque originalmente fue diseñado para las comunicaciones remotas en cualquier campo, ha experimentado una gran aceptación en aplicaciones de IoT por su sencillo modelo de comunicación para dispositivos con recursos limitados como el ESP32 de Espressif [37] (un dispositivo muy extendido en el mundo de IoT) y también en redes que disponen de un ancho de banda limitado con alta latencia.

En 2013, un grupo de empresas se reunieron para estandarizar el protocolo bajo el nombre de OASIS MQTT TC [38]. Cisco, IBM o Microsoft son algunas de las compañías que se encuentran dentro de este proyecto.

OASIS MQTT TC actualmente se encarga de especificar un estándar para este protocolo de comunicación con compatibilidad con MQTT V3.1. Asimismo, aporta documentación de casos de uso, buenas prácticas y orientación para la aplicación del protocolo.

En la Figura 14, se puede observar un ejemplo de comunicación con este protocolo en el que los publicadores y los suscriptores intercambian mensajes a través de un *broker* que utiliza paquetes de control MQTT.

Los publicadores obtienen datos de cualquier tipo, como el de una estación meteorológica con diversos sensores para diferentes aplicaciones. Posteriormente, publican estos datos hacia el *broker* (“Publish”). Los datos que almacena el *broker* provenientes de los publicadores se organizan en forma de temas *topics*.

En el otro lado de la comunicación se encuentran los suscriptores, que reciben avisos del *broker* cada vez que se hayan publicado nuevos datos sobre el *topic* elegido.

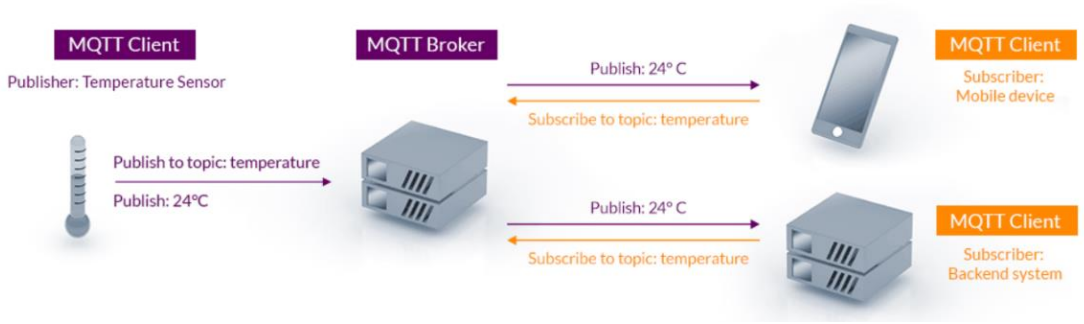

Figura 14. Ejemplo general de comunicación MQTT [38].

La Figura 15 muestra los diferentes paquetes de la comunicación MQTT: CONNECT, CONNACK, PUBLISH, PUBACK, SUBSCRIBE, SUBACK y DISCONNECT. A su vez, se puede apreciar cómo los clientes notifican su estado actual al *broker* mediante los paquetes PINGREQ (solicitud) y PINGRESP (respuesta). Cabe destacar que el protocolo mencionado permite tres niveles de calidad de servicio (QoS), los cuales pueden utilizarse en la comunicación en función de los requerimientos del sistema.

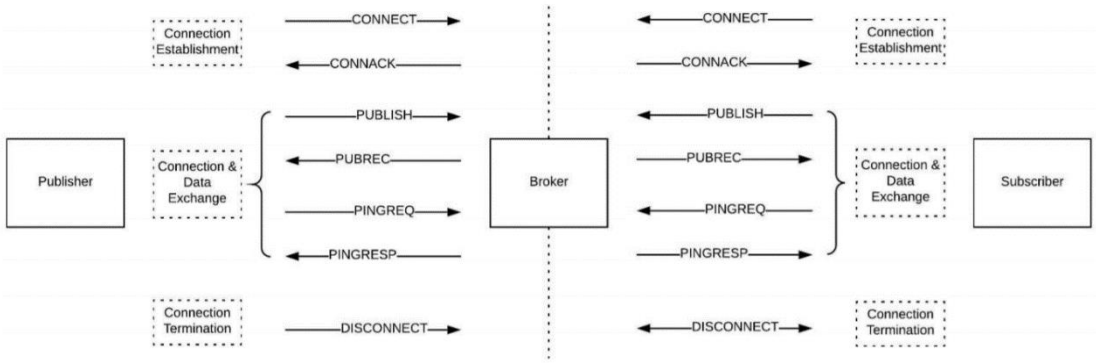

Figura 15. Ejemplo comunicación MQTT con detalle.

Son muchos los paquetes que se intercambian entre los clientes y el *broker.* Por esta razón, se hace necesario identificar correctamente las diferentes vulnerabilidades para poder implementar mecanismos de protección sobre la comunicación MQTT.

6.1. Estructura de ataque

En la Figura 16 se puede observar el patrón de ataque que suelen experimentar por norma general las *Smart Grids*, pudiendo extrapolarse a los sistemas de automatización y comunicación industrial:

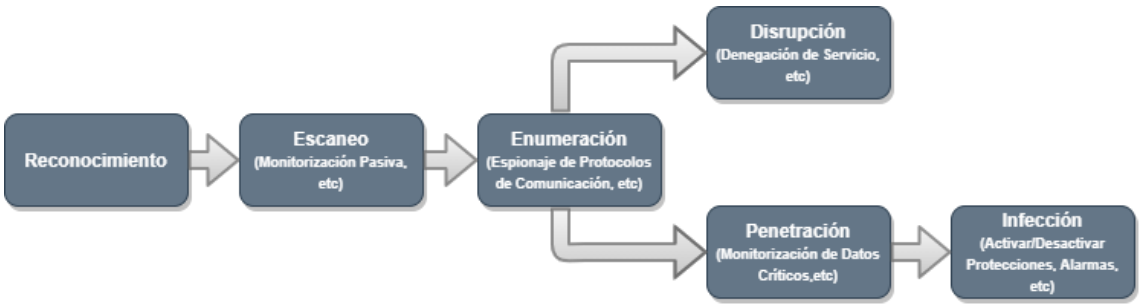

Figura 16. Estructura de Ataque.

Reconocimiento

El atacante intentará obtener toda la información posible sobre el sistema que quiere atacar (elementos de información sobre el sistema o sobre la compañía que lo gestiona), sin ser intrusivo.

Escaneo

Este proceso es utilizado por empresas auditoras para obtener informes de vulnerabilidades.

Desde el punto de vista de un atacante, sería posible identificar los dispositivos y hosts de una red. Además, se podría obtener información sobre qué dispositivo es el maestro y cuál el esclavo en dicha red.

Las empresas llevan a cabo dos tipos de escaneos: el de caja blanca y el de caja negra [39]. Este último es el que más se asemeja a la actuación de un ciberatacante, dado que se les proporciona un solo elemento básico de información (como el nombre de la empresa o la IP de un dispositivo) y, a partir de ese punto, comienzan el proceso de escaneo.

La ausencia de sistemas de autentificación o encriptación en los protocolos de comunicación o dispositivos del sistema puede generar amenazas potenciales para las *Smart Grids* realizando este paso.

Enumeración o recopilación

Este proceso se realiza con el fin de obtener las credenciales necesarias para acceder como superusuario al sistema (elevación de privilegios).

Se pueden encontrar datos como el usuario, el histórico de credenciales, las direcciones IP del maestro o del esclavo, así como patrones de uso personales como se verá en apartados posteriores.

En esta etapa del proceso de ataque aún no se podría realizar un ataque intrusivo en el sistema, aunque las diferentes vulnerabilidades que pueda presentar el protocolo de comunicación empleado pueden proporcionar una ruta para obtener datos. Por ello, es importante realizar un cifrado de estas comunicaciones.

Disrupción

En este proceso se pueden llevar a cabo ataques de denegación de servicio (DoS) tras realizar un análisis de la red del sistema bajo ataque. Para algunos sistemas, los límites de latencia son críticos y pueden ser aumentados por el incremento de tráfico introducido por los paquetes enviados al mismo.

Los efectos de la interrupción del sistema pueden impedir que los comandos de control o las mediciones se transmitan con éxito. Además, este tipo de ataque puede utilizarse para causar distracción a los operadores de control al activarse un gran número de alarmas, causando una desviación de la atención con respecto a otras actividades más intrusivas y críticas dentro del sistema.

Penetración

Una vez ejecutados los pasos anteriores de identificación de las aplicaciones y los dispositivos en la red bajo ataque, se puede realizar una penetración en el sistema.

Un tipo penetración común en las *Smart Grids* es el ataque MiTM. El atacante se coloca en el medio de las comunicaciones entre dos nodos sin que estos detecten su presencia, mientras que intercepta todo el tráfico disponible en las comunicaciones. Un ataque perfecto permite al ciberatacante descartar, añadir o manipular los paquetes que se estén enviando, además de obtener toda la información presente en la comunicación.

Infección

Tras penetrar en el sistema, el ciberatacante podría inyectar *malware* para conseguir su bloqueo, restringir el acceso a determinadas partes, etc.

6.2. Despliegue de estación de pruebas

La estación de pruebas en la que se explotarán las vulnerabilidades descubiertas en el capítulo anterior presenta la estructura de la Figura 17.

La red desplegada dispone de tres dispositivos:

- Estación Meteorológica (Publicador): ESP32 de Espressif [37].
- Mosquitto *Broker*: Raspberry Pi 4 Model B 8 GB Ram [41].

- Suscriptor: Raspberry Pi 4 Model B 8 GB Ram.

La estación (IP: 192.168.11.6) se encarga de leer datos meteorológicos de diferentes sensores localizados en el exterior y situados en una localización próxima a los paneles fotovoltaicos. Desde la estación meteorológica se envían los *topics* al *broker* mosquitto (IP: 192.168.11.2), que distribuye los diferentes *topics* a los clientes que se hayan suscrito a cada uno de estos. Por último, se realizará la suscripción de un cliente externo (IP: 192.168.11.3) para obtener los datos publicados por la estación meteorológica.

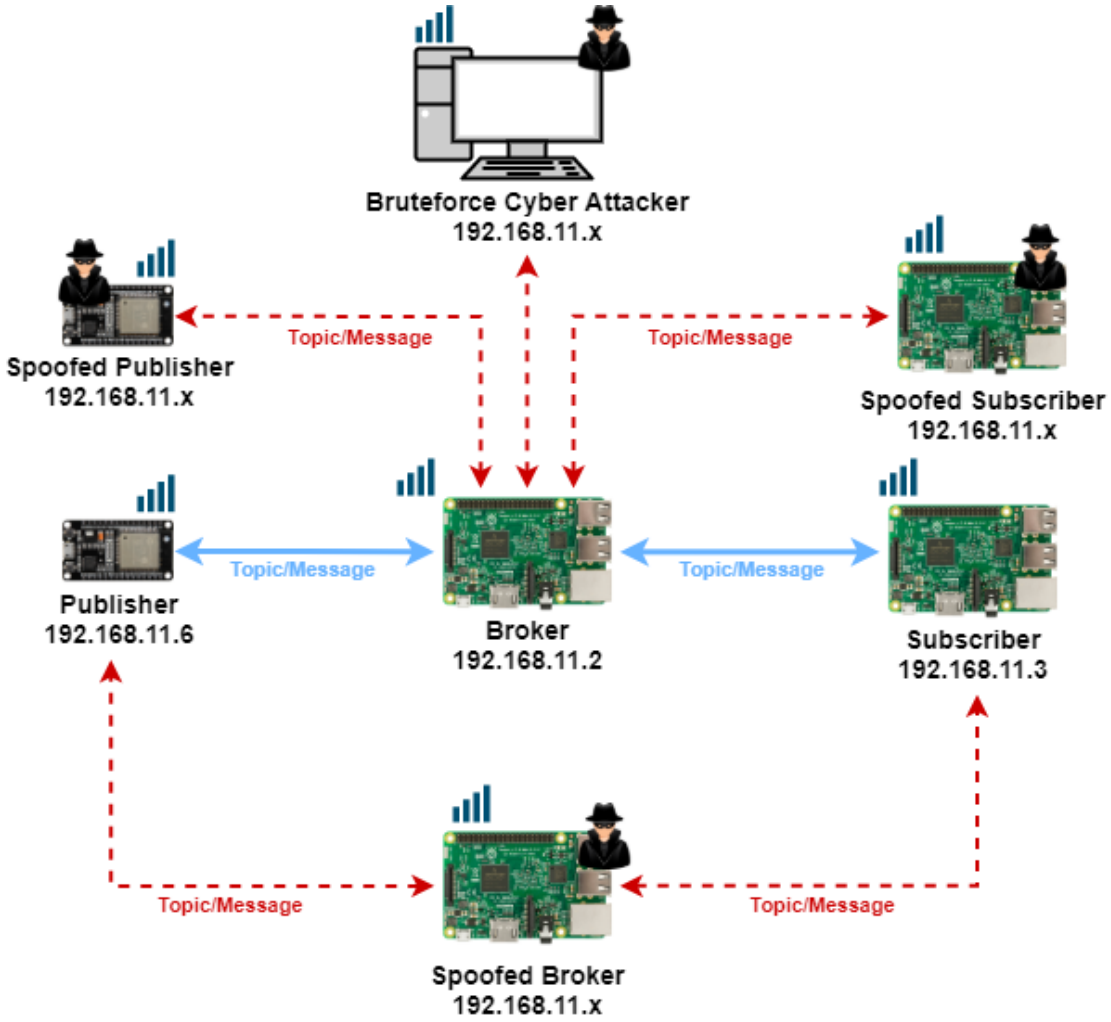

Figura 17. Gráfico red de pruebas.

6.2.1 Comunicación entre clientes y *broker*

Publicación

```
>> mosquitto_pub -d -h 192.168.11.2 -p 1883 -t "esp32/humidity" -m "52" -u "mqtt-explorer" -P "1234" -i "raspberry"
```

- -h: IP del *broker.*
- -p: Puerto mediante el que se va a realizar la comunicación.
- -t: *Topic* al que el cliente quiere subscribirse.
- -m: Dato que se envía a un *topic.*
- -u: Usuario.
- -P: Contraseña.
- -i: Client_ID, en caso de que se quiera indicar uno, de lo contrario, se puede dejar por defecto y lo asignará automáticamente el *broker*.

Como se puede observar en el apartado -m, se está publicando una humedad con un valor de 52.

Suscripción

Para suscribirse a un *topic*, se utiliza el siguiente comando:

```
>> mosquitto_sub -d -h 192.168.11.4 -p 1883 -t "esp32/humidity" -u "mqtt-explorer" -P "1234" -i "raspberry"
```

- -h: IP del *broker.*
- -p: Puerto mediante el que se va a realizar la comunicación.
- -t: *Topic* al que el cliente quiere subscribirse.
- -u: Usuario.
- -P: Contraseña.
- -i: Client_ID, en caso de que se quiera indicar uno, de lo contrario, se puede dejar por defecto y lo asignará automáticamente el *broker*.

Cliente mqtt-explorer

Con el fin de obtener la información de un modo más claro se utiliza un cliente de código de abierto que dispone de interfaz gráfica. El cliente que se ha utilizado es mqtt-explorer [42] y dispone de una interfaz gráfica que facilitará el procesamiento de la información para observar las consecuencias de las diferentes pruebas de penetración que se detallarán en los siguientes apartados.

En la Figura 18 y en la Figura 19 se puede observar la interfaz de la que dispone mqtt-explorer:

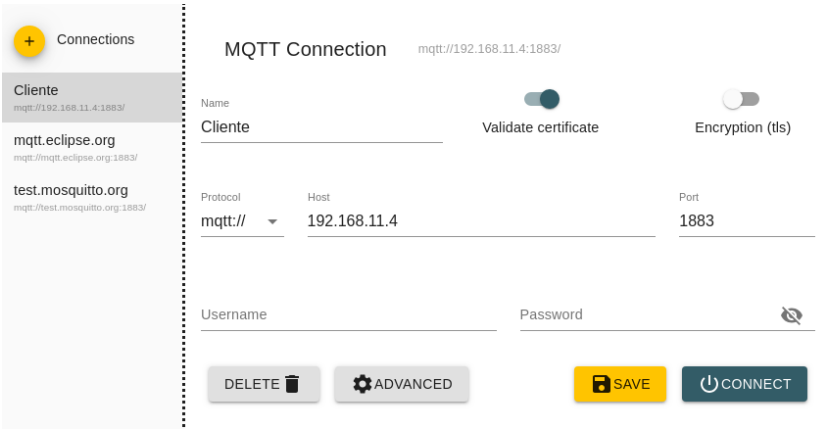

Figura 18. Interfaz MQTT Explorer 1.

La Figura 18 introduce las características de la conexión MQTT:

- IP del *broker.*
- Puerto MQTT (1883 o 8883).
- Usuario y contraseña.
- Certificados.
- Nombre del cliente.

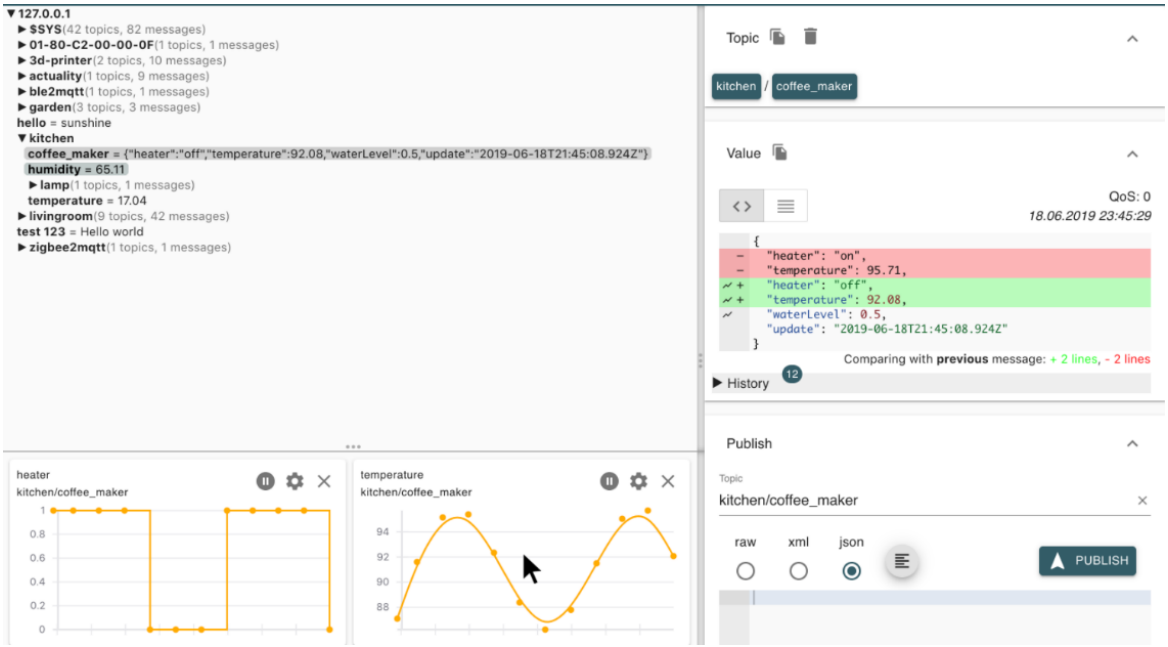

Figura 19. Interfaz MQTT Explorer 2.

En la Figura 19 se pueden observar las diferentes opciones de visualización que permite mqtt-explorer: en primer lugar, los *topics* a los que se ha suscrito el cliente en un listado en orden alfabético y en negrita y, en segundo lugar, las gráficas con los datos correspondientes a cada *topic*. De este modo, es posible observar con mayor claridad si se ha producido un ataque de modificación de información, pues las gráficas representarían datos diferentes a los originales, obteniéndose curvas desiguales.

6.2.2 Funcionamiento de comunicación MQTT

A continuación, en la Figura 20, Figura 21, Figura 22, Figura 23 y Figura 24, se muestran capturas de Wireshark [43] detallando los pasos que realiza el cliente para comenzar a publicar en un *topic.*

Cliente (publicador o suscriptor) envía un paquete "Connect Command" hacia el *broker.*

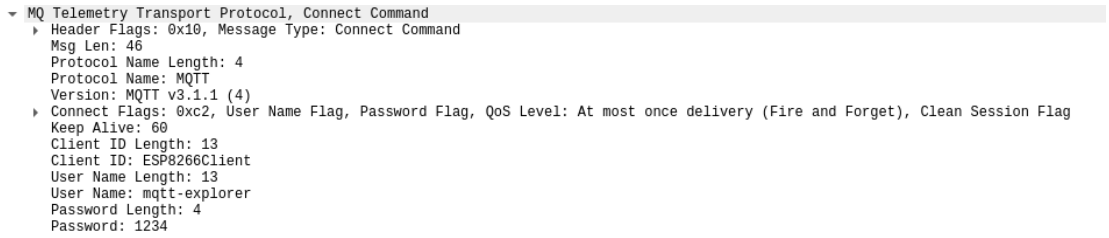

Figura 20. Paquete *Connect* en comunicación MQTT.

Broker acepta o rechaza la conexión, devolviendo paquete "*Connect Ack*".

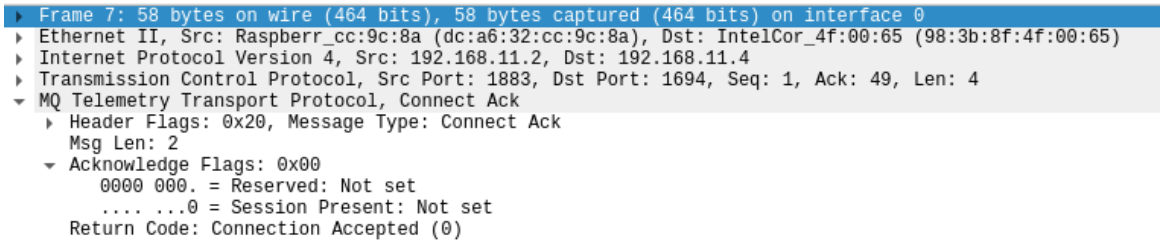

Figura 21. Paquete *Connect ACK* en comunicación MQTT.

Cliente envía una petición de suscripción "*Subscribe Request*" a un *topic* hacia el *broker.*

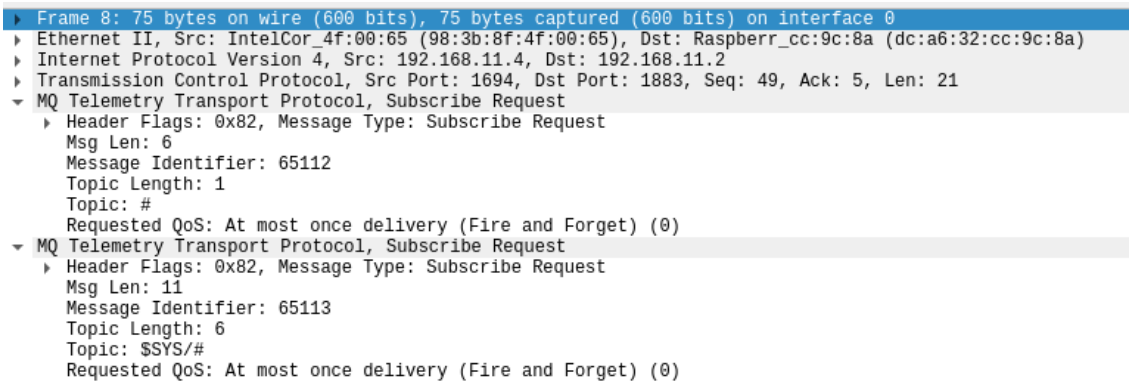

Figura 22. Paquete *Subscribe Request* en comunicación MQTT.

Broker acepta o rechaza la petición de suscripción con el paquete "Subscribe Ack".

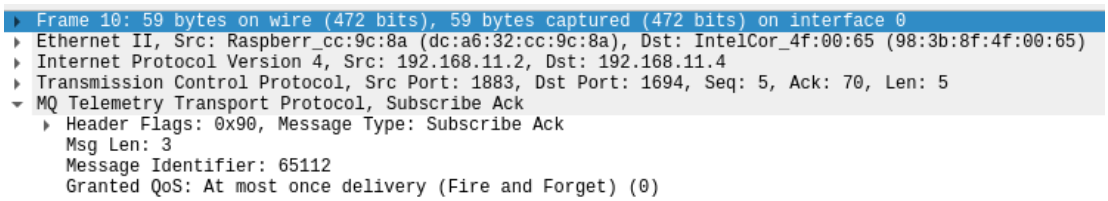

Figura 23. Paquete *Subsribe Ack* en comunicación MQTT.

Cliente publica en el *topic* esp32/humidity con el paquete "*Publish Message*".

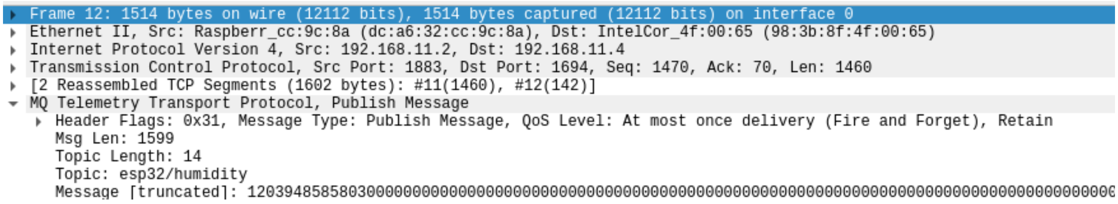

Figura 24. Paquete *Publish* en comunicación MQTT.

6.3. Pruebas de penetración

Las pruebas que se van a realizar a continuación parten de la premisa de que el atacante ha conseguido obtener acceso a la red local, pudiendo este ser un cliente curioso o un trabajador interno con malas intenciones.

6.3.1. Escaneo y recopilación de información

En primer lugar, se realiza un escaneo de la red para la obtención de información acerca de los equipos que se encuentran conectados con el siguiente comando de Nmap:

```
>> sudo nmap -p 1-65535 -T4 -A -vv 192.168.11.0/24
```

El escaneo se realiza con la herramienta Nmap [44]. Por su parte, el comando que se ha empleado realiza un escaneo completo de todas las IPs disponibles en la red.

El resultado del escaneo se muestra en la Figura 25, destacándose en rojo los dos *topics* detectados en la comunicación MQTT. Además, en este escaneo se obtiene la IP del equipo en el que se encuentra el *broker* trabajando con el puerto 1883 (correspondiente a MQTT) abierto.

```
Nmap scan report for 192.168.11.2
Host is up, received conn-refused (0.022s latency).
Scanned at 2021-04-07 10:23:01 CEST for 89s
Not shown: 65534 closed ports
Reason: 65534 conn-refused
PORT     STATE SERVICE                REASON  VERSION
1883/tcp open  mosquitto version 1.5.7 syn-ack
| mqtt-subscribe:
|   Topics and their most recent payloads:
|     $SYS/broker/clients/inactive: 5
|     $SYS/broker/load/sockets/5min: 0.93
|     $SYS/broker/publish/messages/sent: 20740
|     $SYS/broker/clients/total: 11
|     $SYS/broker/load/bytes/received/5min: 536.57
|     $SYS/broker/bytes/sent: 615242
|     $SYS/broker/load/sockets/1min: 2.67
|     $SYS/broker/uptime: 1113651 seconds
|     $SYS/broker/load/bytes/sent/15min: 220.92
|     $SYS/broker/load/messages/received/1min: 32.56
|     $SYS/broker/retained messages/count: 52
|     $SYS/broker/load/publish/sent/1min: 58.91
|     $SYS/broker/messages/sent: 83033
|     $SYS/broker/clients/maximum: 11
|     $SYS/broker/store/messages/bytes: 246
|     $SYS/broker/load/publish/sent/15min: 6.39
|     $SYS/broker/clients/active: 6
|     $SYS/broker/load/messages/received/15min: 19.31
|     esp32/humidity: 53.24
|     $SYS/broker/version: mosquitto version 1.5.7
|     $SYS/broker/subscriptions/count: 17
|     $SYS/broker/messages/received: 99516
|     $SYS/broker/load/connections/15min: 0.35
|     $SYS/broker/store/messages/count: 52
|     $SYS/broker/clients/connected: 6
|     esp32/temperature: 23.23
```

Figura 25. Resultado de escaneo con la herramienta Nmap.

Finalizado el escaneo, se utiliza la herramienta Ettercap [45] para realizar un ataque sobre el protocolo Address Resolution Protocol (ARP) (Figura 26). Posteriormente, a través de una herramienta como Wireshark, será posible ver el tráfico entre las dos IPs elegidas como objetivo del ataque.

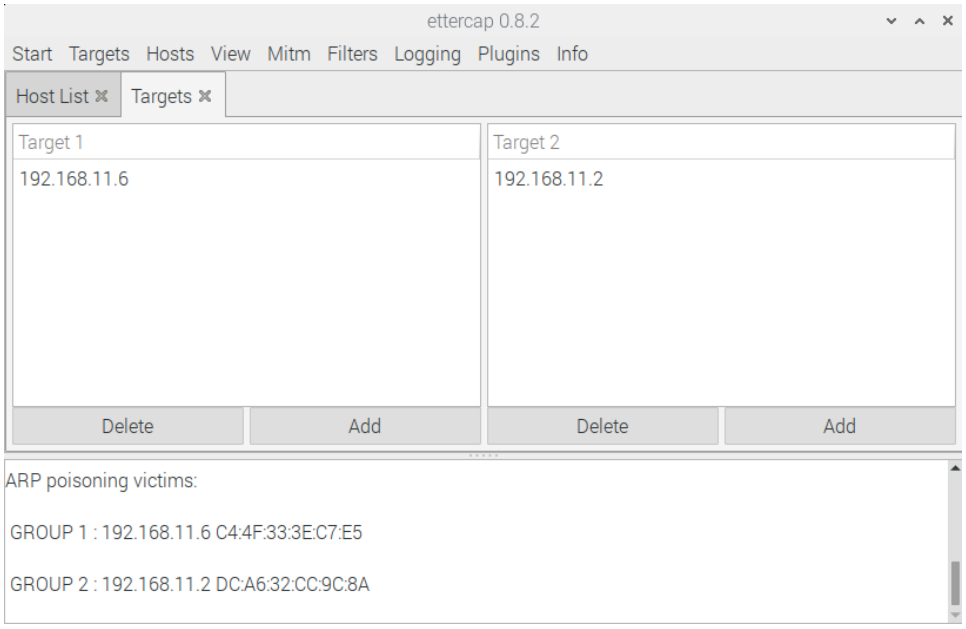

Figura 26. Herramienta Ettercap.

En este caso, en la Figura 26 se han seleccionado como objetivo las siguientes IP:

- IP 192.168.11.2: Raspberry Pi 4 donde se encuentra el *broker*.
- IP 192.168.11.6: ESP32 donde se encuentra la estación meteorológica publicando a los *topics* esp32/humidity y esp32/temperatura.

En la Figura 27 se puede observar una captura de Wireshark en la que aparece el paquete *connect* en texto claro. Además, se le añadió un mecanismo de seguridad mediante contraseña a la comunicación MQTT, apreciándose en texto claro el Client ID, usuario y contraseña.

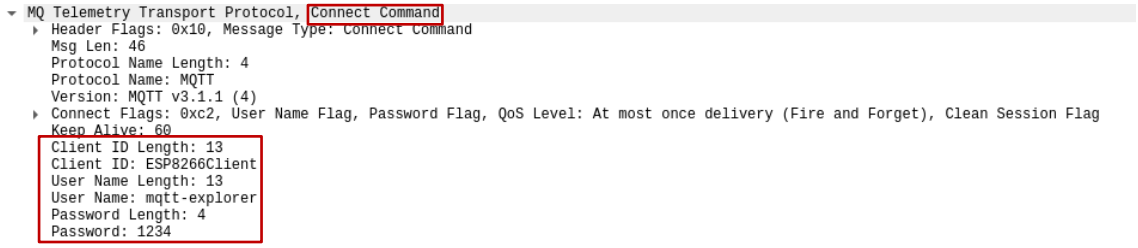

Figura 27. Paquete Connect detectado mediante MiTM.

Una vez se ha obtenido toda la información necesaria, se pueden realizar los ataques mencionados en los apartados 6.3.2. Ataque MiTM (Intrusivo) y 6.3.3. Ataque MiTM (no intrusivo).

6.3.2. Ataque MiTM (Intrusivo)

Con esta información se procedió a realizar la suplantación de identidad del cliente (ESP8266Client), encargado de enviar los datos medidos en la estación meteorológica.

Conocer el id del cliente realizando un escaneo de red es suficiente para suplantar la identidad, ya que no hay ningún tipo de protección de serie en el protocolo.

En la Figura 28 se puede observar como la estación meteorológica está mandando correctamente los datos de humedad y temperatura:

Figura 28. Datos de temperatura y humedad recibidos correctamente.

Sin embargo, al realizar la suplantación de identidad, la estación meteorológica dejó de funcionar, puesto que se suplantó su identidad. En la Figura 29 se puede observar el intento de conexión MQTT, aunque fallido: el ciberatacante ha conseguido conectarse con el *broker* y está desconectando al cliente.

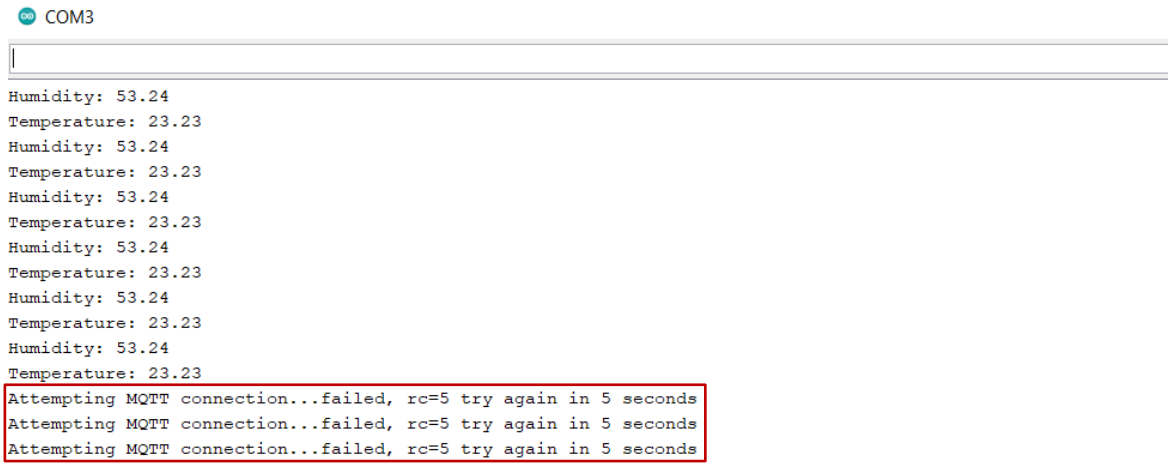

Figura 29. Resultado ataque intrusivo (puerto serie del publicador).

Por otro lado, en la Figura 30, se puede ver como los valores de temperatura y humedad adquirieron valores completamente distintos a los que marcaba la estación meteorológica:

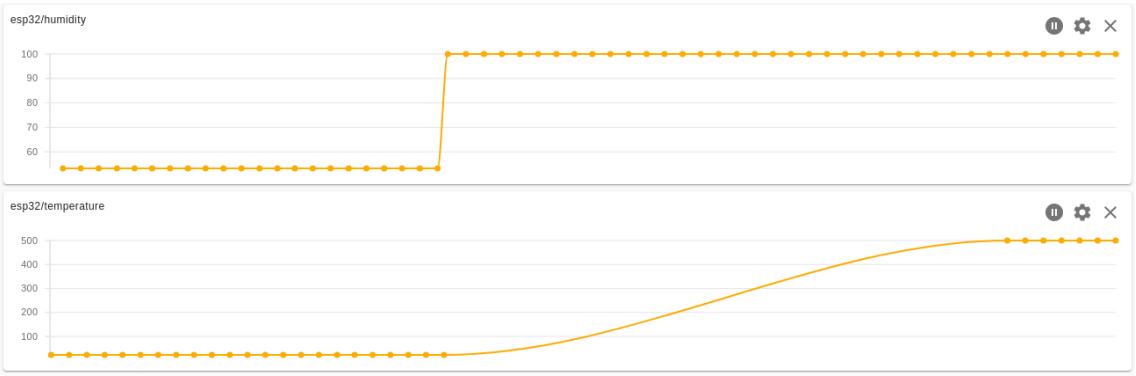

Figura 30. Resultado ataque intrusivo (datos de temperatura recibidos erróneamente).

6.3.3. Ataque MiTM (no intrusivo)

Para realizar el ataque no intrusivo se deben seguir los pasos siguientes:

Instalar librería nfqueue [46]:

1 **>> git clone** https://github.com/kti/python-netfilterqueue.git - Clonación de repositorio
2 **>> cd Python-netfilterqueue** - Situarse en el directorio de trabajo
3 **>> sudo Python setup.py** - Instalación

Instalar librería scapy [47]:

1 **>> sudo apt-get install python3-scapy** - Instalación de la librería

Para ejecutar el código de Python se utiliza el siguiente comando:

```
1   >> sudo python nombrecodigo.py - Ejecución de código en python
```

Es importante usar Python y no Python3 ya que hay problemas de compatibilidad con las diferentes librerías utilizadas.

Una vez instaladas las librerías necesarias, es posible ejecutar el ataque:

1. Se inicia la herramienta Ettercap para realizar un ataque *ARP Poisoning* para conseguir situarse entre el cliente publicador y el *broker*.
2. Una vez instalados en el medio de las comunicaciones, se ejecuta el archivo de Python encargado de buscar un paquete con la trama raw que se le asigne, en este caso, busca el valor 2 en el paquete y lo intercambia por el número 8. El código para realizar dicho ataque se encuentra en el apéndice C.3. Código Python ataque contra integridad en MQTT.
3. Se ejecuta el siguiente comando para redireccionar el tráfico de entrada hacia el script de Python para realizar el ataque [46]:
    a. **>> sudo iptables -I OUTPUT -d 192.168.12.0/24 -j NFQUEUE --queue-num 1**
4. Una vez desarrollados los pasos anteriores, el ataque ha comenzado y puede observarse lo siguiente:

La Figura 31 muestra cómo la estación está mandando un valor de temperatura de 23.23°C y una humedad del 53.34 % hacia el *broker*.

```
Temperature: 23.23
Humidity: 53.34
```

Figura 31. Mensajes enviados por la estación meteorológica

En la Figura 32 y en la Figura 33 se observa cómo, al producirse el ataque, el cliente comienza a recibir valores de temperatura modificados:

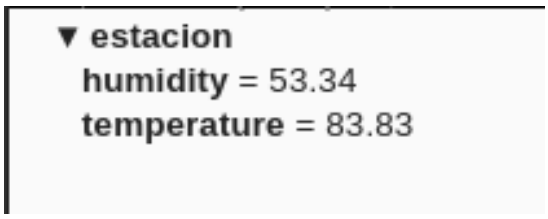

Figura 32. Mensaje recibido erróneamente por el cliente 1.

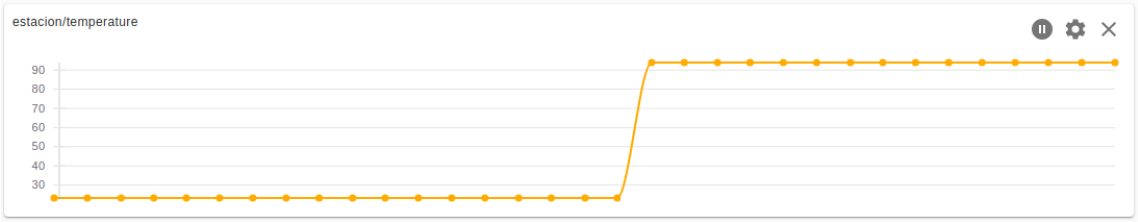

Figura 33. Mensaje recibido erróneamente por el cliente 2.

Por último, en la Figura 34, se puede apreciar la salida que muestra por terminal el código de Python. Este detecta el valor que se le ha pedido (el número 2) y lo modifica por el valor que se le ha impuesto (el número 8):

```
Has been found a Topic: estacion/temperature and Value: 2
Old Value0stacion/temperature23.23
Original checksum 58956recomputedChecksum 57414
New value 0stacion/temperature83.83
sending new_packet...
.
Sent 1 packets.
```

Figura 34. Atacante recibiendo paquetes y realizando modificación.

6.4. Implementación de salvaguardas

En este apartado, se describirán los procedimientos necesarios para la implementación de las salvaguardas necesarias para poder asegurar las comunicaciones MQTT frente a las pruebas de penetración realizadas en el apartado anterior.

6.4.1. Control de acceso mediante usuario y contraseña

Configuración de un usuario y contraseña

1 **sudo mosquitto_passwd -c /etc/mosquitto/passwd usuario** - Creación del fichero de contraseñas passwd con un usuario asignado. Una vez ejecutado el comando, será necesario introducir la contraseña en dos ocasiones.

2 **sudo cd /etc/mosquitto** - Acceso al directorio mosquitto.

3 **sudo gedit mosquitto.conf** - Edición del archivo mosquitto.conf.

#Passwords

4. **password_file /etc/mosquitto/passwd** - Archivo donde se encuentran las contraseñas.
5. **allow_anonymous false** - Solo autoriza la conexión a usuarios previamente autentificados con su usuario y contraseña.

6 **sudo systemctl restart mosquitto** - Reinicio del sistema para establecer los cambios en la configuración.

Gestión de usuarios y contraseñas

1. **mosquitto_passwd -U passwd** - Encriptación de archivo de contraseñas.
2. **mosquitto_passwd -b archivopasswd usuario contraseña** - Creación de usuario adicional con su respectiva contraseña.
3. **mosquitto_passwd -D archivopasswd usuario** - Eliminación de usuario.

Suscripción mediante usuario y contraseña

>> mosquitto_sub -d -h 192.168.11.2 -p 1883 -t "esp32/humidity" -u "mqtt-explorer" -P "1234" -i "raspberry"

- -u (indica el usuario).
- -P (indica la contraseña).
- -i (indica el Client_ID).

En la Figura 35 se puede observar una captura de Wireshark del paquete *connect* con las credenciales de acceso anteriormente mencionadas.

```
▾ MQ Telemetry Transport Protocol, Connect Command
  ▸ Header Flags: 0x10, Message Type: Connect Command
    Msg Len: 46
    Protocol Name Length: 4
    Protocol Name: MQTT
    Version: MQTT v3.1.1 (4)
  ▸ Connect Flags: 0xc2, User Name Flag, Password Flag, QoS Level: At most once delivery (Fire and Forget), Clean Session Flag
    Keep Alive: 60
    Client ID Length: 13
    Client ID: ESP8266Client
    User Name Length: 13
    User Name: mqtt-explorer
    Password Length: 4
    Password: 1234
```

Figura 35. Usuario y contraseña en paquete *Connect* Wireshark

Publicación mediante usuario y contraseña

>> mosquitto_pub -d -h 192.168.11.2 -p 1883 -t "esp32/humidity" -m "-52" -u "mqtt-explorer" -P "1234" -i "raspberry"

6.4.2. Encriptación de la comunicación

La encriptación de la comunicación se implementa para evitar ataques de modificación de contenido de los paquetes, así como escucha activa de la información intercambiada por medio de la comunicación MQTT.

Por ello, se realiza la implementación del protocolo Transport Layer Security (TLS) [48] sobre MQTT. TLS aborda los ataques a la integridad y el cifrado garantiza la confidencialidad del contenido de los paquetes de la comunicación MQTT. Para poder ejecutar cualquiera de estos ataques, el intruso se vería obligado a obtener las claves privadas y las claves de cifrado creadas para este fin.

Para proceder a la encriptación de la comunicación, en primer lugar, es necesario realizar modificaciones sobre el fichero de configuración de Mosquitto *broker* para ordenarle que se ejecute sobre TLS. Estas modificaciones pueden observarse en el apartado D.2. *Broker* Mosquitto [48] del Apéndice D.

Con posterioridad, se realizará únicamente la autentificación del servidor, dado que la implementación de TLS en un entorno con un mayor número de dispositivos con recursos limitados podría hacer que la latencia en la comunicación se viera afectada.

En este caso, solo se requiere la autentificación del servidor TLS y, para ello, este necesita:

- El certificado personal que la autoridad certificadora (CA) ha emitido para el servidor que ha sido auto firmado (sin embargo, se debería acudir a un tercero para poder obtener un certificado válido).
- La clave privada del servidor.

Por su parte, el cliente necesita la siguiente información:

- El certificado de la CA, en este caso, auto firmado.

En el caso de que se configure el servidor TLS para pedir el certificado al cliente, el servidor necesita:

- El certificado personal que la CA ha emitido para el servidor que ha sido auto firmado, aunque se tendría que acudir a un tercero para poder obtener un certificado válido.
- La clave privada del servidor.
- El certificado de la CA externa que ha emitido el certificado de nuestra CA.

Por su parte, el cliente necesita la siguiente información:

- El certificado que la CA externa ha emitido para el cliente.
- La clave privada del cliente.
- El certificado del servidor que ha emitido la CA.

En la Figura 36 se pueden observar los pasos en el funcionamiento de TLS. En los primeros, se realiza un intercambio de claves utilizando cifrado asimétrico para, finalmente, obtener una clave de sesión con la que poder comunicarse con cifrado simétrico.

Figura 36. Diagrama de funcionamiento de TLS [48].

En la Figura 37 se puede observar el comando requerido para generar un par de claves (pública y privada) para la CA mediante cifrado AES128.

```
pi@raspberrypi:~/Desktop/certificados $ sudo openssl genrsa -aes128 -out ca.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................................+++++
.....................................................................................................
.....+++++
e is 65537 (0x010001)
Enter pass phrase for ca.key:
```

Figura 37. Obtención de claves RSA para CA.

Mientras, en la Figura 38, se puede observar el comando requerido para generar un certificado para la CA utilizando la clave producida en la Figura 37. En cuanto a los campos que aparecen, es necesario tener en cuenta que, para que la comunicación funcione correctamente, el apartado Common Name debe incluir el nombre o IP del *broker* MQTT.

```
pi@raspberrypi:~/Desktop/certificados $ sudo openssl req -new -x509 -days 1826 -key ca.key -out ca.crt
Enter pass phrase for ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Madrid
Locality Name (eg, city) []:Alcala de Henares
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Universidad de Alcala
Organizational Unit Name (eg, section) []:UAH
Common Name (e.g. server FQDN or YOUR name) []:192.168.11.2
Email Address []:
```

Figura 38. Certificado para CA firmado con clave

La Figura 39 muestra el comando requerido para generar un par de claves (privada y pública) para el servidor:

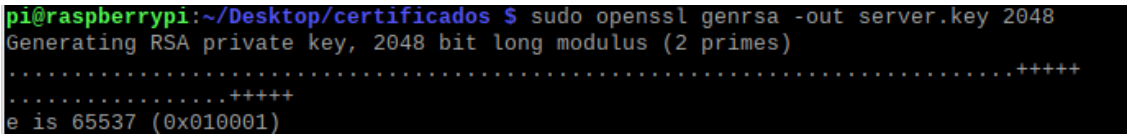

Figura 39. Obtención de claves RSA para *Broker* MQTT

En la Figura 40, se puede observar el comando para solicitar un certificado a la CA para el servidor. En un caso real, habría que realizar un envío de la solicitud a la autoridad certificadora.

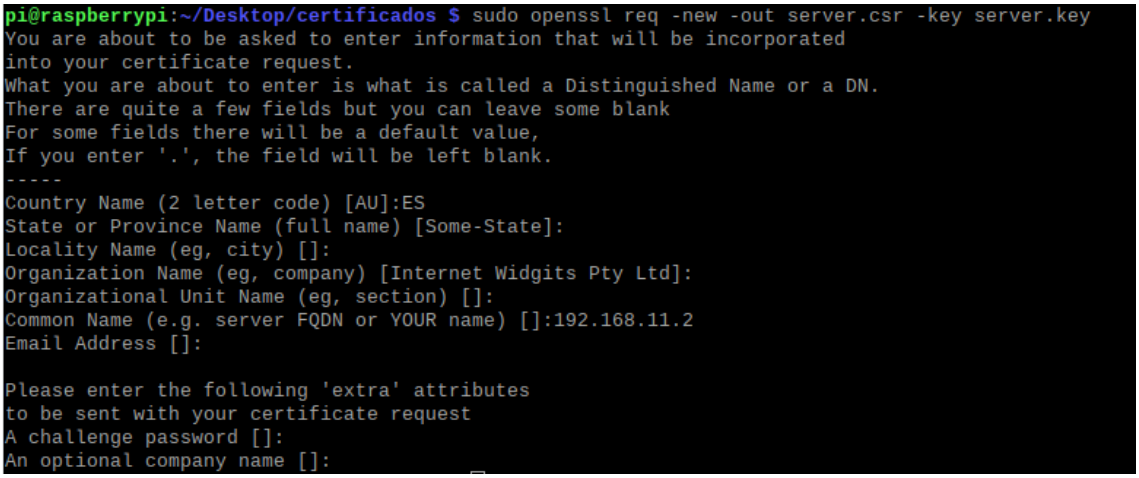

Figura 40. Solicitud de expedición de certificado para el *Broker* MQTT

Por último, en la Figura 41, se puede observar el comando para autorizar la expedición del certificado del servidor, ya que en el presente proyecto se actúa también como CA. En un caso real, se recibiría el certificado por parte de la CA.

Figura 41. Autorización de expedición de certificado para *Broker* MQTT

En la Figura 42 se puede observar como con Wireshark no ha sido posible obtener información acerca de la comunicación MQTT, ya que los paquetes están encriptados mediante TLS.

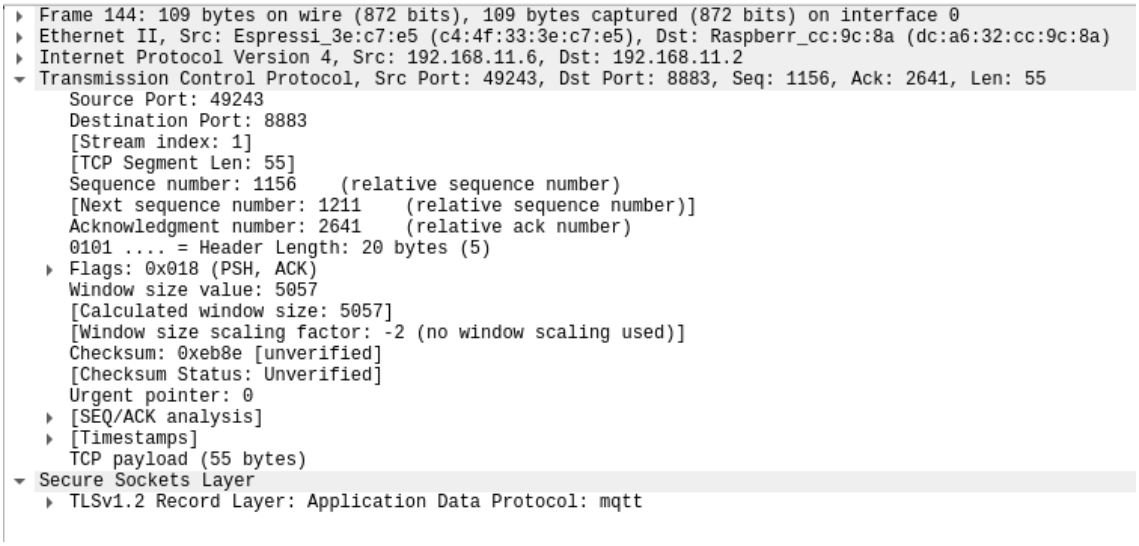

Figura 42. Paquete MQTT con encriptación.

En la Figura 43 se puede observar el resultado de un escaneo mediante Nmap con la comunicación MQTT cifrada. Además, se apreciar como el intento de conexión no ha sido autorizado por el *broker* y la única información obtenida es sobre la entidad certificadora.

```
8883/tcp open  ssl/mqtt syn-ack
| mqtt-subscribe: Connection rejected: Not Authorized
| ssl-cert: Subject: commonName=192.168.11.2/organizationName=Internet Widgits Pty Ltd/sta
| Issuer: commonName=192.168.11.2/organizationName=Universidad de Alcala/stateOrProvinceNa
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-05-05T08:54:34
| Not valid after:  2022-04-30T08:54:34
| MD5:   bd43 0d9e cf52 b0a7 c617 3557 86c6 cbbe
| SHA-1: 882f 97b6 a99a 6af1 3d5f 2682 1d1b 9e01 c164 908e
| -----BEGIN CERTIFICATE-----
| MIIDYjCCAkoCFDm8iTyxxDs1QGdkVdzl2dX/pdy5MA0GCSqGSIb3DQEBCwUAMH8x
| CzAJBgNVBAYTAkVTMQ8wDQYDVQQIDAZNYWRyaWQxGjAYBgNVBAcMEUFsY2FsYSBk
| ZSBIZW5hcmVzMR4wHAYDVQQKDBVVbml2ZXJzaWRhZCBkZSBBbGNhbGExDDAKBgNV
| BAsMA1VBSDEVMBMGA1UEAwwMMTkyLjE2OC4xMS4yMB4XDTIxMDUwNTA4NTQzNFoX
| DTIyMDQzMDA4NTQzNFowXDELMAkGA1UEBhMCRVMxEzARBgNVBAgMClNvbWUtU3Rh
| dGUxITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDEVMBMGA1UEAwwM
| MTkyLjE2OC4xMS4yMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzaxh
| E8AnZW+3yEidWy5Y4OX0Zc6c+sIcdy3L8R+oEpTflfwjlyFCgWkuoWRYFlJSeXah
| g4NSW3SqAmSrNHvFwe7cJRj5xaFDTJgFOvBBn8qHflvwBRXDp5sCJkAE2J31pIS4
| Sn7jiVkVo4BpJVkHgPbLWCjcxZjolEJspqf2aclS7KDtwEveW5dwnIEztnjk3iVm
| QJcFh4qmSYHKt7ogna/6TmYKEF22WN06sThhprB+snv2lziWEIQQ3oo2iJsPK9wn
| AZhKhj3HjWhr19z6rYTXMzXiX5O84+oS+mkKQevmtXHw+2ajjAvN48ZqnMVoiV7U
| nQFq9cOJNGTYsGWpNQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQARNfR6u9OVbsmp
| DOTrtC7zlnd/ZqwAE7VIhA7dnlCZhFvEIkWfuFlMwHZvvdE2jM4h3HQXIB6HWhwH
| dJw2NjJzI+C1eEXSeC3IlKStLsknNo7wwl/V3iP1CDzJy3ZGUiAXpN+/6sy2uN6T
| jNqYoMy7q9e3xl3FTUfaBwKSAoS3Bqmn7eT3PaZa83Xj+95RBOCoCGy2YozkUy38
| c5AxYUbAwok6Ew7Yw08UHXUNugHhgaExSj8iyPjpfdWhQFoI1kxG0h+U0Mw3wLMj
| AAgTXSa4okIM2NIegOEeed2krjR0XOiTVCHuJ2iYe7351haw7/rhzD4KnUJypxVO
| c7nkU0iV
|_-----END CERTIFICATE-----
```

Figura 43. Resultado escaneo con comunicación MQTT encriptada.

6.4.3. Implementación de un IDS

El sistema de detección de intrusiones utilizado es Suricata IDS [50], un software de código de abierto que permite detectar intrusiones en tiempo real (IDS), así como prevenir estas (IPS).

Figura 44. Logo Suricata IDS.

En la *release* 6.0.2 de marzo de 2021, se añadió un *parser* para detectar intrusiones en el protocolo de comunicación MQTT. Suricata IDS está evolucionando conforme el sector de la ciberseguridad así lo requiere y dispone de soporte para algunos de los protocolos de comunicación más utilizados en el mundo energético, como Modbus o DNP3.

La instalación y configuración del IDS se puede observar en el Apéndice D.1. Suricata IDS. Hay varios tipos de IDS, siendo Suricata IDS un *Host Based IDS* basado en firmas.

El formato de las firmas (también denominadas reglas) es el siguiente:

ACCIÓN PROTOCOLO IP_ORIGEN PUERTO_ORIGEN DIRECCIÓN (->, <- o <>) IP_DESTINO PUERTO_DESTINO (*keywords* separada entre sí por ";")

- **Acción**

En la Tabla 7 se pueden observar las diferentes acciones que se pueden realizar con Suricata:

ACCIÓN	**Descripción**
alert	Generar una alerta si se activa la regla.
pass	Si se activa la regla, Suricata no alerta sobre el paquete.
drop	Alerta y desecha el paquete si se activa la regla.

reject	Rechazo activo del paquete si se activa la regla. Para los paquetes TCP, Suricata envía un TCP rst mientras que, para el resto, envía un paquete de error ICMP.
rejectsrc	El paquete de rechazo se envía al origen de la regla que se activa.
rejectdst	El paquete de rechazo se envía al destinatario de la regla que se activa.
rejectboth	El paquete de rechazo se envía a origen y destino.

Tabla 7. Acciones Reglas de Suricata IDS.

- **Protocolo**

Hay diversos detectores de protocolos de comunicación de las capas de red (3), transporte (4) y aplicación (7) del modelo OSI. Por su parte, Suricata tiene *Keywords* específicas para cada uno de estos protocolos.

Algunos ejemplos de las capas 3 y 4 pueden ser TCP, UDP o ICMP; mientras que de la capa de aplicación pueden encontrarse Modbus, DNP3 o MQTT (bastante comunes en el sector energético).

Hoy en día, Suricata no dispone de soporte para IEC61850, el estándar más utilizado actualmente en el sector eléctrico.

- **IPs y puertos**

Se pueden poner directamente sobre la regla, sin embargo, en caso de que fuesen varias IPs juntas, lo mejor sería situarlas por medio de un *array* en el archivo de configuración suricata.yaml.

- **Keywords**

Las *keywords* son específicas para cada protocolo y permiten implementar reglas particulares para detectar un paquete en concreto.

En la Figura 45 se pueden observar las diferentes *keywords* para MQTT [51] que tiene implementadas Suricata IDS actualmente:

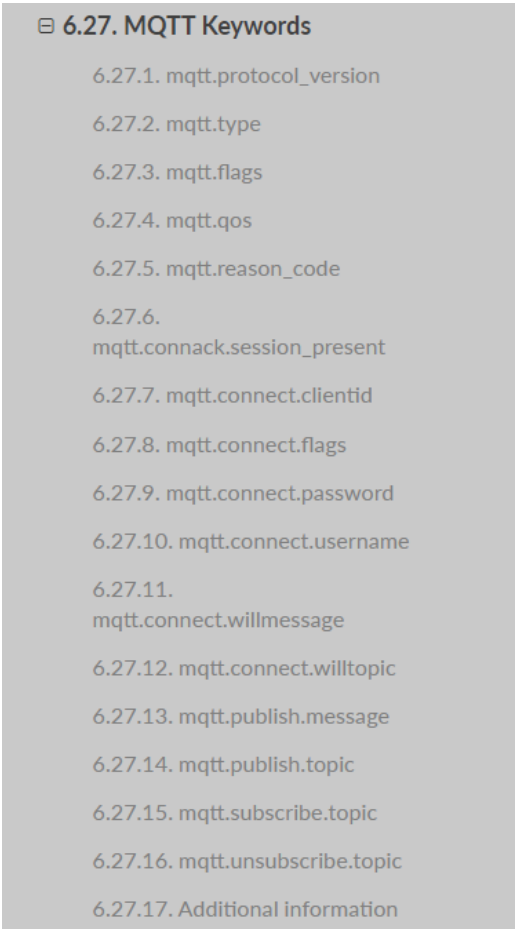

Figura 45. *Keywords* para MQTT en Suricata IDS.

Bloqueo de intento de conexión desde una IP desconocida

El ciberatacante intenta realizar el ataque de suplantación al conocer todos los datos de la comunicación MQTT (usuario, contraseña y clientID de uno de los equipos considerado como conocido por el *broker*).

La siguiente regla de Suricata detecta y bloquea una conexión desde una IP conocida, pero con un Client ID que no concuerda con el que está asignado a ese equipo.

```
>> Drop mqtt !$EXTERNAL_NET any -> $HOME_NET any (msg:" Paquete desde una IP \
desconocida"; sid:9000000; rev:1;)
```

Al introducir una negación, !$EXTERNAL_NET, bloquea la conexión MQTT desde una IP que sea desconocida.

En la Figura 46 se puede observar cómo el equipo atacante recibe el código rc = -4. Este código, según la documentación de MQTT, es el siguiente:

MQTT_CONNECTION_TIMEOUT: el servidor no respondió dentro del tiempo establecido.

```
COM3

Attempting MQTT connection...failed, rc=-4 try again in 5 seconds
Attempting MQTT connection...failed, rc=-4 try again in 5 seconds
Attempting MQTT connection...failed, rc=-4 try again in 5 seconds
Attempting MQTT connection...failed, rc=-4 try again in 5 seconds
Attempting MQTT connection...failed, rc=-4 try again in 5 seconds
Attempting MQTT connection...failed, rc=-4 try again in 5 seconds
Attempting MQTT connection...failed, rc=-4 try again in 5 seconds
Attempting MQTT connection...failed, rc=-4 try again in 5 seconds
Attempting MQTT connection...failed, rc=-4 try again in 5 seconds
Attempting MQTT connection...failed, rc=-4 try again in 5 seconds
Attempting MQTT connection...failed, rc=-4 try again in 5 seconds
Attempting MQTT connection...failed, rc=-4 try again in 5 seconds
Attempting MQTT connection...failed, rc=-4 try again in 5 seconds
Attempting MQTT connection...failed, rc=-4 try again in 5 seconds
Attempting MQTT connection...failed, rc=-4 try again in 5 seconds
Attempting MQTT connection...
```

Figura 46. Salida puerto serie de atacante de bloqueo de paquetes desde una IP desconocida con Suricata.

En la Figura 47 se puede observar lo siguiente:

- *src_ip*: Indica la IP de origen del ataque.
- *dst_ip*: Indica la IP de destino del ataque.
- *action*: *blocked:* Indica que se ha bloqueado la acción.
- *signature:* "Paquete de una ip desconocida detectado y bloqueado".


```
{
  "timestamp": "2021-06-04T12:33:25.360094+0200",
  "flow_id": 440427445677710,
  "event_type": "alert",
  "src_ip": "192.168.11.6",
  "src_port": 50455,
  "dest_ip": "192.168.11.2",
  "dest_port": 1883,
  "proto": "TCP",
  "alert": {
    "action": "blocked",
    "gid": 1,
    "signature_id": 9000000,
    "rev": 1,
    "signature": "Paquete de una ip desconocida detectado y bloqueado"
    "category": "",
    "severity": 3
  },
  "mqtt": {
    "connect": {
      "qos": 0,
      "retain": false,
      "dup": false,
      "protocol_string": "MQTT",
      "protocol_version": 4,
      "client_id": "ESP8266Client",
      "flags": {
        "username": true,
        "password": true,
        "will_retain": false,
        "will": false,
        "clean_session": true
      },
      "username": "mqtt-explorer",
      "password": "1234"
    }
  },
  "app_proto": "mqtt",
  "flow": {
    "pkts_toserver": 4,
    "pkts_toclient": 3,
    "bytes_toserver": 216,
    "bytes_toclient": 132,
    "start": "2021-06-04T12:33:22.454286+0200"
  }
```


Figura 47. Detección y bloqueo de cualquier paquete desde una IP desconocida.

Detección de Paquete Connect desde una IP desconocida

El ciberatacante intenta realizar una conexión mediante MQTT desde una IP desconocida.

La siguiente regla de Suricata detecta el envío de un paquete *connect* desde una IP desconocida. Igualmente, se podría actuar como en el caso anterior y bloquear el mensaje usando la acción *drop*.

>> alert mqtt $EXTERNAL_NET any -> $HOME_NET any (msg:" Paquete Connect \ detectado"; mqtt_type:CONNECT; sid:9000001; rev:1;)

En la Figura 48 se muestra lo siguiente:

- *src_ip*: Indica la IP de origen del ataque.
- *dst_ip:* Indica la IP de destino del ataque.
- *action*: *allowed:* Indica que se ha detectado la acción, pero no se ha bloqueado.
- *signature:* "Paquete *connect* detectado".


```
{
  "timestamp": "2021-06-04T12:42:45.511198+0200",
  "flow_id": 44906091755277,
  "event_type": "alert",
  "src_ip": "192.168.11.6",
  "src_port": 49409,
  "dest_ip": "192.168.11.2",
  "dest_port": 1883,
  "proto": "TCP",
  "tx_id": 0,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 9000001,
    "rev": 1,
    "signature": "Paquete connect detectado",
    "category": "",
    "severity": 3
  },
  "mqtt": {
    "connect": {
      "qos": 0,
      "retain": false,
      "dup": false,
      "protocol_string": "MQTT",
      "protocol_version": 4,
      "client_id": "ESP8266Client",
      "flags": {
        "username": true,
        "password": true,
        "will_retain": false,
        "will": false,
        "clean_session": true
      },
      "username": "mqtt-explorer",
      "password": "1234"
    },
    "connack": {
      "qos": 0,
      "retain": false,
      "dup": false,
      "session_present": false,
      "return_code": 0
    }
  },
  "app_proto": "mqtt",
  "flow": {
    "pkts_toserver": 6,
    "pkts_toclient": 6,
    "bytes_toserver": 337,
    "bytes_toclient": 253,
    "start": "2021-06-04T12:42:45.243469+0200"
  }
}
```


Figura 48. Detección de paquete *connect* desde una IP desconocida.

Bloqueo de intento de conexión con suplantación de una IP conocida y distinto ClientID

El ciberatacante intenta realizar una suplantación de la IP de uno de los equipos considerado como conocido por el broker.

El atacante podría desconocer el ClientID de la comunicación MQTT, por lo que deja el que viene por defecto o lo escoge al azar.

La siguiente regla de Suricata IDS permite detectar y bloquear una conexión desde una IP conocida, pero con un Client ID que no concuerda con el asignado a ese equipo:

>> Drop mqtt $EXTERNAL_NET any -> $HOME_NET any (msg:" Client ID desconocido \ detectado y bloqueado"; mqtt.connect.clientid; content: !"ESP8266Client"; sid:9000002; \ rev:1;)

A la IP considerada como conocida se le ha asignado el Client ID -> ESP8266Client. En el apartado *content* de la regla, se ha introducido una negación sobre el contenido. Por ende, la regla actúa y descarta los paquetes MQTT enviados desde la IP conocida hacia el *broker* con un Client ID distinto del especificado en la regla.

La Figura 49 muestra cómo el equipo atacante recibe el código rc = -4. Este código, según la documentación de MQTT, es el siguiente:

MQTT_CONNECTION_TIMEOUT: el servidor no respondió dentro del tiempo establecido.

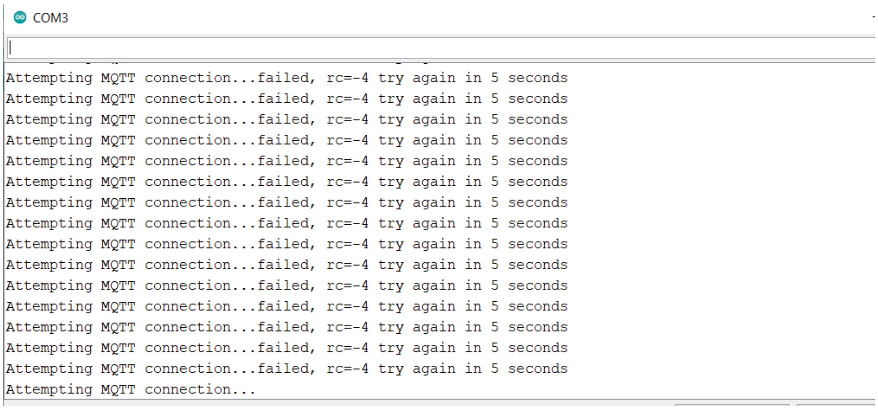

Figura 49. Resultado puerto serie de atacante de bloqueo de paquete con Client ID distinto con Suricata.

En la Figura 50 se puede observar la salida de los *logs* de Suricata:

```
{
  "timestamp": "2021-06-03T12:36:04.006060+0200",
  "flow_id": 585797846959708,
  "event_type": "alert",
  "src_ip": "192.168.11.6",
  "src_port": 51851,
  "dest_ip": "192.168.11.2",
  "dest_port": 1883,
  "proto": "TCP",
  "tx_id": 0,
  "alert": {
    "action": "blocked",
    "gid": 1,
    "signature_id": 9000002,
    "rev": 1,
    "signature": "Client ID desconocido detectado y bloqueado",
    "category": "",
    "severity": 3
  },
  "mqtt": {
    "connect": {
      "qos": 0,
      "retain": false,
      "dup": false,
      "protocol_string": "MQTT",
      "protocol_version": 4,
      "client_id": "ESP8267Client",
      "flags": {
        "username": true,
        "password": true,
        "will_retain": false,
        "will": false,
        "clean_session": true
      },
      "username": "mqtt-explorer",
      "password": "1234"
    }
  },
  "app_proto": "mqtt",
  "flow": {
    "pkts_toserver": 3,
    "pkts_toclient": 1,
    "bytes_toserver": 172,
    "bytes_toclient": 44,
    "start": "2021-06-03T12:36:04.001628+0200"
  }
}
```


Figura 50. Detección de ataque con misma IP con distinto Client ID.

Por último, en la Figura 50 se puede observar lo siguiente:

- *src_ip*: Indica la IP de origen del ataque.
- *dst_ip*: Indica la IP de destino del ataque.
- *action*: *blocked:* Indica que se ha bloqueado la acción.
- *signature:* "Client ID desconocido detectado y bloqueado".
- *client_id:* "ESP8267Client", diferente al especificado en la regla "ESP8266Client".

Capítulo 7

Presupuesto

7.1. Costes de equipo

Este apartado incluye los costes de equipo, tanto de hardware como de software.

	Concepto	Cantidad	Precio unitario (€)	Total (€) Sin IVA
Hardware	Ordenador portátil Lenovo ThinkPad T480	1	800	800
	Raspberry Pi 4 Model B 8 GB	2	59,26	118,52
	Adafruit Feather ESP32	1	19,95	19,95
	Router TP-Link Archer AX10	1	58,26	58,26
Total de Hardware				996,73
Software	Sistema Operativo Windows	1	114,55	114,55
	Sistema Operativo Ubuntu	1	0	0
	Sistema Operativo Raspberry Pi OS	1	0	0
	Licencia de Office 365 (anual)	1	54,51	54,51
	Suricata IDS	1	0	0
	Eclipse Mosquitto	1	0	0
	Mqtt-explorer	1	0	0
	Nmap	1	0	0
	Ettercap	1	0	0
	Wireshark	1	0	0
	IDE Arduino	1	0	0
Total de Sofware				**169,06**
Coste Total de Material				**1165,79**

Tabla 8. Costes de equipo.

7.2. Costes profesionales

En esta sección se muestra el coste profesional del proyecto. Este se calcula como salario bruto.

La Tabla 9 incluye todas las actividades profesionales relacionadas con el proyecto.

Concepto		Precio unitario (€/hora)	Cantidad (horas)	Total (€) Sin IVA
Honorarios profesionales	Ingeniería	15	500	7500
	Memoria	10	200	2000
Coste Total Honorarios Profesionales				**9500**

Tabla 9. Costes profesionales.

7.3. Coste visado de proyecto

Según el Colegio de Ingenieros Técnicos Industriales de Madrid [52], cuando el coste del proyecto es inferior a 30.050 € se le aplica un porcentaje de 0.255% sobre coste total, resultando 27,19 €.

Costes de Material (€)	1165,79
Costes Profesional (€)	9500
Total	**10.665,79**

Tabla 10. Costes totales.

Sin embargo, el Colegio también indica que los costes asociados a un visado proyecto y su dirección técnica han de ser 50 € como mínimo.

7.4. Coste total del proyecto

Coste Total (€)	10665,79
Visado del proyecto (€)	50
Total (Sin IVA)	10715,79
Total (Con IVA)	12966,10

Tabla 11. Coste total del proyecto.

El coste total del proyecto asciende a doce mil novecientos sesenta y seis euros con diez céntimos.

Capítulo 8

Conclusiones y futuras líneas

8.1. Conclusiones

Como se ha podido observar a lo largo del presente documento, las instituciones son las responsables de sentar las bases teóricas aplicadas al desarrollo de nuevos proyectos de ciberseguridad en las *Smart Grids.*

Las redes inteligentes constituyen un campo de la ingeniería que se nutre de varias vertientes en las que los profesionales de las telecomunicaciones y la ingeniería industrial deben trabajar a la par. Por ello, resulta necesario elaborar una guía de buenas prácticas en la ciberseguridad de las redes inteligentes con el fin de que los profesionales de ambas ramas puedan entenderse y realizar su actividad de forma satisfactoria en este campo multidisciplinar y en constante evolución.

Por otro lado, se ha identificado la necesidad del diseño por seguridad de los sistemas desplegados en las *Smart Grids*, ya que muchos de estos sistemas disponen de conexión a internet y pueden presentar multitud de vectores de ataque. Particularizando en el caso del sistema inteligente de gestión de energía desplegado en la EPS y dado que en un inicio la ciberseguridad no había sido tenida en cuenta en su diseño, se ha llevado a cabo una localización de activos, una evaluación de amenazas y una cuantificación de riesgos, con el fin de obtener una visión más completa del sistema.

Cabe destacar que las amenazas podrían cambiar o aumentar si el modelo de amenaza difiriese al que se ha tratado de definir en el presente proyecto: un modelo de amenaza realista conforme al tipo de sistema evaluado.

Siguiendo en la línea del entendimiento entre profesionales, se puede concluir que el C4 Model es una buena forma gráfica de modelar software para que otros profesionales que trabajen en el sector (pero no sean expertos en software) puedan entender el funcionamiento, al menos, de un modo básico.

La metodología STRIDE para la evaluación de amenazas, junto con MAGERIT en la cuantificación de los riesgos, han servido para obtener una visión de las zonas del sistema que pueden presentar más vulnerabilidades.

El último capítulo del documento demuestra el análisis teórico realizado, pues ha sido posible probar los ataques que se habían previsto con este. Además, como el propio nombre de este TFM indica en una de sus partes, con la "ciberseguridad" se ha conseguido solventar el problema de los ataques contra la comunicación MQTT.

Por otro lado, se han realizado pruebas exitosas con el detector de intrusiones Suricata IDS. Pese a que se encuentra en su primera versión, el *parser* de MQTT en Suricata IDS ha funcionado a la perfección en todas las pruebas realizadas. Aunque este tipo de detector de intrusiones (basado en firmas) es algo limitado para los casos en el que los vectores de ataque puedan ser desconocidos.

Finalmente, es necesario remarcar que el universo de la ciberseguridad, y más en concreto de la ciberseguridad en las *Smart Grids*, se encuentra en continua evolución. Es necesario introducir mecanismos de protección en los proyectos que se realicen para evitar futuros ataques que se podrían haber solucionado con la implementación de dichos recursos.

Resulta importante destacar la seguridad mediante confianza cero, ya que en sistemas críticos como las redes inteligentes no se pueden omitir elementos sin protección pues, como se ha estudiado, pueden aparecer multitud de amenazas en el sistema.

Sin embargo, se debe tener en cuenta que el presente documento constituye un pequeño ejemplo en comparación con la cantidad de sistemas que se encuentran desplegados hoy en día en la red eléctrica.

8.2. Futuras líneas de investigación

Como futuras líneas futuras de investigación se plantea:

- Profundizar en el análisis de amenazas y cuantificación de riesgos de los sistemas del C4 Model del Apéndice A.
- Diseñar un detector de intrusiones basado en anomalías mediante aprendizaje automático para la seguridad del protocolo MQTT, ya que el implementado en el presente proyecto, basado en firmas, puede ser limitado en algunas situaciones.
- Diseñar una metodología para la creación de nuevas firmas para el protocolo MQTT en Suricata IDS mediante aprendizaje automático.
- Implementar un *parser* del protocolo IEC 61850 para Suricata IDS o similar, ya que es uno de los más utilizados actualmente en el sector de las energías.
- Realizar una mejora del método de encriptación implementando curvas logarítmicas o similares para poder cifrar las comunicaciones en dispositivos con recursos limitados.

Bibliografía

[1] «Helios Sharing (GEISER),» [En línea]. Available: http://geiser.depeca.uah.es/index.php/research-projects/helios-sharing.

[2] «STRIDE Microsoft,» [En línea]. Available: https://docs.microsoft.com/es-es/azure/security/develop/threat-modeling-tool-threats.

[3] «C4 Model,» [En línea]. Available: https://c4model.com/.

[4] «MAGERIT,» [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

[5] «NIST,» [En línea]. Available: https://www.nist.gov/.

[6] NIST, Guidelines for Smart Grid Cybersecurity: Vol.1, Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements, 2014.

[7] NIST, Guidelines for Smart Grid Cyber Security: Vol.2, Privacy and the Smart Grid, 2014.

[8] NIST, Guidelines for Smart Grid Cybersecurity: Vol.3, Supportive Analyses and References, 2010.

[9] NESCOR, Electric Sector Failure Scenarios and Impact Analyses - Version 3.0, 2015.

[10] Consejo Superior de Administración Electrónica del Gobierno de España, Libro I: Método, 2012.

[11] Consejo Superior de Administración Electrónica del Gobierno de España, Libro II: Catálogo de elementos, 2012.

[12] Consejo Superior de Administración Electrónica del Gobierno de España, Libro III: Guía de Técnicas, 2012.

[13] S. Mishra, K. Anderson, B. Miller, K. Boyer y A. Warren, «Microgrid resilience: A holistic approach for assesing threats, indentifying vulnerabilities, and designing corresponding mitigation strategies,» *Applied Energy,* vol. 264, 2020.

[14] N. Priyadharshini, S. Gomathy y M. Sabarimuthu, «A review on microgrid architecture, cyber security threats and standards,» *Materials Today: Proceedings,* 2020.

[15] M. Z. Gunduz y R. Das, «Cyber-security on smart grid: Threats and potential solutions,» *Computer Networks (ELSEVIER),* 2020.

[16] D. Faquir, N. Chouliaras, V. Sofia, K. Olga y L. Maglaras, «Cybersecurity in smart grids,

challenges and solutions,» *Electronics and Electrical Engineering (AIMS),* pp. 24-37, 2021.

[17] A. Volkova, M. Niedermeier, R. Basmadjian y H. d. Meer, «Security Challenges in Control Network Protocols: A Survey,» *IEEE Communications Surveys & Tutorials,* vol. 21, pp. 619-639, 2018.

[18] L. Langer, P. Smith y M. Hutle, «Smart grid cybersecurity risk assessment,» *International Symposium on Smart Electric Distribution Systems and Technologies (IEEE),* 2015.

[19] S. N. Firdous, Z. Baig, C. Valli y A. Ibrahim, «Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol,» *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),* p. 8, 2017.

[20] C. Pater y N. Doshi, «A Novel MQTT Security framework In Generic IoT Model,» *Procedia Computer Science,* vol. 171, Junio 2020.

[21] «E.DSO,» [En línea]. Available: https://www.edsoforsmartgrids.eu/home/why-smart-grids/.

[22] CEN, CENELEC, ETSI y S. G. Coordination. [En línea]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_security.pdf.

[23] N. M. Tabatabei, E. Kabalci y N. Bizon, Microgrid Architectures, Control and Protection Methods, Springer, 2020.

[24] «Security for smart Electricity GRIDs,» [En línea]. Available: https://segrid.eu/wp-content/uploads/2017/07/Whitepaper-SEGRID.pdf.

[25] «OCPP,» [En línea]. Available: https://www.openchargealliance.org/.

[26] «OpenADR,» [En línea]. Available: https://www.openadr.org/.

[27] «SPower,» [En línea]. Available: https://www.securityweek.com/cisco-firewall-vulnerability-exploited-attack-us-renewable-energy-provider .

[28] «Colonial Pipeline,» [En línea]. Available: https://www.theguardian.com/technology/2021/may/19/colonial-pipeline-cyber-attack-ransom.

[29] «Shamoon Virus,» [En línea]. Available: https://www.securitymagazine.com/articles/88818-saudi-arabia-investigating-critical-infrastructure-cyberattack.

[30] «caser seguros,» [En línea]. Available: https://www.caser.es/seguros-empresas/articulos/que-es-un-ciberataque-y-tipos.

[31] «ROS,» [En línea]. Available: https://www.ros.org/about-ros/.

[32] «Node-RED,» [En línea]. Available: https://nodered.org/about/.

[33] «Hyperledger Fabric,» [En línea]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/.

[34] M. T. Ágreda, Implementación de un sistema de control y gestión de una microrred, Alcalá de Henares: TFM UAH, 2020.

[35] «FreeRTOS,» [En línea]. Available: https://www.freertos.org/.

[36] «ThingSpeak,» [En línea]. Available: https://thingspeak.com/.

[37] «Espressif (ESP32),» [En línea]. Available: https://www.espressif.com/en/products/socs/esp32.

[38] «OASIS MQTT TC,» [En línea]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=mqtt.

[39] «MQTT,» [En línea]. Available: https://mqtt.org/.

[40] «OSTEC,» [En línea]. Available: https://ostec.blog/es/seguridad-perimetral/pentest-concepto-tipos/.

[41] «Raspberry,» [En línea]. Available: https://www.raspberrypi.org/products/raspberry-pi-4-model-b/.

[42] «mqtt-explorer,» [En línea]. Available: https://mqtt-explorer.com/.

[43] «Wireshark,» [En línea]. Available: https://www.wireshark.org/.

[44] «Nmap,» [En línea]. Available: https://nmap.org/.

[45] «Ettercap,» [En línea]. Available: https://www.ettercap-project.org/.

[46] «NetfilterQueue,» [En línea]. Available: https://pypi.org/project/NetfilterQueue/ .

[47] «Scapy,» [En línea]. Available: https://scapy.readthedocs.io/en/latest/installation.html.

[48] «IBM TLS,» [En línea]. Available: https://www.ibm.com/docs/es/ibm-mq/9.0?topic=ssfksj-9-0-0-com-ibm-mq-sec-doc-q009940--htm.

[49] «Mosquitto,» [En línea]. Available: https://mosquitto.org/.

[50] «Suricata,» [En línea]. Available: https://suricata.io/.

[51] «MQTT Keywords Suricata IDS,» [En línea]. Available: https://suricata.readthedocs.io/en/suricata-6.0.0/rules/mqtt-keywords.html.

[52] «COITIM,» [En línea]. Available: http://coitim.es/coitim/cms/contenidos/contenido.asp?Id=21&IdMenu=163.

Apéndice A - C4 Model de bajo nivel

En la Figura 51 se puede observar el C4 Model correspondiente a FreeRTOS, que se encuentra integrado en el ESP32 que incluya la estación meteorológica.

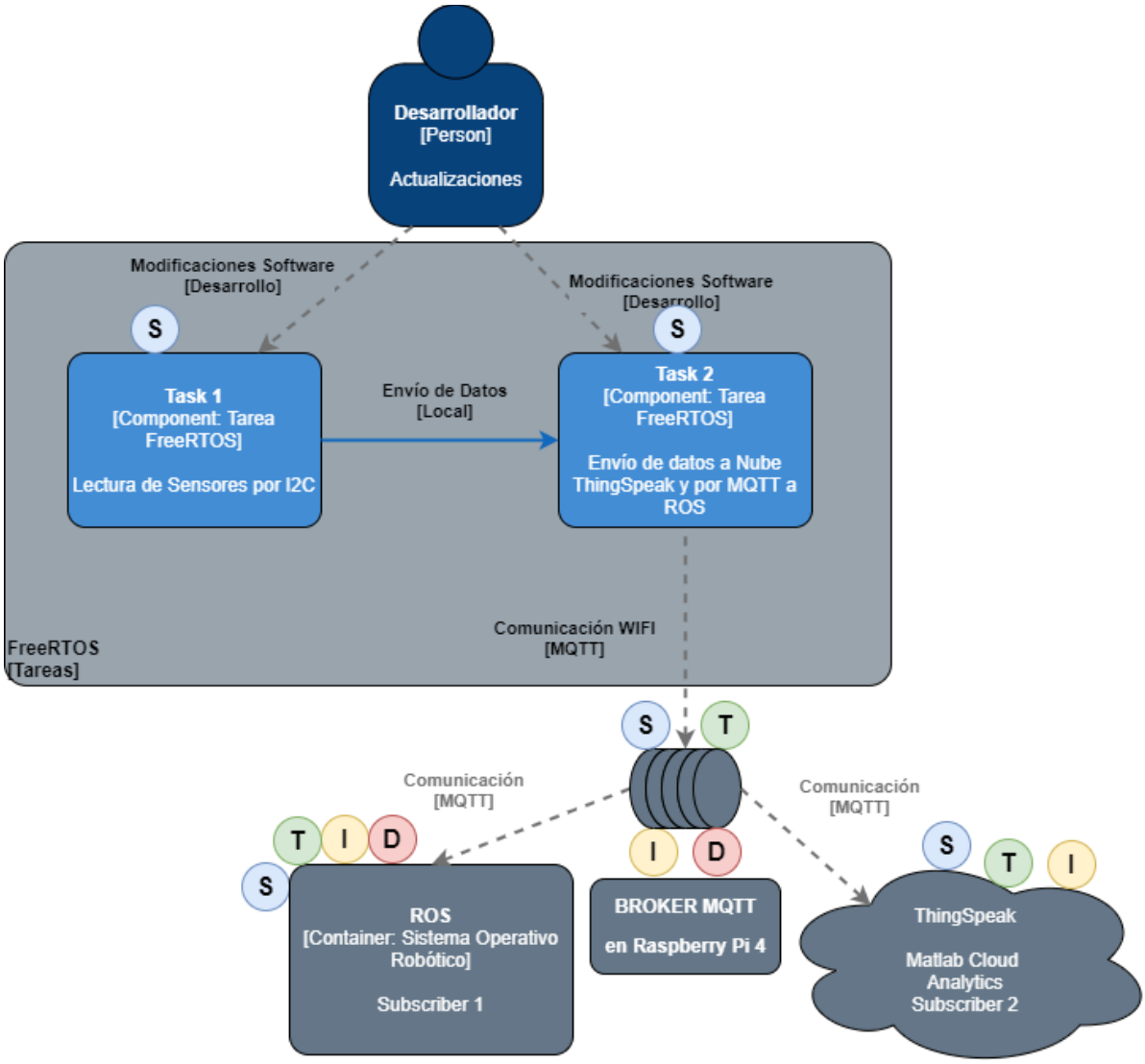

Figura 51. C4 Model FreeRTOS.

En la Figura 52 se puede observar el C4 Model del blockchain creado mediante Hyperledger Fabric. Además, se ha incluido un caso de uso en el que se puede apreciar el funcionamiento normal de este.

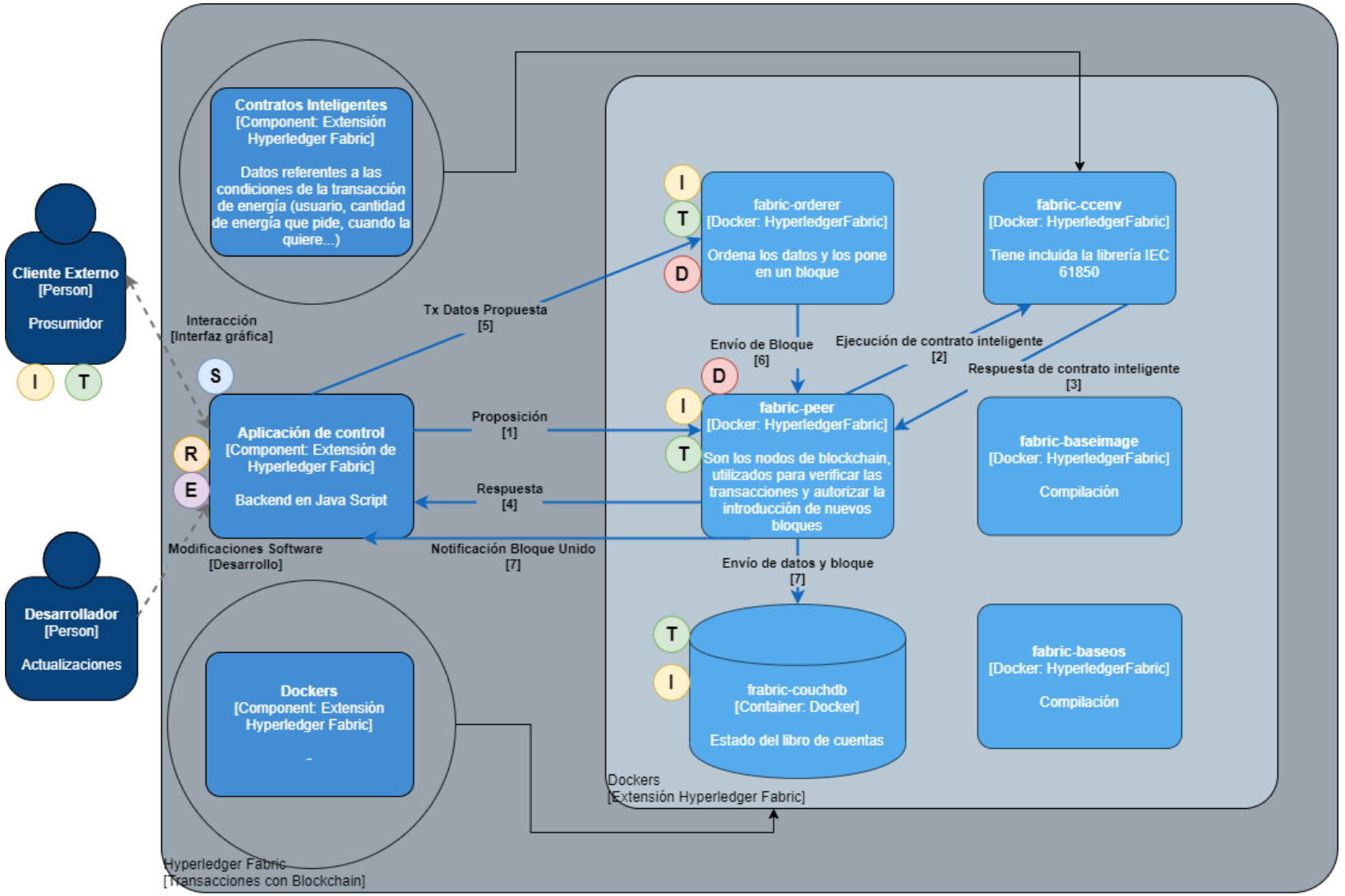

Figura 52. C4 Model Hyperledger Fabric.

En la Figura 53 se puede observar el C4 Model correspondiente a ROS, en el que se pueden observar los 4 nodos que se han creado para gestionar la información de la microrred:

- Lectura de sensores físicos.
- Puente MQTT-ROS para realizar la comunicación con la estación meteorológica.
- Comunicación con el regulador DC mediante Modbus.
- Comunicación con Cliente IEC 61850 y EMS.

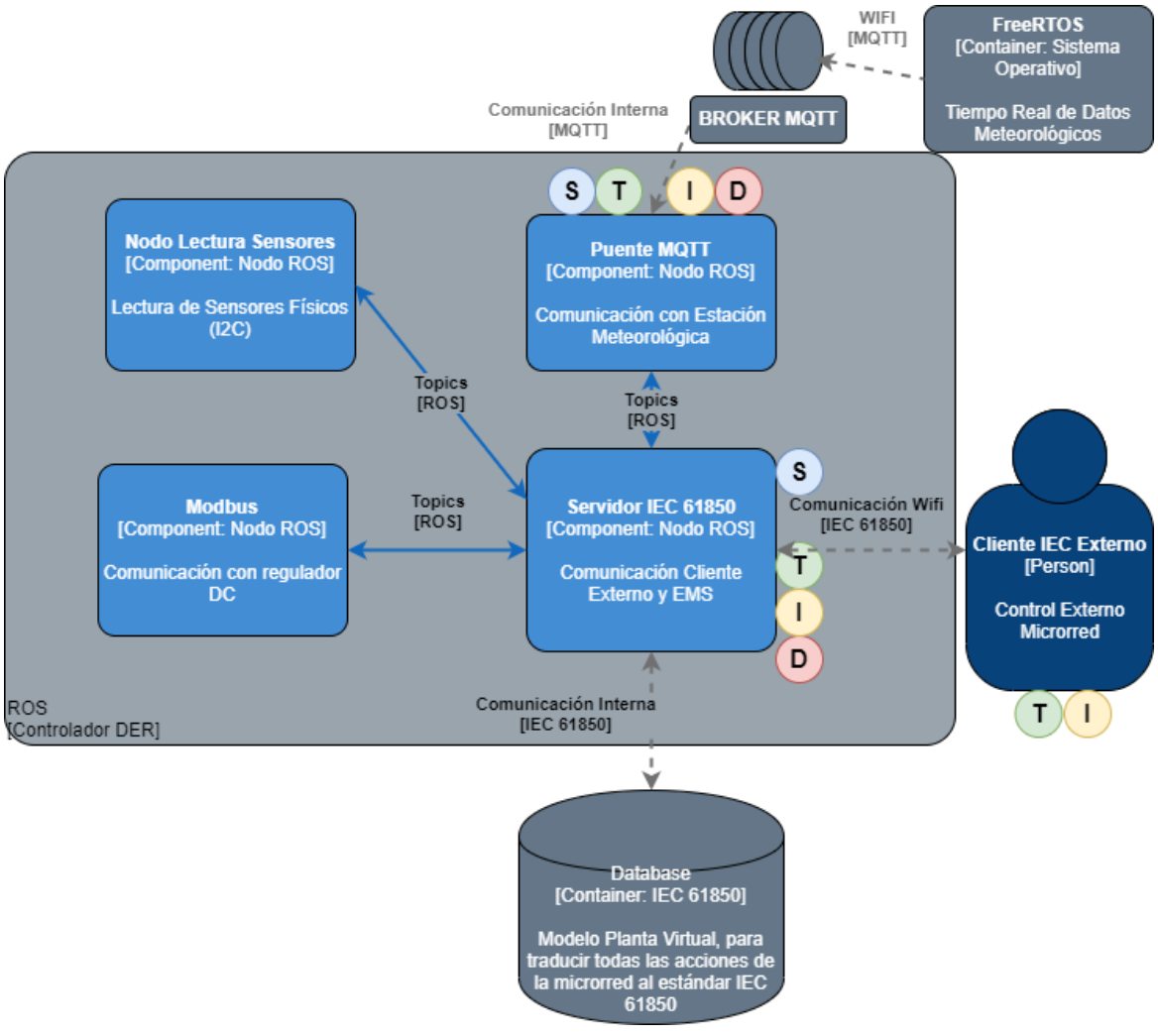

Figura 53. C4 Model ROS.

En la Figura 54 se pueden apreciar los flujos de información entre los distintos nodos que se han creado en NodeRED para diseñar el HMI.

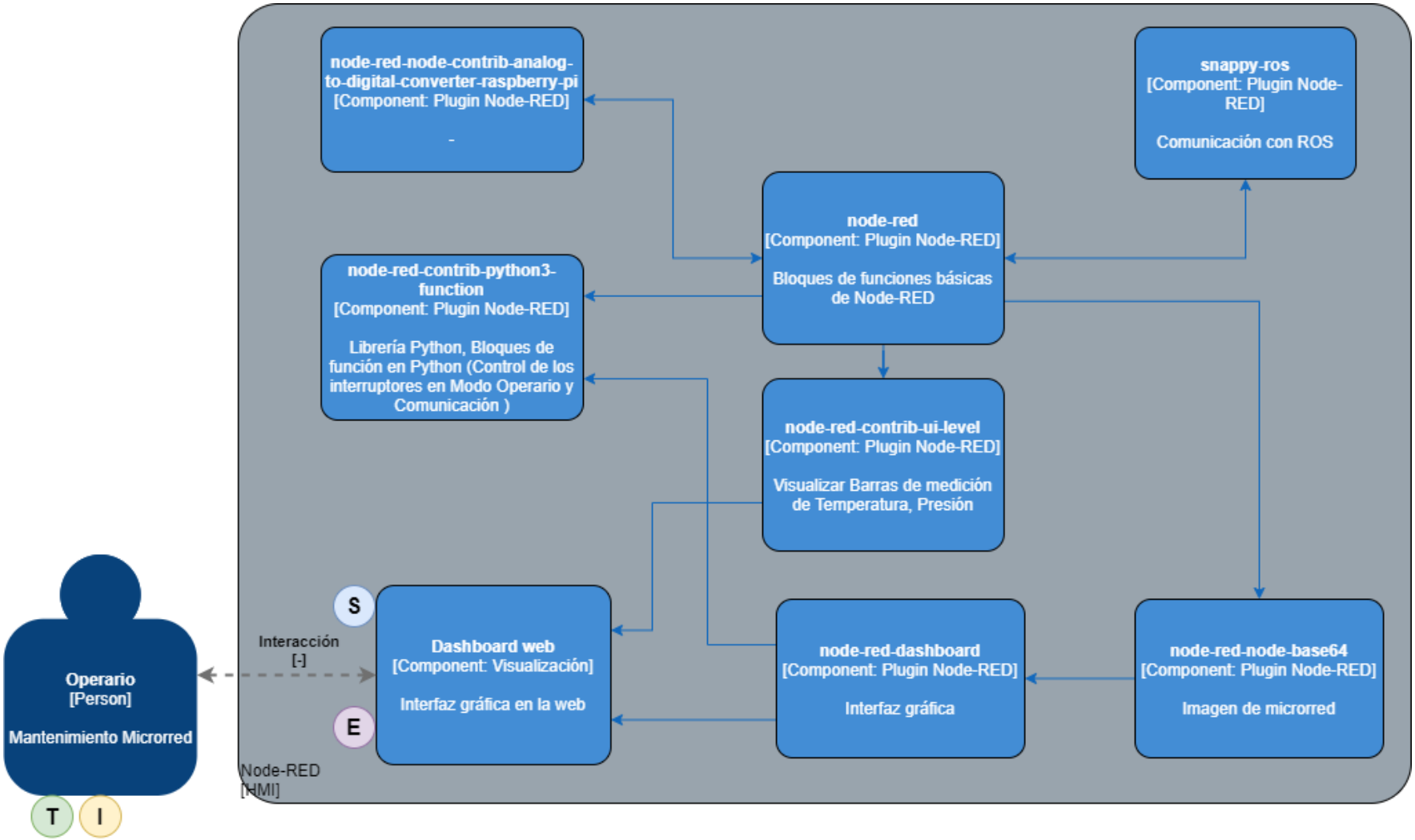

Figura 54. C4 Model NodeRED.

Apéndice B - Tablas de evaluación de riesgos

B.1. Tabla de evaluación de impacto total

Código Amenaza	Activo	Amenazas STRIDE	Código Magerit	I	C	D	Impacto
2	Base de Datos IEC 61850	Tampering	[A.15]	5	3	1	**3**
3	Base de Datos IEC 61850	Information Disclosure	[A.14]	3	5	1	**3**
4	Comunicación Wifi (IEC61850) Cliente IEC 61850 hacia ROS	Spoofing	[A.5]	5	5	5	**5**
5	Comunicación Wifi (IEC61850) Cliente IEC 61850 hacia ROS	Tampering	[A.15]	5	3	1	**3**
6	Comunicación Wifi (IEC61850) Cliente IEC 61850 hacia ROS	Information Disclosure	[A.14]	3	5	1	**3**
7	Comunicación Wifi (IEC61850) Cliente IEC 61850 hacia ROS	Denial of Service	[A.24]	1	1	5	**3**
8	Comunicación Wifi (IEC61850) ROS hacia Cliente IEC 61850	Tampering	[A.15]	5	3	1	**3**
9	Comunicación Wifi (IEC61850) ROS hacia Cliente IEC 61850	Information Disclosure	[A.14]	3	5	1	**3**
10	Comunicación Wifi (MQTT) Broker MQTT hacia ROS	Spoofing	[A.5]	5	5	5	**5**
11	Comunicación Wifi (MQTT) Broker MQTT hacia ROS	Tampering	[A.15]	5	3	1	**3**
12	Comunicación Wifi (MQTT) Broker MQTT hacia ROS	Information Disclosure	[A.14]	3	5	1	**3**
13	Comunicación Wifi (MQTT) Broker MQTT hacia ROS	Denial of Service	[A.24]	1	1	5	**3**
14	Interacción Desarrollador hacia ROS	Spoofing	[A.5]	5	5	5	**5**
15	Interacción Desarrollador hacia ROS	Elevation of Privilege	[A.11]	5	5	5	**5**

16	Comunicación Wifi MQTT de FreeRTOS hacia Broker MQTT	Spoofing	[A.5]	5	5	5	**5**
17	Comunicación Wifi MQTT de FreeRTOS hacia Broker MQTT	Tampering	[A.15]	5	3	1	**3**
18	Comunicación Wifi MQTT de FreeRTOS hacia Broker MQTT	Information Disclosure	[A.14]	3	5	1	**3**
19	Comunicación Wifi MQTT de FreeRTOS hacia Broker MQTT	Denial of Service	[A.24]	1	1	5	**3**
20	Interacción Desarrollador hacia Node-RED	Spoofing	[A.5]	5	5	5	**5**
21	Interacción Desarrollador hacia Node-RED	Elevation of Privilege	[A.11]	5	5	5	**5**
22	Comunicación Remota Operario Mantenimiento hacia Node-RED	Spoofing	[A.5]	5	5	5	**5**
23	Comunicación Remota Operario Mantenimiento hacia Node-RED	Tampering	[A.15]	5	3	1	**3**
24	Comunicación Remota Operario Mantenimiento hacia Node-RED	Information Disclosure	[A.14]	3	5	1	**3**
25	Comunicación Remota Operario Mantenimiento hacia Node-RED	Elevation of Privilege	[A.11]	5	5	5	**5**
26	Comunicación Node-RED hacia Operario Mantenimiento	Tampering	[A.15]	5	3	1	**3**
27	Comunicación Node-RED hacia Operario Mantenimiento	Information Disclosure	[A.14]	3	5	1	**3**
28	Interacción Desarrollador hacia Hyperledger Fabric	Spoofing	[A.5]	5	5	5	**5**
29	Interacción Desarrollador hacia Hyperledger Fabric	Elevation of Privilege	[A.11]	5	5	5	**5**
30	Comunicación Prosumidor con Hyperledger Fabric	Spoofing	[A.5]	5	5	5	**5**
31	Comunicación Prosumidor hacia	Tampering	[A.15]	5	2	1	**3**

	Hyperledger Fabric						
32	Comunicación Prosumidor hacia Hyperledger Fabric	Repudiation	[A.13]	5	2	1	**3**
33	Comunicación Prosumidor hacia Hyperledger Fabric	Information Disclosure	[A.14]	3	5	1	**3**
34	Comunicación Prosumidor hacia Hyperledger Fabric	Denial of Service	[A.24]	1	1	3	**2**
35	Comunicación Prosumidor hacia Hyperledger Fabric	Elevation of Privilege	[A.11]	5	5	5	**5**
36	Comunicación Hyperledger Fabric hacia Prosumidor	Tampering	[A.15]	5	3	1	**3**
37	Comunicación Hyperledger Fabric hacia Prosumidor	Information Disclosure	[A.14]	3	5	1	**3**
38	Desarrollador hacia FreeRTOS	Spoofing	[A.5]	5	5	5	**5**
39	Comunicación MQTT de Broker MQTT hacia ThingSpeak	Spoofing	[A.5]	5	5	5	**5**
40	Comunicación MQTT de Broker MQTT hacia ThingSpeak	Tampering	[A.15]	5	3	1	**3**
41	Comunicación MQTT de Broker MQTT hacia ThingSpeak	Information Disclosure	[A.14]	3	5	1	**3**

Tabla 12. Resultado evaluación de impacto total.

B.2. Tabla de evaluación de riesgo final

Código Amenaza	Activos	Amenazas STRIDE	Código Magerit	I	P	R	Posibles mitigaciones	Riesgo Final
2	Base de Datos IEC 61850	Tampering	[A.15]	3	2	**6**	Encriptar información	**1**
3	Base de Datos IEC 61850	Information Disclosure	[A.14]	3	2	**6**	Encriptar información	**1**
4	Comunicación Wifi (IEC61850) Cliente IEC 61850 hacia ROS	Spoofing	[A.5]	5	2	**10**	Control de acceso con roles	**2**
5	Comunicación Wifi (IEC61850) Cliente IEC	Tampering	[A.15]	3	4	**12**	Encriptar comunicación	**3**

	61850 hacia ROS							
6	Comunicación Wifi (IEC61850) Cliente IEC 61850 hacia ROS	Information Disclosure	[A.14]	3	4	**12**	Encriptar comunicación	**3**
7	Comunicación Wifi (IEC61850) Cliente IEC 61850 hacia ROS	Denial of Service	[A.24]	3	2	**6**	Detectar comandos anómalos	**1**
8	Comunicación Wifi (IEC61850) ROS hacia Cliente IEC 61850	Tampering	[A.15]	3	3	**9**	Encriptar comunicación	**3**
9	Comunicación Wifi (IEC61850) ROS hacia Cliente IEC 61850	Information Disclosure	[A.14]	3	3	**9**	Encriptar comunicación	**3**
10	Comunicación Wifi (MQTT) Broker MQTT hacia ROS	Spoofing	[A.5]	5	3	**15**	Control de acceso con roles	**4**
11	Comunicación Wifi (MQTT) Broker MQTT hacia ROS	Tampering	[A.15]	3	3	**9**	Encriptar comunicación	**2**
12	Comunicación Wifi (MQTT) Broker MQTT hacia ROS	Information Disclosure	[A.14]	3	3	**9**	Encriptar comunicación	**2**
13	Comunicación Wifi (MQTT) Broker MQTT hacia ROS	Denial of Service	[A.24]	3	3	**9**	Detectar comandos anómalos	**3**
14	Interacción Desarrollador hacia ROS	Spoofing	[A.5]	5	1	**5**	Control de acceso con roles	**1**
15	Interacción Desarrollador hacia ROS	Elevation of Privilege	[A.11]	5	1	**5**	Control de acceso con roles	**1**
16	Comunicación Wifi MQTT de FreeRTOS	Spoofing	[A.5]	5	3	**15**	Control de acceso con roles	**4**

	hacia Broker MQTT							
17	Comunicación Wifi MQTT de FreeRTOS hacia Broker MQTT	Tampering	[A.15]	3	4	**12**	Encriptar comunicación	**2**
18	Comunicación Wifi MQTT de FreeRTOS hacia Broker MQTT	Information Disclosure	[A.14]	3	4	**12**	Encriptar comunicación	**2**
19	Comunicación Wifi MQTT de FreeRTOS hacia Broker MQTT	Denial of Service	[A.24]	3	4	**12**	Detectar comandos anómalos	**3**
20	Interacción Desarrollador hacia Node-RED	Spoofing	[A.5]	5	1	**5**	Control de acceso con roles	**1**
21	Interacción Desarrollador hacia Node-RED	Elevation of Privilege	[A.11]	5	2	**10**	Control de acceso con roles	**2**
22	Comunicación Remota Operario Mantenimiento hacia Node-RED	Spoofing	[A.5]	5	2	**10**	Control de acceso con roles	**2**
23	Comunicación Remota Operario Mantenimiento hacia Node-RED	Tampering	[A.15]	3	2	**6**	Red privada virtual	**2**
24	Comunicación Remota Operario Mantenimiento hacia Node-RED	Information Disclosure	[A.14]	3	2	**6**	Red privada virtual	**2**
25	Comunicación Remota Operario Mantenimiento hacia Node-RED	Elevation of Privilege	[A.11]	5	3	**15**	Control de acceso	**1**
26	Comunicación Node-RED hacia Operario	Tampering	[A.15]	3	3	**9**	Detectar datos anómalos	**3**

	Mantenimiento							
27	Comunicación Node-RED hacia Operario Mantenimiento	Information Disclosure	[A.14]	3	3	**9**	Red privada virtual	**3**
28	Interacción Desarrollador hacia Hyperledger Fabric	Spoofing	[A.5]	5	1	**5**	Control de acceso con roles	**1**
29	Interacción Desarrollador hacia Hyperledger Fabric	Elevation of Privilege	[A.11]	5	1	**5**	Control de acceso con roles	**1**
30	Comunicación Prosumidor con Hyperledger Fabric	Spoofing	[A.5]	5	2	**10**	Control de acceso con roles	**3**
31	Comunicación Prosumidor hacia Hyperledger Fabric	Tampering	[A.15]	3	1	**3**	Encriptar comunicación	**1**
32	Comunicación Prosumidor hacia Hyperledger Fabric	Repudiation	[A.13]	3	1	**3**	Blockchain	**3**
33	Comunicación Prosumidor hacia Hyperledger Fabric	Information Disclosure	[A.14]	3	2	**6**	Encriptar comunicación	**1**
34	Comunicación Prosumidor hacia Hyperledger Fabric	Denial of Service	[A.24]	2	1	**2**	Detectar comandos anómalos	**1**
35	Comunicación Prosumidor hacia Hyperledger Fabric	Elevation of Privilege	[A.11]	5	2	**10**	Control de acceso con roles	**3**
36	Comunicación Hyperledger Fabric hacia Prosumidor	Tampering	[A.15]	3	2	**6**	Red privada virtual	**2**

37	Comunicación Hyperledger Fabric hacia Prosumidor	Information Disclosure	[A.14]	3	2	**6**	Red privada virtual	**2**
38	Desarrollador hacia FreeRTOS	Spoofing	[A.5]	5	1	**5**	Control de acceso con roles	**1**
39	Comunicación MQTT de Broker MQTT hacia ThingSpeak	Spoofing	[A.5]	5	3	**15**	Control de acceso con roles	**3**
40	Comunicación MQTT de Broker MQTT hacia ThingSpeak	Tampering	[A.15]	3	3	**9**	Encriptar comunicación	**3**
41	Comunicación MQTT de Broker MQTT hacia ThingSpeak	Information Disclosure	[A.14]	3	3	**9**	Encriptar comunicación	**3**

Tabla 13. Resultado obtención de riesgo final.

Apéndice C - Código

C.1. Código C++ ESP32 sin seguridad

```
#include <WiFi.h>
#include <PubSubClient.h>
#include <Wire.h>


char ssid[] = "";       // PONER AQUÍ NOMBRE DE LA RED
char password[] = ""; // PONER AQUÍ CONTRASEÑA DE LA RED


const char* mqtt_server = "192.168.11.2";     // MQTT BROKER IP

const char* id = "ESP8266Client";             // ID CLIENTE

WiFiClient espClient;
PubSubClient client(espClient);

long lastMsg = 0;
char msg[50];
int value = 0;


float temperature = 0;
float humidity = 0;

//////////////////////////////////////////////////////////////////////
//////////////////////////////////////////
//////////////////////////////////////////////////////////////////////
//////////////////////////////////////////


void setup_wifi() {
  delay(10);
  // We start by connecting to a WiFi network
  Serial.println();
  Serial.print("Connecting to ");
  Serial.println(ssid);

  WiFi.begin(ssid, password);

  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }

  Serial.println("");
  Serial.println("WiFi connected");
  Serial.println("IP address: ");
  Serial.println(WiFi.localIP());
}
```

```
void reconnect() {
  // Loop until we're reconnected
  while (!client.connected()) {
    Serial.print("Attempting MQTT connection...");
    // Attempt to connect
    if (client.connect(id,user,pass)) {
      Serial.println("connected");
      // Subscribe
      client.subscribe("esp32/output");
    } else {
      Serial.print("failed, rc=");
      Serial.print(client.state());
      Serial.println(" try again in 5 seconds");
      // Wait 5 seconds before retrying
      delay(5000);
    }
  }
}

/////////////////////////////////////////
/////////////////////////////////////////////////////////////////////////
/////////////////////////////////////////

void setup() {
  Serial.begin(115200);

  setup_wifi();
  client.setServer(mqtt_server, 1883);


}

/////////////////////////////////////////
/////////////////////////////////////////////////////////////////////////
/////////////////////////////////////////

void loop() {
  if (!client.connected()) {
    reconnect();
  }
  client.loop();

  long now = millis();
  if (now - lastMsg > 5000) {
    lastMsg = now;

    humidity = 53.34;

    // Convert the value to a char array
    char humString[6];
    dtostrf(humidity, 1, 2, humString);
    Serial.print("Humidity: ");
    Serial.println(humString);
    client.publish("estacion/humidity", humString);

    delay(2000);
    temperature = 23.23;

    // Convert the value to a char array
    char tempString[6];
    dtostrf(temperature, 1, 2, tempString);
    Serial.print("Temperature: ");
    Serial.println(tempString);
```

```
    client.publish("estacion/temperature", tempString);

  }
}
```

C.2. Código C++ ESP32 con seguridad

```
#include <WiFi.h>
#include "src/dependencies/WiFiClientSecure/WiFiClientSecure.h"
//using ESPRESSIF OFFICIAL WiFiClientSecure
#include <time.h>
#include <PubSubClient.h>

#ifndef SECRET
  const char ssid[] = "GEISER-HELIOS";
  const char pass[] = "";

  #define HOSTNAME "MQTT-STATION"

  const char *MQTT_HOST = "192.168.11.2"; // MQTT BROKER IP
  const int MQTT_PORT = 8883;             // MQTT PORT
  const char *MQTT_USER = "mqtt-explorer";// MQTT USUARIO
  const char *MQTT_PASS = "1234";         // MQTT CONTRASEÑA


  const char* local_root_ca = \
    "-----BEGIN CERTIFICATE-----\n" \
"MIID3zCCAsegAwIBAgIUMiKPdChjGRtwth/sYq1lDDnT6kAwDQYJKoZIhvcNAQEL\n" \
"BQAwfzELMAkGA1UEBhMCRVMxDzANBgNVBAgMBk1hZHJpZDEaMBgGA1UEBwwRQWxj\n" \
"YWxhIGRlIEhlbmFyZXMxHjAcBgNVBAoMFVVuaXZlcnNpZGFkIGRlIEFsY2FsYTEM\n" \
"MAoGA1UECwwDVUFIMRUwEwYDVQQDDAwxOTIuMTY4LjExLjIwHhcNMjEwNTA1MDg0\n" \
"ODAyWhcNMjYwNTA1MDg0ODAyWjB/MQswCQYDVQQGEwJFUzEPMA0GA1UECAwGTWFk\n" \
"cmlkMRowGAYDVQQHDBFBbGNhbGEgZGUgSGVuYXJlczEeMBwGA1UECgwVVW5pdmVy\n" \
"c2lkYWQgZGUgQWxjYWxhMQwwCgYDVQQLDANVQUgxFTATBgNVBAMMDDE5Mi4xNjgu\n" \
"MTEuMjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL+VSEGgXNpzTYiX\n" \
"cSxNaPik9OuPVWtJcKgfwdBkurE1q7qlUwcNOk6fN9GiyCVqs5vUYMbWfSjt+rjt\n" \
"5ejV5SI4uO4qwKObZeLEIGBqu/m4ezYVxWJ2cT2cMOcTzasiHHX+xZsTukuf7zgb\n" \
"iD/AGdMMGBKNINYQWnQhQGbHqmo88d3Wvf8+p4x1NPq74Us7bbpzTklySMR9Bqjw\n" \
"yNzZWMGxAqLs0ffIqRo9wTu/sA1RCKFp1v/0WvSwNkH9YAp4Inw1zDMaf3S12sLe\n" \
"Lo/B+k9SGfDjNYXCk0oPsCPvHT6ap7LVUyiDnS/yA2NDQoIcOCzTAWGjPUTyrFfu\n" \
"hanU/k8CAwEAAaNTMFEwHQYDVR0OBBYEFJuPOaFY84EQDXpPm/LD1DK7XOh0MB8G\n" \
"A1UdIwQYMBaAFJuPOaFY84EQDXpPm/LD1DK7XOh0MA8GA1UdEwEB/wQFMAMBAf8w\n" \
"DQYJKoZIhvcNAQELBQADggEBABg0a2bxIUxVMtBOZyO69hvdH4zYWAuO1ivKUotS\n" \
"FsMg4479wsNUftwQSWZjEdLO7TQa8nVUhiESSOmmhp8tPTHcI8AUirjK29FKS5yb\n" \
"PGD6cQTVCxvb76FrwqgsWeQJYpmZv9/aLwdD6k9Aag8ZqdCQs0ebWrkdRE31lpvZ\n" \
"teQkLfAY7QjxkgX6nxuzbHwhKH7kVzwZjbjWc4OAyVdsjfOIilHBKbD5LCGW5rbH\n" \
"TzJnEsA7qlZurxfbuWhFIvGBRdKh7HdXh1BsO/8ku1xh+0pwWemQZ17mRXTv8gL9\n" \
"vhMG1/RfOEaeZAR5otxL2FkE2SSsFsFmwd961CHVDykoQHU=\n" \
    "-----END CERTIFICATE-----";

#endif

const char MQTT_SUB_TOPIC[] = "home/" HOSTNAME "/in";
const char MQTT_PUB_TOPIC[] = "home/" HOSTNAME "/out";

WiFiClientSecure mqttserver;
PubSubClient client(mqttserver);

time_t now;
unsigned long lastMillis = 0;
```

```
float temperature = 0;
float humidity = 0;


void mqtt_connect()
{
    while (!client.connected()) {
     client.connect(HOSTNAME, MQTT_USER, MQTT_PASS);
    Serial.print("MQTT connecting");

    if (client.connect(HOSTNAME, MQTT_USER, MQTT_PASS)) {
       Serial.println("connected");
      client.subscribe(MQTT_SUB_TOPIC);

    } else {
           Serial.print("failed, status code =");
      Serial.print(client.state());
      Serial.println("try again in 5 seconds");
      /* Wait 5 seconds before retrying */
      delay(5000);

    }
  }

}

void receivedCallback(char* topic, byte* payload, unsigned int length)
{
  Serial.print("Received [");
  Serial.print(topic);
  Serial.print("]: ");
  for (int i = 0; i < length; i++) {
    Serial.print((char)payload[i]);
  }
}

void setup()
{
  Serial.begin(115200);

  Serial.print("Attempting to connect to SSID: ");
  Serial.println(ssid);
  WiFi.setHostname(HOSTNAME);
  WiFi.mode(WIFI_AP_STA);
  WiFi.begin(ssid, pass);
  while (WiFi.status() != WL_CONNECTED)
  {
    Serial.print(".");
    delay(1000);
  }
  Serial.println();
  Serial.print("Connected to ");
  Serial.println(ssid);

  mqttserver.setCACert(local_root_ca);
  client.setServer(MQTT_HOST, MQTT_PORT);

  mqtt_connect();
}

void loop()
{
  now = time(nullptr);
```

```
  if (WiFi.status() != WL_CONNECTED)
  {
    Serial.print("Checking wifi");
    while (WiFi.waitForConnectResult() != WL_CONNECTED)
    {
      WiFi.begin(ssid, pass);
      Serial.print(".");
      delay(10);
    }
    Serial.println("connected");
  }
  else
  {
    if (!client.connected())
    {
      mqtt_connect();
    }
    else
    {
      client.loop();
    }
  }

  if (millis() - lastMillis > 5000) {
    lastMillis = millis();

              humidity = 53.34;

    // Convert the value to a char array
    char humString[6];
    dtostrf(humidity, 1, 2, humString);
    Serial.print("Humidity: ");
    Serial.println(humString);
    client.publish("estacion/humidity", humString);

    delay(2000);
            temperature = 23.23;

    // Convert the value to a char array
    char tempString[6];
    dtostrf(temperature, 1, 2, tempString);
    Serial.print("Temperature: ");
    Serial.println(tempString);
    client.publish("estacion/temperature", tempString);
  }
}
```

C.3. Código Python ataque contra integridad en MQTT

```
#Script para ataque contra integridad en MQTT

from netfilterqueue import NetfilterQueue
import socket
from scapy.all import *

target="estacion/temperature"
old_value="2"
new_value="9"


def print_and_accept(pkt):
```

```
   pkt2= IP(pkt.get_payload())
   h=IP(pkt.get_payload())
   if pkt2[IP].dst =='192.168.11.2':
      packet=IP(pkt.get_payload())
      if packet.haslayer(Raw):
         if(str(packet[Raw].load).find(target)!=-1 and
str(packet[Raw].load).find(old_value)!=-1):
            print("Has been found a Topic: "+target +" and Value:
"+old_value)
            print("Old Value"+packet[Raw].load)

packet[Raw].load=str(packet[Raw].load).replace(old_value,new_value)
            originalChecksum=packet['TCP'].chksum
            del packet['TCP'].chksum
            packet=IP(str(packet))
            recomputedChecksum=packet['TCP'].chksum
            print("Original checksum
"+str(originalChecksum)+"recomputedChecksum "+str(recomputedChecksum))
            new_packet=IP(str(packet))
            print("New value "+new_packet[Raw].load)
            print("sending new_packet...")
            send(new_packet)
         else:
            pkt.accept()
      else:
         pkt.accept()
   else:
     pkt.accept()

nfqueue = NetfilterQueue()
nfqueue.bind(1, print_and_accept)
s = socket.fromfd(nfqueue.get_fd(), socket.AF_UNIX,
socket.SOCK_STREAM)
try:
       nfqueue.run_socket(s)
except KeyboardInterrupt:
       print('')
s.close()
nfqueue.unbind()
```

Apéndice D – Manual de Instalación

D.1. Suricata IDS

D.1.1. Instalación

1. **sudo apt install libpcre3 libpcre3-dbg libpcre3-dev build-essential libpcap-dev libyaml-0-2 libyaml-dev pkg-config zlib1g zlib1g-dev make libmagic-dev libjansson-dev rustc cargo python-yaml python3-yaml liblua5.1-dev** - Instalación de Librerías necesarias.
2. **wget https://www.openinfosecfoundation.org/download/suricata-6.0.2.tar.gz** - Descarga de última versión estable 6.0.2.
3. **tar -xvf suricata-6.0.2.tar.gz** - Descompresión del archivo.
4. **cd $HOME/suricata-6.0.2/** - Directorio de instalación.
5. **./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var --enable-nfqueue --enable-lua** - Configuración de instalación, importante habilitar nfqueue.
6. **make** - Compilación.
7. **sudo make install** - Instalación.
8. **cd $HOME/suricata-6.0.2/suricata-update** - Directorio de instalación.
9. **sudo python setup.py build** - Compilación.
10. **sudo python setup.py install** - Instalación.
11. **cd $HOME/suricata-6.0.2** - Directorio de instalación.
12. **sudo make install-full** - Instalación de suricata con reglas.
13. **sudo suricata-update** - Actualización de las reglas.

D.1.2. Configuración de Suricata

El primer paso es configurar la red del host y las redes externas, así como los puertos por los que se van a realizar las comunicaciones como se puede observar en la Figura 55.

```
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    #HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
    HOME_NET: "[192.168.11.2]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    #EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"
    EXTERNAL_NET: "[192.168.11.6]"
    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: "$EXTERNAL_NET"
    DC_SERVERS: "$HOME_NET"
    DNP3_SERVER: "$HOME_NET"
    DNP3_CLIENT: "$HOME_NET"
    MODBUS_CLIENT: "$HOME_NET"
    MODBUS_SERVER: "$HOME_NET"
    ENIP_CLIENT: "$HOME_NET"
    ENIP_SERVER: "$HOME_NET"

  port-groups:
    HTTP_PORTS: "80"
    SHELLCODE_PORTS: "!80"
    ORACLE_PORTS: 1521
    SSH_PORTS: 22
    DNP3_PORTS: 20000
    MODBUS_PORTS: 502
    FILE_DATA_PORTS: "[$HTTP_PORTS,110,143]"
    FTP_PORTS: 21
    GENEVE_PORTS: 6081
    VXLAN_PORTS: 4789
    TEREDO_PORTS: 3544
    MQTT_PORT: 1883
```

Figura 55. Configuración de IP en suricata.yaml.

En Figura 56 se puede apreciar el procedimiento para habilitar la obtención de contraseñas del protocolo MQTT en Suricata IDS:

```
        - mqtt:
            # passwords: yes           # enable output of passwords
```

Figura 56. Habilitar obtención de contraseñas MQTT en suricata.yaml.

En la Figura 57 se puede observar la configuración para habilitar el *parser* de MQTT en Suricata IDS:

```
722     # MQTT, disabled by default.
723     mqtt:
724       # enabled: yes
725       # max-msg-length: 1mb
```

Figura 57. Habilitar procesamiento de paquetes MQTT en suricata.yaml.

En la Figura 58 se observa la configuración del directorio donde se van a guardar las reglas creadas para el protocolo MQTT:

```
1862 ## Configure Suricata to load Suricata-Update managed rules.
1863 ##
1864
1865 default-rule-path: /var/lib/suricata/rules
1866
1867 rule-files:
1868   - suricata.rules
```

Figura 58. Configuración de directorio de reglas en suricata.yaml.

D.1.3. Ejecución de Suricata en modo *Inline*

```
1  >> sudo iptables -I FORWARD -j NFQUEUE
2  >> sudo iptables -I INPUT -j NFQUEUE
3  >> sudo iptables -I OUTPUT -j NFQUEUE
```

Y seguidamente:

```
1  sudo suricata -c /etc/suricata/suricata.yaml -q 0
```

En la Figura 59 se puede observar el resultado que debe dar la ejecución correcta de Suricata IDS.

```
pi@raspberrypi:/etc/suricata $ sudo suricata -c /etc/suricata/suricata.yaml -q 0
3/6/2021 -- 12:25:26 - <Notice> - This is Suricata version 6.0.2 RELEASE running in SYSTEM mode
3/6/2021 -- 12:25:58 - <Notice> - all 6 packet processing threads, 4 management threads initialized, engine started.
```

Figura 59. Resultado de ejecución de Suricata IDS por terminal.

D.2. *Broker* Mosquitto [49]

D.2.1. Instalación

1. **sudo apt-get update** - Actualizar información de apt.
2. **sudo apt-get upgrade**
3. **sudo apt-cache mosquitto** - Comprobar paquetes.
4. **sudo apt-get install mosquitto mosquitto-clients** - Instalar.
5. **sudo systemctl enable mosquitto.service** - Configurar arranque al inicio.
6. **sudo systemctl status mosquitto.service** - Ver estado de mosquitto broker.

Una vez que se ha realizado la instalación se debe realizar una prueba de funcionamiento para comprobar que *broker* está ejecutándose de forma correcta.

D.2.2. Archivo de configuración mosquitto.conf sin seguridad

```
# Place your local configuration in /etc/mosquitto/conf.d/
#
# A full description of the configuration file is at
# /usr/share/doc/mosquitto/examples/mosquitto.conf.example

pid_file /var/run/mosquitto.pid

persistence true
persistence_location /var/lib/mosquitto/


include_dir /etc/mosquitto/conf.d

#Note that this will not allow anonymous access by default
listener 1883

#Save all log in file
log_dest file /var/log/mosquitto/mosquito.log
log_type all
log_timestamp true

#Contraseñas

password_file /etc/mosquitto/passwd
allow_anonymous false

```

Figura 60. Archivo mosquitto.conf sin seguridad.

D.2.3. Archivo de configuración mosquitto.conf con seguridad

```
# Place your local configuration in /etc/mosquitto/conf.d/
#
# A full description of the configuration file is at
# /usr/share/doc/mosquitto/examples/mosquitto.conf.example

pid_file /var/run/mosquitto.pid

persistence true
persistence_location /var/lib/mosquitto/


include_dir /etc/mosquitto/conf.d

#Note that this will not allow anonymous access by default
#listener 1883

#Save all log in file
log_dest file /var/log/mosquitto/mosquito.log
log_type all
log_timestamp true

#Con seguridad
listener 8883
cafile /etc/mosquitto/ca_certificates/ca.crt
certfile /etc/mosquitto/certs/server.crt
keyfile /etc/mosquitto/certs/server.key


#Contraseñas

password_file /etc/mosquitto/passwd
allow_anonymous false


```

Figura 61. Archivo mosquitto.conf con seguridad.

Universidad de Alcalá

Escuela Politécnica Superior

ESCUELA POLITECNICA SUPERIOR

Universidad de Alcalá