UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:
PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:
DISEÑO DE UNA ARQUITECTURA DE CIBERSEGURIDAD EN LA INFRAESTRUCTURA DE IOT ORIENTADO A ORGANIZACIONES TIPO PYME

AUTORES:
CARLOS ROBERTO CUAICAL ANGULO
ISRAEL SEBASTIÁN DE LA TORRE TRUJILLO

DIRECTOR:
JUAN CARLOS DOMÍNGUEZ AYALA

CUENCA – ECUADOR
2023

Autores:

Carlos Roberto Cuaical Angulo
Ingeniero Electrónico.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
ccuaical@est.ups.edu.ec

Israel Sebastián De la Torre Trujillo
Ingeniero Electrónico.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
idel2@est.ups.edu.ec

Dirigido por:

Juan Carlos Domínguez Ayala
Ingeniero de Sistemas.
Magister en Redes de Comunicaciones.
jdominguez@ups.edu.ec

DEDICATORIA

Este documento lo dedico con mucho cariño a mis padres porque por medio de su trabajo, sacrificio y sabiduría han sido mi inspiración para poder lograr mis metas.

A mis hermanas y hermano Thane, Sofia y Alejandro por apoyarme todos los días.

Carlos Roberto Cuaical Angulo

DEDICATORIA

Dedico este esfuerzo a Dios, quién siempre supo colocarme en el momento y lugar correcto con las personas correctas dándome la fuerza para perseverar en cada instante.

A mis padres, cuyo compromiso con verme triunfar hoy rinden frutos. Su amor incondicional es el cimiento sobre el cual construyo mis logros, cada uno es resultado de su amor y dedicación con la que han guiado mis pasos.

A mi querido hermano, quién es mi tesoro. Sin ti la vida no es vida verte feliz realmente me completa.

A mi tío, quién ha sido cómplice en mi vida profesional enseñándome a conquistar montañas.

A mis amigos, con quiénes hemos contemplado las amanecidas hombro a hombro.

Esta tesis no solo representa un triunfo académico, si no un tributo humilde y sincero a cada uno de ustedes. Sin su apoyo y amor, este logro carecería de significado.

Que estas palabras reflejen la gratitud profunda que siento en mi corazón, y que esta obra sea testimonio de mi amor y respeto hacia cada uno de ustedes.

Israel Sebastián De la Torre Trujillo

AGRADECIMIENTO

Agradezco a mis compañeros por todo su apoyo durante el proceso de formación académica, muchas gracias por toda su paciencia y esfuerzo.

Un agradecimiento muy especial a mis padres por apoyarme en todas las metas que me he planteado.

A todos quienes colaboraron en la preparación de este documento en especial al Ing. Juan Carlos Domínguez.

Carlos Roberto Cuaical Angulo

AGRADECIMIENTO

En el camino de completar esta tesis, he sido bendecido con el apoyo y la colaboración de personas excepcionales a las que deseo expresar mi más profundo agradecimiento.

A mi Tutor Juan Carlos Domínguez cuya orientación experta y visión crítica han sido fundamentales en la elaboración de este trabajo.

Expreso mi gratitud a mi familia, su apoyo constante es el motor que me ha impulsado a superar obstáculos y a perseguir las metas con determinación.

A mi compañero y amigo Carlos Cuaical, valió la pena cada amanecida!

Este logro no es solo mío, es el resultado de un esfuerzo colectivo.

Israel Sebastián De la Torre Trujillo

Tabla de Contenido

Diseño de una arquitectura de ciberseguridad en la infraestructura de IoT orientado a organizaciones tipo pyme

Autor(es):

Carlos Roberto Cuaical Angulo &
Israel Sebastián De la Torre Trujillo

Resumen

El presente trabajo plantea un diseño de arquitectura de ciberseguridad con una infraestructura de IoT orientado a las organizaciones tipo PYMES, acorde a las necesidades básicas de la organización.

La arquitectura que se propone funciona mediante el uso del protocolo MQTT/TLS, el cual será instalado en una Raspberry Pi que está configurada como bróker y dispositivos ESP32 que serán los clientes encargos de enviar la información recolectada por los sensores hacia el bróker, para que todo esto se pueda visualizar en una interfaz gráfica de fácil uso para el usuario.

Para la utilización del protocolo MQTT/TLS se muestra la manera de realizar certificados y llaves criptográficas con el programa de código abierto Openssl con el fin de realizar una comunicación segura.

Palabras clave:

Ciberseguridad, IoT, MQTT, TLS, Certificados criptográficos, OpenSSL, PYMES

ABSTRACT

The present work proposes an information security architecture design with an IoT infrastructure oriented to SME-type organizations or also known as small and medium-sized companies, analyzing the most common vulnerabilities suffered by this type of organization, following a guideline of the ISO 27001 standard, according to the needs of the organization.

The proposed architecture works using the MQTT/TLS protocol, which will be installed on a Raspberry Pi that is configured as a broker and ESP32 devices that will be the clients in charge of sending the information collected by the sensors to the broker, so that all this can be viewed in a user-friendly graphical interface.

For the use of the MQTT/TLS protocol, it shows how to create certificates and cryptographic keys with Openssl which is an open-source program to conduct secure communication.

Palabras clave:
Cybersecurity, IoT, MQTT, TLS, Cryptographic certificates, OpenSSL, PYMEs

1. INTRODUCCIÓN

Las organizaciones PYMES suelen enfrentar desafíos únicos cuando se trata de la seguridad cibernética, ya que a menudo cuentan con recursos limitados para implementar medidas de seguridad robustas. Además, con el aumento de la popularidad de IoT, estas organizaciones pueden estar expuestas a más riesgos de seguridad si no se implementan medidas de seguridad adecuadas.

La arquitectura de ciberseguridad propuesta utiliza el protocolo MQTT/TLS, que es un protocolo de comunicación de mensajes ligero y seguro que se utiliza comúnmente en aplicaciones de IoT. Al utilizar MQTT/TLS, se garantiza que la comunicación entre los dispositivos en la infraestructura de IoT es segura y protegida de posibles ataques.

La Raspberry Pi funciona como un bróker centralizado que recibe los datos de los dispositivos ESP32 que actúan como clientes. Los datos enviados por los clientes se cifran utilizando certificados y llaves criptográficas generados con el programa de código abierto OpenSSL para garantizar una comunicación segura.

2. Determinación del Problema

Dado que las organizaciones de pymes a menudo tienen recursos limitados para implementar medidas de seguridad cibernética robustas, pueden estar expuestas a riesgos de seguridad si no se toman medidas adecuadas. Además, con el aumento de la popularidad de IoT, las organizaciones pueden enfrentar un mayor riesgo de vulnerabilidades y ataques en sus dispositivos y sistemas de IoT.

Por lo tanto, el diseño de arquitectura de ciberseguridad propuesto busca proporcionar una solución escalable y rentable para garantizar la seguridad y protección de los datos en una infraestructura de IoT para organizaciones PYMES, utilizando el protocolo MQTT/TLS y certificados criptográficos generados con OpenSSL para asegurar una comunicación segura y protegida de posibles ataques.

3. Marco teórico referencial

El avance tecnológico en nuestro país ha tenido un gran impacto en cuanto al manejo de datos e implementación de la IoT para las diferentes actividades en las organizaciones tipo Pymes; ya que, día con día estas empresas necesitan acceder a grandes cantidades de información, además de otras funcionalidades, por lo que en la mayoría de los casos requiere un gran presupuesto para una correcta implementación tal como lo menciona Cari Marcelo en su tesis: “Diseño de una Arquitectura de ciberseguridad para los servicios de plataformas IoT en el área de TI dentro de la empresa Pacífico Seguros”, además menciona que la automatización que proporciona la IoT hace que se genere un tráfico de datos importantes para una empresa, entonces si no se trata de manera correcta, toda esa información se vuelve vulnerable a posibles ataques cibernéticos con fines perjudiciales (Lombardi & Arevalo, 2020).

Por lo tanto, considerando los grandes beneficios de la tecnología IoT, también se deben tener en cuenta sus debilidades o posibles vulnerabilidades en este tipo de organizaciones, ya que la mayoría de los fabricantes de IoT desarrollan componentes para permitir que los dispositivos se conecten. Esto es una desventaja porque los objetos conectados a Internet están expuestos, lo que convierte a estos dispositivos en objetivos fáciles para los ciberdelincuentes, ya que aprovechan esta vulnerabilidad para ataques informáticos. Como resultado, muchas unidades de negocio se vieron afectadas, como el caso del proveedor de Internet estadounidense Dyn en 2016, los ciberdelincuentes han llevado a cabo un ataque a sus sistemas de dominio de internet, afectando principalmente a la costa este de EE. UU., registrando un volumen de tráfico de 1,2 terabytes por segundo. Este tipo de ataque se conoce como Botnet Mirai, en el que el programa maligno o programas maliciosos afectan a los sitios web de empresas conocidas como Amazon, PayPal y Spotify (Morales Suárez et al., 2019).

Analizando a detalle, algunas aplicaciones y dispositivos IoT no cuentan con las políticas de ciberseguridad adecuadas, esto se debe a que muchos fabricantes y desarrolladores de software dejan de brindarle soporte como actualizaciones y parches o no cuentan con dispositivos de ciberseguridad para protección de la información (Morales Suárez et al., 2019).

Uno de los ciberataques más conocidos a nivel mundial conocidos fue WannaCry, este ataque afectó a varias empresas internacionales con la intención de captación de sus datos y la petición de un rescate de 300 dólares en bitcoins, luego de este ataque informático, la empresa de Microsoft se centró en actualizar de inmediato los sistemas operativos con un parche para cubrir esa vulnerabilidad (Lombardi & Arevalo, 2020).

Ahora debido a la pandemia el uso de la IoT se ha ampliado bastante debido a la necesidad de estos medios de comunicación y dispositivos para realizar diferentes trabajos y actividades alrededor del mundo y los ciberataques no se quedaron atrás; tenemos otro ejemplo de ataque cibernético el cual ocurrió en junio del 2017, donde la empresa MAERSK sufrió un ataque de ransomware el cual afectó de manera directa realizando una entrada abrupta a su sistema generando pérdidas de 264 millones de dólares, en la investigación realizada de este ataque informático se determinó que el ataque se llevó cabo gracias a la instalación de un software no controlado en la laptop de un empleado en Ucrania; más tarde en el mismo año una empresa llamada “COSCO” sufrió un ataque de dos alteraciones operativas en su sede de Estados Unidos y en septiembre del 2018 el puerto de Barcelona en España fue víctima de ataques de ransomware provocando alteraciones en sus actividades administrativas, dejándoles sin información de las pérdidas económicas debido al ataque (Naciones Unidas, 2020).

Las pérdidas económicas por ataques de ciberseguridad incrementan a medida que la digitalización o virtualización de los procesos y actividades avanzan. Además, es importante tener en cuenta que estas cifras de pérdidas económicas expuestas son únicamente de los ataques denunciados, debido a que muchos de estos incidentes

no son reportados para no dañar la reputación de la empresa y son solucionados de manera privada (Naciones Unidas, 2020).

Por lo tanto, si tomamos en cuenta que los ataques cibernéticos siguen en aumento conforme avanza la tecnología se debe disponer de una buena infraestructura de ciberseguridad para este tipo de dispositivos y asegurar los datos que puedan tener ya que si no se dispone de dicha arquitectura de IoT las consecuencias serían catastróficas hasta irremediables, ya que los ciberdelincuentes tendrían la facilidad de ingresar a los dispositivos con vulnerabilidades y comprometer nuestra información además de proporcionar una variedad de entradas y convertir a los dispositivos como un mediador para todo tipo de actividades inseguras (Caiza Narváez et al., 2021).

Por lo que es necesario atender la necesidad de la implementación de medidas de ciberseguridad en la red para los dispositivos IoT, y con ello el funcionamiento de la inteligencia artificial, ya que existe un mecanismo que actualmente se utiliza en todo el mundo para diferentes operaciones que acorta los Espacios de seguridad que se pueden presentar en los sistemas de red, provocando que aumente el riesgo de que los datos se vean comprometidos, creando así las herramientas y mecanismos adecuados que brinden un alto nivel de seguridad, reduciendo así la posibilidad de sufrir un ataque cibernético y la amenaza a los diferentes dispositivos debido a que los riesgos cibernéticos ya no son amenazas inusuales. Actualmente muchas empresas del sector público y privado intentan mejorar sus sistemas de seguridad invirtiendo grandes sumas de dinero y buscan académicos que puedan desarrollar alternativas que se adapten a las necesidades de cada uno de estos para proteger sus datos, sin embargo, esto genera altos costos, que algunas organizaciones no se lo pueden permitir, dejando sus dispositivos en riesgo y vulnerables a ataques, por lo que buscan crear una arquitectura IoT para crear protección en estos dispositivos, lo que permite el análisis de tráfico malicioso (Caiza Narváez et al., 2021).

En el proceso de construcción de la arquitectura adecuada de IoT, es importante destacar los estudios previos los mismos que sirven como ejemplo para llevar a cabo

esta investigación, en 2021 en un estudio realizado por Chulde L., a través de un diseño de modelo de ciberseguridad en el cual mediante el análisis y tratamiento de los riesgos, identifica los activos, las amenazas, el impacto y las salvaguardas, aplicando la metodología Maggerit, con el fin de diseñar el modelo de ciberseguridad IADI mediante los controles elegidos de la norma de seguridad ISO/IEC 27002:2017(Chulde & Défaz, 2021), también tenemos otro ejemplo de arquitectura donde M. Aminu Lawal en 2020, desarrolla un estudio que propone un marco de reducción de anomalías para IoT, utilizando la computación en red para garantizar una detección de anomalías más rápida y precisa, los métodos de detección utilizados en este estudio basado en firmas y anomalías para sus dos módulos.

De esta forma, los módulos basados en firmas utilizan una base de datos de fuentes de ataque, como direcciones IP incluidas en la lista negra, para garantizar una detección más rápida y eficiente cuando los ataques a la red se realizan desde direcciones IP incluidas en la lista negra, mientras que los módulos basados en firmas basadas en firmas anómalas utilizan un Gradient Boosting extremo. Algoritmo para la clasificación precisa del tráfico de red normal o anormal que arroja los resultados de los dos métodos de emisión actuales. En un estudio realizado por H. Haddad Pajouh en 2020, se propone una arquitectura de seguridad para la infraestructura de capa de borde de IoT, denominada arquitectura AI4SAFE-IoT, que se basa en módulos de seguridad basados en IA de capa de borde para proteger la infraestructura de IoT y analiza la atribución de amenazas cibernéticas, firewalls de aplicaciones web inteligentes, búsqueda de amenazas e inteligencia de amenazas cibernéticas (Haddad Pajouh et al., 2020).

Con base en toda la información recopilada y los datos relevantes sobre los ataques cibernéticos, este estudio tiene como objetivo hacer recomendaciones de diseño para la infraestructura de ciberseguridad, respaldando posibles soluciones a los principales problemas de los ataques de vulnerabilidad de dispositivos. Análisis de la implementación de algunos mecanismos de seguridad de IoT Esta técnica considera los protocolos de seguridad de la red, los modelos de arquitectura de

comunicación y el análisis de las vulnerabilidades y amenazas más comunes en los entornos de IoT y cómo se pueden mitigar mediante la implementación de mecanismos de seguridad de IoT.

3.1 Conceptos básicos

Para realizar la propuesta de diseño de la arquitectura de seguridad de la información, se debe tener claro los conceptos básicos y los fundamentos teóricos necesarios para implementarlos de manera eficaz y correcta, por lo cual a continuación se dará a conocer los conceptos que están relacionados con nuestra propuesta de diseño:

3.1.1. Pyme (pequeñas y medianas empresas)

Se puede definir a las Pymes como pequeñas empresas conformadas por menos de 20 trabajadores y empresas medianas que disponen entre 20 y 500 trabajadores. Sin embargo, esta definición puede variar de acuerdo con el contexto que se maneje en cada país según lo económico o hechos históricos por lo que no existe una definición exacta que le describa como tal a las Pymes debido a los diferentes y diversos criterios acerca de este tipo de organización (Iavarone Gisella Paula, 2012).

Las primeras PYMES en el Ecuador surgieron en las industrias textil, transporte y metal, antes de expandirse al comercio y los servicios, sin embargo, a principios del siglo XX, las empresas tipo PYME evolucionaron para poder expandir su gestión empresarial no solo a nivel nacional sino también en el extranjero grandes corporaciones, corporaciones y conglomerados, que dan lugar al surgimiento de corporaciones multinacionales, que surgen en el proceso de expansión del mercado empresarial (Rodríguez-Mendoza & Aviles-Sotomayor, 2020).

3.1.2. Internet de las cosas (IoT)

Actualmente alrededor del mundo existe una gran cantidad de dispositivos electrónicos los cuales utilizan los servicios de internet tanto para los hogares como para el campo laboral y estudiantil. A estos dispositivos también se los llama objetos

inteligentes y no es necesario que sean operados directamente por un ser humano, ya que existen componentes electrónicos existentes en edificios, vehículos o están distribuidos en cualquier lugar (Morales Suárez et al., 2019). En Ingeniería se utiliza el término redes de objetos inteligentes para referirse a la Internet de las Cosas, por lo tanto, estos objetos inteligentes se los puede definir como dispositivos que comúnmente tienen algunas limitaciones como: la cantidad de energía, la memoria, capacidad procesamiento y el ancho de banda. En el trabajo empresarial se organiza en base a requisitos establecidos para permitir la interoperabilidad entre varios tipos de objetos inteligentes, además, se puede añadir que el internet de las cosas es una infraestructura mundial para la comunidad informática que proporciona la prestación de servicios mediante la interconexión de objetos, ya sea físicos o virtuales gracias a la interconexión de estos (Rose et al., 2015).

También se la puede definir como una red constituida por objetos físicos que poseen sensores, software y otro tipo de tecnologías con el propósito de realizar una conexión e intercambiar datos con otros dispositivos electrónicos y sus sistemas a través de la red de internet, estos objetos pueden ser dispositivos de uso doméstico, empresarial o estudiantil, tales como teléfonos inteligentes, computadoras, teléfonos IP, etc (Jhordany Serna Valdivia & Mejia Miranda, 2020).

3.1.3. Internet de las cosas (IoT)

Actualmente alrededor del mundo existe una gran cantidad de dispositivos electrónicos los cuales utilizan los servicios de internet tanto para los hogares como para el campo laboral y estudiantil. A estos dispositivos también se los llama objetos inteligentes y no es necesario que sean operados directamente por un ser humano, ya que existen componentes electrónicos existentes en edificios, vehículos o están distribuidos en cualquier lugar (Morales Suárez et al., 2019). En Ingeniería se utiliza el término redes de objetos inteligentes para referirse a la Internet de las Cosas, por lo tanto, estos objetos inteligentes se los puede definir como dispositivos que comúnmente tienen algunas limitaciones como: la cantidad de energía, la memoria, capacidad procesamiento y el ancho de banda. En el trabajo empresarial se organiza en base a requisitos establecidos para permitir la interoperabilidad entre varios

tipos de objetos inteligentes, además, se puede añadir que el internet de las cosas es una infraestructura mundial para la comunidad informática que proporciona la prestación de servicios mediante la interconexión de objetos, ya sea físicos o virtuales gracias a la interconexión de estos (Rose et al., 2015).

También se la puede definir como una red constituida por objetos físicos que poseen sensores, software y otro tipo de tecnologías con el propósito de realizar una conexión e intercambiar datos con otros dispositivos electrónicos y sus sistemas a través de la red de internet, estos objetos pueden ser dispositivos de uso doméstico, empresarial o estudiantil, tales como teléfonos inteligentes, computadoras, teléfonos IP, etc (Jhordany Serna Valdivia & Mejia Miranda, 2020).

Se lo puede definir como programa que concede a los usuarios el libre uso de este con fines de estudiarlo o realizar algunos cambios en su código con el propósito de mejorar sus funcionalidades y luego distribuirlo a toda la comunidad informática, actualmente el software libre es muy importante, ya que con este tipo software, el usuario tiene acceso a su código fuente y así poder modificarlo de acuerdo con los criterios y necesidades para su uso en una organización. El uso más importante de este tipo de software se da en las empresas y las instituciones educativas ya que no tiene costo alguno. A continuación, se muestra las características principales del Software libre (Guzmán Y Valle et al., 2019):

- Su código es abierto.
- Se puede modificar el código.
- Libertad de estudiarlo y adaptarlo a sus necesidades.
- La Libertad de distribuir copias y publicar sus cambios.

3.1.4. Redes de computadoras

Se puede definir como una interconexión de computadoras con el fin de intercambiar información de datos, recursos o servicios, por lo general este tipo de conexiones pueden ser hechas mediante un enlace físico o inalámbrico, comúnmente las redes de computadoras están conformadas por 3 computadoras en adelante conectadas entre sí, Para establecer la interconexión entre las

computadoras se requieren de un sistema de red que utilice protocolos de conexón de red, (Valderrama Jhon Edinson, 2017) las redes de computadoras pueden clasificarse de la siguiente manera:

- Área de red local (LAN)
- Área de red metropolitana (MAN)
- Área de red limpia (WAN)
- Área de red personal (PAN)

El uso de redes informáticas permite tipos de conexiones complejas, ya que se pueden enviar videos para que los empleados de empresas ubicadas en sucursales diferentes y distantes puedan ver, escuchar las reuniones a medida que se llevan a cabo lo que reduce el costo y el tiempo dedicado a los viajes de los empleados. También contamos con escritorio compartido, que permite a los empleados remotos acceder a las computadoras de la empresa e interactuar con ellas de manera muy sencilla, así mismo, puede escribir documentos o pizarras remotas entre dos empleados, usar documentos en línea o pizarras virtuales, y hacer lo que hacen los empleados. Las correcciones son inmediatas, visible para otros o aquellos que participan en el documento o reunión en línea (Tanenbaum & Wetherall, 2012).

3.1.5. CIBERSEGURIDAD

El objetivo principal de la seguridad de la red o la seguridad informática es mantener, asegurar o proteger los recursos del sistema de una organización utilizando políticas de seguridad o siguiendo las pautas estándar establecidas por la empresa para garantizar que los usuarios autorizados ingresen información confidencial. Evitar que cualquier intruso o ciberdelincuente ingrese a la organización. La ciberseguridad se encarga de diseñar reglas destinadas a establecer condiciones seguras y manejar datos vitales de los sistemas informáticos de una organización (Valderrama Jhon Edinson, 2017). La ciberseguridad comprende tres aspectos muy importantes los cuales son:

- Confidencialidad
- Integridad

- Disponibilidad

De los cuales, confidencialidad se refiere a la privacidad de la información de la organización, por ende, esta información debe ser resguardada y el sistema informático de ingreso a esta información debe tener protección evitando así el ingreso de intrusos o programas maliciosos. La integridad hace referencia a la cualidad que posee un archivo o documento el cual no ha sufrido ninguna alteración por agentes externos, por lo que con la integridad se permite verificar que no se ha producido ninguna manipulación a los datos de un documento o archivo de la empresa, y por último la disponibilidad viene a ser la capacidad que tiene un sistema informático de reestablecerse luego de algún incidente o también hace referencia a la velocidad de consulta de datos por parte del personal autorizado de la organización cuando lo requieran (Valderrama Jhon Edinson, 2017).

3.1.6. VULNERABILIDAD

Se puede entender como vulnerabilidad a un punto de entrada por el cual un ciberdelincuente o hacker puede obtener acceso al sistema o a los datos de una empresa u organización, una vulnerabilidad se considera un problema el cual va en base a alguna política de seguridad establecida en la organización, de ahí la necesidad de realizar un análisis de vulnerabilidades de un sistema. (Jhordany Serna Valdivia & Mejia Miranda, 2020).

Las vulnerabilidades pueden aparecer en los dispositivos IoT de muy diversas formas, ya que normalmente estas se originan en entornos web sin medidas de seguridad como el bloqueo de cuentas por intentos fallidos de acceso, por lo que los ciberdelincuentes aprovechan aspectos de seguridad informática de estas vulnerabilidades para capturar datos de estas interfaces, como sucede cuando las contraseñas no son muy fuertes o muy simples, también, pueden existir interfaces en la nube inseguras por la falta de encriptación en la conexión, estas mismas vulnerabilidades que surgen en los dispositivos IoT o vulnerabilidades más prevalentes en el entorno, lo que permite a los ciberdelincuentes explotar estas vulnerabilidades e ingresar o manipular información a su gusto (Morales Suárez et al., 2019).

3.1.7. Amenaza

Una amenaza es aquella que aprovecha las vulnerabilidades existentes en un sistema o dispositivo de IoT y son utilizados como medios para realizar cualquier tipo de ataque informático los cuales comprometan el sistema de una organización y con ello a la información, datos dispositivos que dependen del correcto funcionamiento de dicho sistema. Un ejemplo de amenaza a dispositivos IoT es la utilización de los recursos de un hardware de manera inapropiada para ser utilizados como minas de bitcoins y actualmente los ciberdelincuentes han encontrado una forma de ataque a través de estos medios como una manera de conseguir dinero fácil, otro tipo de amenaza muy común son los ataques tipo DDos por tener alta efectividad y también por su simpleza (Morales Suárez et al., 2019).

3.1.8. Riesgo

Se puede definir al riesgo como una probabilidad de que un incidente, ataque o algo negativo suceda dañando los recursos, información o activos de una organización, también se considera como riesgo informático a todas las amenazas existentes que aprovechen una vulnerabilidad de un sistema ya sea físico o digital el cual pueda afectar al rendimiento y disponibilidad del sistema de una organización, la gestión de los riesgos está determinado por el correcto manejo de los mismos, teniendo como objetivo mitigar los riesgos dando más fortaleza a la seguridad de un sistema en caso de algún ataque o intromisión de un agente malicioso, la mitigación de los riesgos no solo está a cargo del área de seguridad sino también de otras áreas que conforman el departamento de ciberseguridad de una empresa (Pinzón Iraldo, 2014). Estas áreas de seguridad informática cumplen un papel muy importante a la hora de resguardar la información o un sistema informático de una organización estas áreas son las siguientes:

- Alta dirección
- Jefe de Informática
- Gerentes
- Directores y oficiales de seguridad
- Profesionales de TI

- Formadores de conciencia de seguridad

Todas estas áreas están encargadas de dar seguridad informática correspondiente y administrar las directrices de seguridad y gestionar los riesgos existentes en la organización, esto se realiza empezando por la gerencia, ya que ellos se encargan de realizar las capacitaciones y concientizar todo el personal de la organización haciendo énfasis en la importancia de llevar buenas prácticas de ciberseguridad teniendo en cuenta los activos a proteger los cuales son: la seguridad física, los controles de acceso, la protección de datos y la seguridad de las redes de comunicación (Pinzón Iraldo, 2014).

3.1.9. Ataques informáticos

Existen varios tipos de ataques informáticos, estos ataques utilizan diferentes estrategias o softwares diferentes, los cuales son usados por los ciberdelincuentes para explotar las vulnerabilidades de un sistema, a continuación, se muestra la definición de algunos de los medios y ataques que son los más comunes (Maggi Murillo Paul & Gomez Omar, 2021):

- **Virus informático:** Es un software malicioso que tiene como objetivo infectar a los archivos de un sistema de uno o varios dispositivos que se encuentren en la misma red de comunicación, esto lo hacen para tener el control de estos dispositivos además de capturar información o modificar archivos de importancia para una organización.
- **SPAM:** Es un método de envío masivo de correos electrónicos comúnmente llamados correo basura desde un equipo desconocido y por lo general utiliza publicidad en el contenido de los mensajes de estos correos.
- **Keylogger:** Es un software o un equipo que puede ser instalado en un sistema y parecer un archivo legítimo del equipo con el objetivo de capturar todo lo que el usuario digite en ese sistema.
- **Ataque de fuerza bruta:** Este es un tipo de ataque el cual trata de obtener el acceso a una cuenta empresarial o de uso personal, estas cuentas pueden ser de algún sitio web o de un correo electrónico, etc. Este ataque consiste en utilizar

diferentes combinaciones de contraseñas utilizando diccionarios que son exclusivos para este tipo de ataques hasta lograr el acceso a la cuenta atacada.

- **Virus Troyano:** Es un tipo de virus informático que tiene la finalidad de engañar a los usuarios haciéndose pasar por un programa de uso habitual o un archivo del sistema del dispositivo, creando así una puerta trasera.
- **Phishing:** Es un tipo de ataque que consiste en obtener información del usuario de manera fraudulenta, utilizando como medio de ataque el envío de correos electrónicos con el objetivo de engañar al usuario haciendo que se ingrese a sitios web infestados de programa maligno.

3.2. Entornos pyme con IoT

La ciberseguridad en entornos de pequeñas y medianas empresas (Pymes) en el contexto de Internet de las Cosas (IoT), la intersección de las Pymes con la tecnología IoT se ven afectadas con ataques informáticos para lo cual es necesario estrategias y software para contrarrestar estos ataques visualizando cual es la importancia de la ciberseguridad en un entorno PYME con IoT.

3.3. Ciberseguridad de entornos pyme

Según el informe anual realizado por la empresa Cisco llamado “Elementos esenciales de seguridad en las Pymes” las Pymes invierten alrededor de 2 235 018 de dólares al año, este valor representa el importe que gastan las Pymes en consecuencia de haber sido víctimas de un ciberataque, debido a los daños o al robo de información valiosa o recursos de IoT y el cese de las actividades y operaciones normales de las mismas, además en ese informe se menciona que el 43% de las Pymes son objetivo de ciberataques, un porcentaje que cada vez va en aumento, esto ha provocado que el 60% de las Pymes cierren sus negocios debido a los ataques informáticos. También menciona que un 53% de las Pymes han participado en un informe llamado “En el 2017 el estado de la ciberseguridad en las pequeñas y medianas empresas” un informe realizado por el instituto Ponemon, dice que las

Pymes han reportado que han sido víctimas de ataques de ransomware en un periodo de un año (Cisco, 2018).

El grupo de investigación contra amenazas de Cisco ha descubierto un nuevo tipo de amenaza llamada VPNFilter, el cual pone en riesgo a más de 500 000 routers y redes de comunicación conectados a dispositivos de almacenamiento de información de oficinas pequeñas alrededor del mundo, este tipo de amenaza permite que los atacantes revisen el tráfico entre los dispositivos para robar información de las copas de seguridad de la red, donde posiblemente obtengan acceso a las redes corporativas de una empresa. En el informe de Cisco se menciona que las organizaciones demoran 191 días en detectar una vulnerabilidad y 66 días en tratar de corregirla, por lo que es necesario detectar las brechas o vulnerabilidades lo más pronto posible para limitar los daños ocasionados por un ataque informático. Todos los ataques informáticos que afectan a las Pymes son debido a que algunas de estas empresas no cuentan con un sistema de seguridad informática o no poseen una estrategia clara de seguridad informática, otra causa es que intentan considerar todas las posibilidades y terminan con un problema de acumulación de soluciones, es decir que la empresa lleva a cabo varias soluciones a la vez provocando que no se solucione correctamente los problemas o se agraven más. Otro caso en particular del informe mencionado anteriormente menciona que el 54% de las Pymes tienen empleados negligentes y ese era el origen de los problemas de seguridad informática, además se menciona que el 59% de las Pymes encuestadas afirman que no poseen buenas prácticas en la creación de contraseñas siendo estas contraseñas muy débiles o fáciles de descifrar y mencionan que el 68% de las Pymes no aplican estrictamente políticas de seguridad para contraseñas y cifrados o no están seguros del nivel en el que se administra la seguridad de las mismas (Cisco, 2018).

3.3.1. Ciberseguridad de entornos Pyme en Ecuador

En el Ecuador en los últimos años las Pymes han aumentado de manera significativa en cuanto a su cartera de inversión y de su producción brindado más opciones de

empleo, sin embargo en cuanto a ciberseguridad se encuentran un poco desvinculadas respecto al tema ya que no cuentan con u modelo de seguridad informática establecido o en todo caso no manejan políticas de seguridad de la información acorde a las necesidades de la organización, ya que no implementan métodos de detección de accesos no autorizados, además no le dan tanta importancia al ciberseguridad debido a que no disponen del dinero para invertir en esta área o simplemente lo ven como un gasto innecesario, además el personal de estas Pymes no cuentan con una capacitación adecuada respecto a estos temas de seguridad informática (Zuña Edgar et al., 2019). La ciberseguridad en Ecuador es parte de las responsabilidades constitucionales del país, Especialmente en lo que se refiere al desarrollo y establecimiento de una cultura de paz. La política nacional de ciberseguridad incluye aspectos que caen dentro de las capacidades de ciberdefensa, ciberinteligencia y ciberdiplomacia. La ciberseguridad paulatinamente se convertirá en un tema relevante en la agenda de seguridad, desarrollo y derechos humanos del Ecuador, por lo que es necesario desarrollar y fortalecer capacidades nacionales, políticas, estrategias, planes, programas y proyectos intersectoriales en materia de ciberseguridad (Ministerio de Telecomunicaciones, 2021). En cuanto a la política digital de Ecuador, se dice que su principal objetivo es transformar al país en una economía basada en tecnologías digitales mediante la reducción de la brecha digital y la adopción digital en los sectores sociales y económicos, asumiendo que las políticas de tres ejes que componen esta política son: un Ecuador interconectado, un Ecuador eficiente y ciberseguro, y un Ecuador innovador y competitivo garantizando la participación ciudadana, la Gestión de la Seguridad de la Información y la protección de datos personales (Ministerio de Telecomunicaciones, 2021).

3.4. Pymes con arquitecturas de ciberseguridad

La ciberseguridad es un tema crucial en la era digital en la que vivimos. Las empresas, especialmente las pymes, son vulnerables a los ataques cibernéticos que pueden comprometer sus datos y sistemas críticos. Por lo tanto, la implementación

de arquitecturas de ciberseguridad efectivas es fundamental para proteger los recursos y la información de la empresa.

Una de las arquitecturas de ciberseguridad más importantes para las pymes es el firewall. El firewall es una barrera de seguridad que se coloca entre la red interna de la empresa y la red externa (Internet). El firewall puede bloquear el tráfico no deseado y proteger contra los ataques de programa maligno, virus y otros tipos de amenazas.

Otra arquitectura de ciberseguridad importante es la red privada virtual (VPN). La VPN permite a los empleados acceder de forma segura a los recursos de la empresa a través de Internet, ya sea desde la oficina o desde una ubicación remota. La VPN es una herramienta útil para garantizar que la información confidencial esté protegida y que solo los empleados autorizados tengan acceso.

Además, las pymes deben tener un plan de copia de seguridad y recuperación de desastres para garantizar que los datos críticos estén protegidos en caso de un fallo del sistema o de un desastre. También es importante que las pymes se mantengan actualizadas con las últimas actualizaciones de seguridad y parches de software para corregir vulnerabilidades conocidas. Las políticas de seguridad claras y comunicadas a todos los empleados también son fundamentales para garantizar que estén alineados con las mejores prácticas de ciberseguridad.

Sin embargo, la implementación de arquitecturas de ciberseguridad efectivas no es suficiente. Las pymes deben trabajar en colaboración con proveedores de seguridad de confianza para seleccionar las arquitecturas de ciberseguridad adecuadas y garantizar que se implementen de manera efectiva y adecuada. Además, la capacitación de los empleados en buenas prácticas de ciberseguridad y la conciencia de los riesgos son esenciales para garantizar que la empresa esté protegida contra los ataques cibernéticos.

3.5. Mecanismos y herramientas de seguridad IoT para organizaciones Pyme

A lo largo de los años se han realizado numerosos estudios sobre cómo afrontar los riesgos y problemas que plantean los ataques informáticos, y las Pymes no se quedan atrás. Un mecanismo de seguridad que se podría implementar es un filtro Kalman en el SCADA del sistema, el objetivo de predecir ciberataques y alertar a los ingenieros de sistemas de la empresa de posibles acciones ante un posible evento, y existen otros estudios basados en cómo mitigar los efectos de estos ataques. Otro mecanismo de seguridad es comparar dos métodos cuantitativos destinados a reducir el costo de su implementación: la Programación por Conjuntos de Respuesta o ASP y el método de Programación Lineal o PL. Existe también un mecanismo de seguridad que consiste en un modelo de auditoría de seguridad de la información llamado CSAM, el cual se utiliza para evaluar la seguridad informática en cuanto a su estado actual y su mecanismo de respuesta frente a ataques cibernéticos, además este mecanismo tiene como objetivo detectar las brechas existentes en el sistema de seguridad informática y detectar las necesidades de la organización para fomentar una conciencia cibernética en el personal de la organización, este modelo se puede implementar para realizar auditorías internas o externas de la seguridad de la información de la empresa. Por último, existe un mecanismo de seguridad el cual se basa en el uso de un sistema de seguridad perimetral como un firewall el cual permita reducir el riesgo de ser afectado por un ataque cibernético, ya que con este sistema se incrementará la detección de intrusos o agentes externos a la organización mitigando el riesgo de sufrir daños o robos de la información de la empresa garantizando así la seguridad de la información y la integridad, confidencialidad y disponibilidad del sistema de la organización (Peralta Marco & Aguilar Daniela,2021).

Para el caso práctico que se llevará a cabo en esta investigación, se utilizará herramientas de código abierto como Open SSL y los dispositivos raspberry pi y los módulos esp32, cabe destacar que como mecanismo de seguridad se utilizará el protocolo MQTL/TLS..

4. Materiales y metodología

4.1. Materiales y herramientas

Para el desarrollo de la arquitectura de ciberseguridad para la organización tipo Pyme, se utilizará diferentes aplicativos tecnológicos, estas herramientas permiten obtener mejores resultados y realizar un análisis más detallado acorde al tipo de organización que se ha elegido y acorde a los lineamientos establecidos en la arquitectura y necesidades de la organización tipo Pyme, las herramientas a usar son las siguientes:

- Raspberry PI
- Módulos ESP32
- Computador, Laptop
- Cables de conexión
- Internet

4.2. Selección de Metodologías

En el diseño de la arquitectura de ciberseguridad se necesita llevar a cabo ciertos procesos en base a metodologías que permitan alcanzar los diferentes objetivos planteados, todo esto utilizando diferentes protocolos y dependiendo del tipo de metodología como se detalla a continuación:

4.2.1 Metodología por Beneficio

La metodología para aplicar en base al criterio de beneficio y enfoque para organizaciones tipo Pyme sería la metodología de la normativa ITIL, la misma que en base a investigación se tiene lo siguiente:

- **Normativa ITIL:** En la investigación de (Ramírez Bravo Pía, 2006) se menciona que esta metodología ITIL desde el punto de vista de los negocios su propósito es gestionar de manera eficiente el diseño y administración de las infraestructuras y

bases de datos de una organización dentro de un marco de trabajo enfocado a la administración de los procesos de IoT tomando en cuenta procesos de ciberseguridad y buscando reducir los costos de provisión y soporte de los servicios de IT, garantizando los requerimientos de seguridad de la información, siendo esta metodología la más adecuada para organizaciones tipo Pyme.

4.2.2 Metodología por alcance

La metodología ITIL se encuentra conformada por dos áreas las cuales abarcan todos los posibles inconvenientes en la gestión de la seguridad de la información de una organización con sistemas IoT estas áreas se muestran a continuación con cada uno de los procesos de gestión que llevan a cabo, según lo indica (Ramírez Bravo Pía, 2006) en su detalle del enfoque de esta metodología:

Área de Entrega de Servicios

- Gestión de Cuentas
- Gestión de Nivel de Servicio
- Gestión de Continuidad de Servicio
- Gestión de Disponibilidad Usuario
- Gestión Financiera
- Gestión de Capacidad

4.2.3 Metodología por objetivos definidos

Según lo indica (Ramírez Bravo Pía, 2006) la metodología ITIL tiene como objetivo principal diseminar las mejores prácticas en la gestión de servicios y seguridad de las tecnologías de la información de manera sistemática y coherente, basándose en la calidad de servicio y desarrollo eficaz de todos los procesos de una organización.

Los estándares de ITIL exigen un replanteamiento del área tecnológica de la organización y también la definición de los elementos y procesos que son cruciales dentro de cualquier empresa. En comparación con las normas ISO que son bastante rígidas con los negocios, la normativa ITITL en cambio trata de facilitar el mejoramiento y la estandarización de calidad en todos sus procesos relacionados

con tecnología y su seguridad, manteniendo sus niveles de fiabilidad consistencia y calidad de cada organización (Ramírez Bravo Pía, 2006).

La filosofía que maneja la normativa ITIL trata de adoptar la gestión de procesos y tiene como base principal que para cumplir con los objetivos de administración, los procesos de gestión de tecnología deben ser usados por el personal y herramientas tecnológicas de manera efectiva, ya que una de las áreas que gestiona esta normativa ITIL es la de ciberseguridad ya que cubre todos los aspectos relacionados con la administración de bases de datos e información de la empresa, además de que esta normativa se encarga del control de las aplicaciones operativas o en fase de desarrollo que pueda tener la organización por lo que se alinea con el manejo de gestión de ciberseguridad de una organización tipo Pyme.

4.3 Metodología para el desarrollo de la arquitectura

4.3.1 Definición del alcance

Es importante que la empresa identifique la misión, visión, objetivos y prioridades dentro de la organización, de esta manera se determinan los posibles riesgos cibernéticos que pueden afectar el funcionamiento de los sistemas y activos de la institución (Lombardi & Arevalo, 2020).

La empresa necesita conocer la situación actual de la seguridad de la institución, a continuación, se contextualizará las actividades que definen el alcance de este estudio.

Tabla 1

Actividades iniciales para definir el alcance de la metodología aplicada

Actividad	Descripción	Tareas
Identificar la situación actual del área de TI	En esta actividad se identifica el área de TI para realizar el diseño	➢ Políticas de TI ➢ Principios de TI

	de la arquitectura de ciberseguridad.	
Analizar la ciberseguridad de las plataformas IoT en la organización Pyme	Análisis de la ciberseguridad relacionada con la ejecución de las plataformas IoT en la organización Pyme.	➢ Estado actual de las plataformas IoT en la organización Pyme.

4.3.2 Diagnóstico inicial del estado actual de la organización tipo Pyme

Para obtener un perfil actual del estado de la organización Pyme es importante gestionar los riesgos cibernéticos visualizando si se ha cumplido las políticas de seguridad, así se podrá crear un perfil objetivo al cual se desea llegar, teniendo un progreso positivo en la implementación del diseño de la arquitectura. Además de estos parámetros iniciales, se debe tener en cuenta el estado de la seguridad informática de las plataformas IoT que maneje la organización Pyme, realizan una tabla en la cual se mencione todos los equipos, infraestructura de red, software y demás hardware que maneje la organización. Por lo general, las organizaciones tipo Pyme actualmente ya manejan este tipo de dispositivos, con la finalidad de realizar un análisis de todos los sistemas activos y con ello llevar a cabo la evaluación pertinente y eventualmente priorizar los criterios para el desarrollo de la arquitectura de ciberseguridad, en este caso para una organización tipo Pyme (Lombardi & Arevalo, 2020).

4.3.3 Determinación y análisis de vulnerabilidades

Para la determinación y análisis de vulnerabilidades es importante conocer el nivel de ciberseguridad en las plataformas IoT, a continuación, se da a conocer las actividades para determinar y analizar las vulnerabilidades.

Tabla 2

Actividades para identificar el estado actual de la organización tipo Pyme

ACTIVIDAD	DESCRIPCIÓN	TAREAS
Identificar el estado actual del nivel de ciberseguridad en el área TI.	Se conocerá las políticas de seguridad implementadas y si se están cumpliendo dentro de las directrices.	➢ Evaluar el estado actual de la seguridad de las plataformas IoT, políticas y directrices.
Identificar el estado actual de sistemas y activos usados en las plataformas IoT.	Se realizará una bitácora de los equipos y programas de software.	➢ Activos y sistemas o programas de software.

4.3.4 Análisis de riesgos y amenazas

La empresa necesita saber el estado actual de la seguridad para lo cual es necesario ejecutar un análisis de riesgos y amenazas. El análisis consiste en identificar las distintas vulnerabilidades en los sistemas y activos lo cual se revisó en el anterior ítem. Para el desarrollo de este análisis se usará herramientas que permitan visualizar el riesgo y las amenazas existentes dentro de la infraestructura de la institución.

Tabla 3

Actividades relacionadas con la identificación de riesgos y amenazas

ACTIVIDAD	DESCRIPCIÓN	TAREAS
Identificar el riesgo en la ciberseguridad	Se analiza el entorno operativo para identificar los riesgos existentes esto quiere decir los distintos eventos o incidentes de ciberseguridad	➢ Riesgos de ciberseguridad en la infraestructura del área TI.

	para conocer el impacto que se ha producido en la infraestructura de la institución.	
Reconocer las amenazas de ciberseguridad	En base a las vulnerabilidades existentes se identificará las amenazas que afectan al área TI.	➢ Amenazas de ciberseguridad.

4.3.5 Implementación de acciones frente a riesgos cibernéticos

La finalidad de este paso es poder realización un plan de acción después de gestionar un análisis de los riesgos de ciberseguridad. a continuación, se presentan actividades referentes al plan de acción de riesgos.

Tabla 4

Actividades para la implementación del plan de acción frente a riesgos y amenazas

ACTIVIDAD	DESCRIPCIÓN	TAREAS
Evaluación y monitoreo continuo	Es necesario evaluar y monitorear el sistema, así se identificará cualquier anomalía que pueda existir y respaldar la información de forma rápida.	➢ Monitoreo continuo

4.3.6 Protocolo MQTT (TLS/SSL)

El protocolo MQTT es un protocolo muy utilizado dentro de las Pymes ya que es de fácil uso, requiere de un mínimo ancho de banda y su código es liviano lo cual lo hace perfecto para conectar muchos dispositivos IoT en una red. El protocolo funciona mediante la publicación y suscripción de mensajes entre clientes y servidor (Broker) como se muestra en la Figura 1.

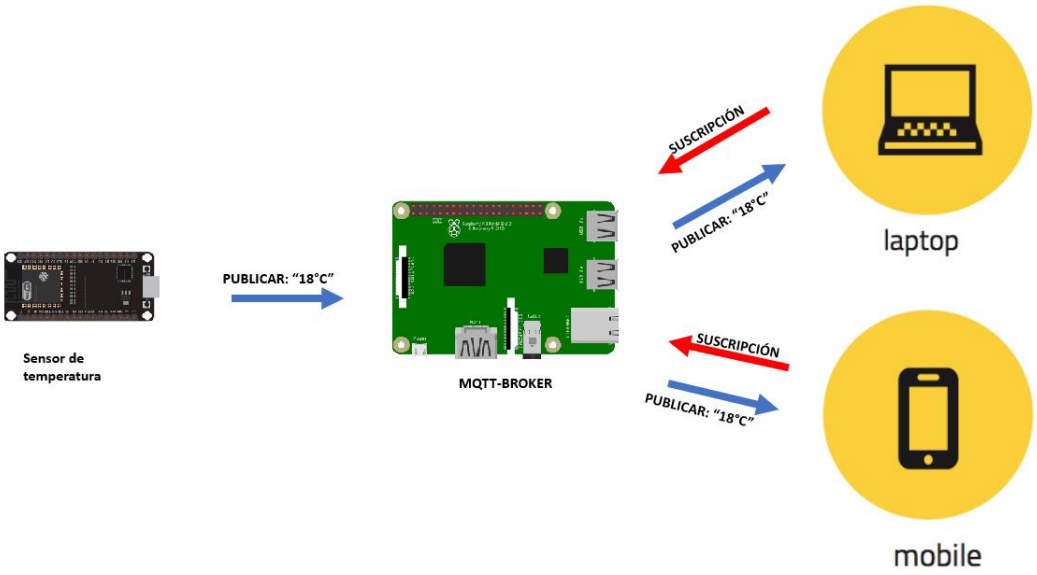

Figura 1. Manejo de mensajes en el protocolo MQTT.

A pesar de que este protocolo ofrece la posibilidad de configurar parámetros de autenticación y autorización entre clientes y bróker es muy inseguro y es propenso a un ataque, el puerto por defecto que utiliza este protocolo es el 1883 y si bien es cierto es posible establecer una contraseña y usuario para cada dispositivo, estas credenciales no son cifradas.

La seguridad de la capa de transporte (TLS) y la capa de conectores seguros (SSL) son dos opciones que se puede implementar en el protocolo para una comunicación segura encriptada entre clientes y bróker, para hacer uso de este protocolo los clientes deben tener certificados de tipo digital para poderse autenticar al bróker, con estos certificados es posible garantizar la identidad de cada uno de los clientes

evitando de esta manera ataques que pueden interceptar los mensajes o manipularlos, el puerto utilizado para este protocolo es el 8883.

4.3.7 Creación de firmas electrónicas y llaves para el uso del protocolo MQTT(TLS/SSL)

El propósito de utilizar certificados electrónicos y llaves es para poder establecer una conexión cifrada que garantice los tres pilares fundamentales que se muestran en la Tabla 5.

Tabla 5

Pilares principales del protocolo MQTT (TLS/SSL)

Autenticación	El dispositivo que envía el mensaje es el que realmente dice ser.
Encriptación	Impide la lectura del mensaje de cualquier atacante que lo intercepte en el camino.
Integridad	Impide la modificación del mensaje.

OpenSSL es un programa gratuito que puede ser usado por cualquier persona y permite realizar certificados y firmas electrónicas, integra todos los requisitos necesarios para la implementación de la capa de seguridad de transporte (TLS), está incluido en los sistemas operativos LINUX.

Con el comando que se muestra en la Figura 2 se procede a generar una contraseña para el certificado.

```
root@raspberrypi:/home/carlos# openssl genrsa -des3 -out ca.key 2048
```

Figura 2. Comando para generar contraseña para el certificado.

Se pedirá primero el ingreso de la contraseña y después es necesario confirmarla como se muestra en la Figura 3.

```
carlos@raspberrypi:~ $ sudo su
root@raspberrypi:/home/carlos# openssl genrsa -des3 -out ca.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.................................+++++
.................+++++
e is 65537 (0x010001)
Enter pass phrase for ca.key:
Verifying - Enter pass phrase for ca.key:
```

Figura 3. Ingreso de clave para el certificado.

Con el siguiente comando se crea el certificado utilizando la contraseña que se puso en el paso anterior como se muestra en la Figura 4.

```
root@raspberrypi:/home/carlos# openssl req -new -x509 -days 1826 -key ca.key -out ca.crt
```

Figura 4. Comando para la creación del certificado CA.

El programa nos pedirá una serie de parámetros como la provincia, ciudad, nombre de país, email, nombre común del servidor, nombre de la compañía y nombre de la sección. Todos esos parámetros se pueden colocar y en el caso de querer dejar en blanco alguno de ellos se debe colocar un punto como se muestra en la Figura 5.

```
-----
Country Name (2 letter code) [AU]:EC
State or Province Name (full name) [Some-State]:Pichincha
Locality Name (eg, city) []:Quito
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IOT
Organizational Unit Name (eg, section) []:client
Common Name (e.g. server FQDN or YOUR name) []:test
Email Address []:.
```

Figura 5. Parámetros generales para colocar en el certificado.

Lo siguiente es generar una contraseña para el servidor con el comando que se utiliza en la Figura 6.

```
root@raspberrypi:/home/carlos# openssl genrsa -out server.key 2048
```

Figura 6. Comando para generar contraseña del servidor.

Con el siguiente comando se genera una petición de certificado CSR, se puede observar en la Figura 7.

```
root@raspberrypi:/home/carlos# openssl req -new -out server.csr -key server.key
```

Figura 7. Comando para generar la petición de firma de certificado.

Dentro de los parámetros que se pide colocar está el nombre común que en este caso será la IP de la Raspberry Pi que será el servidor bróker, se observa en la Figura 8.

```
Country Name (2 letter code) [AU]:EC
State or Province Name (full name) [Some-State]:Pichincha
Locality Name (eg, city) []:Quito
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IOT
Organizational Unit Name (eg, section) []:server
Common Name (e.g. server FQDN or YOUR name) []:192.168.1.57
Email Address []:.

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.
An optional company name []:.
```

Figura 8. Colocación de la IP del servidor para la petición de firma del certificado.

En la Figura 9 se visualiza como se ocupa la contraseña que se realizó en el certificado CA para validar y firmar el certificado del servidor.

```
root@raspberrypi:/home/carlos# openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days
360
```

Figura 9. Comando para firmar el certificado del bróker.

Los archivos que se han generado con los comandos ingresados se pueden visualizar dentro de la ruta /home/Carlos, como se observa en la Figura 10.

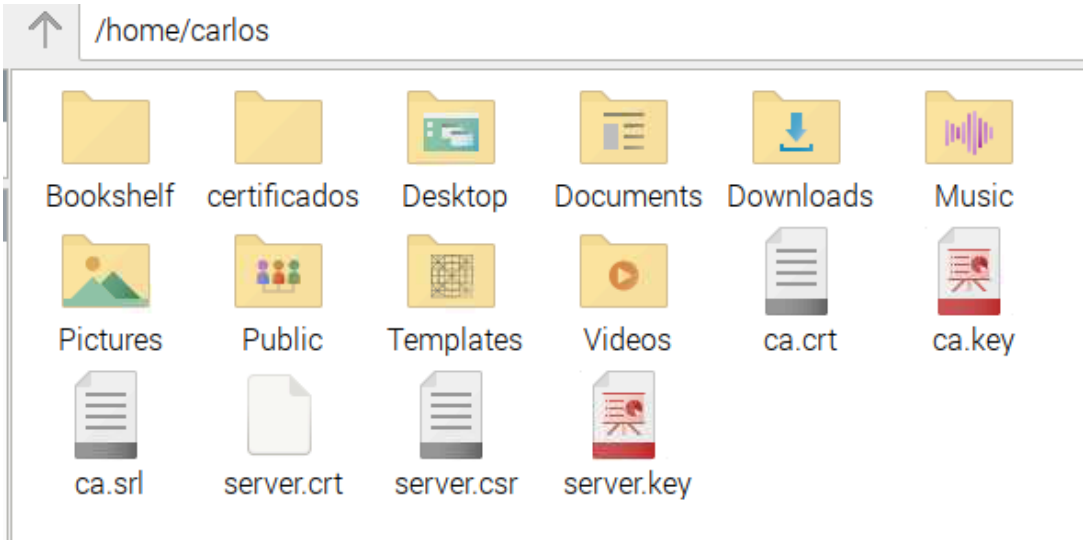

Figura 10. Certificados generados.

4.3.8 Instalación y configuración de Mosquitto

Para la instalación de Mosquitto se ejecutan los siguientes comandos en una terminal de la Raspberry pi como se muestra en la Tabla 6.

Tabla 6

Comandos para instalación de Mosquitto bróker

sudo apt update && sudo apt upgrade	Comando para actualizar el sistema.
sudo apt install -y mosquitto mosquitto-clients	Comando para instalar Mosquitto bróker.
sudo systemctl enable mosquitto.service	Comando para que Mosquitto se ejecute automáticamente cada que se reinicie el bróker.

Se crea un nuevo archivo de configuración para Mosquito en la ruta que se muestra en la Figura 11, en donde se creó un archivo test.conf.

```
root@raspberrypi:/home/carlos# nano /etc/mosquitto/test.conf
```

Figura 11. Creación de archivo de configuración.

Los 6 certificados que se muestran en la Figura 10 deben ser copiados en la ruta que se muestra en la Figura 12.

```
root@raspberrypi:/etc/mosquitto/certs# ls
ca.crt  ca.key  ca.srl  README  server.crt  server.csr  server.key
```

Figura 12. Copia de certificados en nueva ruta.

Es necesario cambiar el permiso de todos los archivos de las carpetas donde se guardan los certificados con el comando que se muestra en la Figura 13 y también cambiar los permisos de las carpetas con el comando de la Figura 14.

```
carlos@raspberrypi:~ $ sudo su
root@raspberrypi:/home/carlos# chmod 0644 ./ca_certificates/* ./certs/*
```

Figura 13. Comando para cambiar los permisos de los archivos.

```
carlos@raspberrypi:~ $ sudo su
root@raspberrypi:/home/carlos# chmod 0755 ./ca_certificates/ ./certs
```

Figura 14. Comando para cambiar los permisos de las carpetas.

Dentro del archivo test.conf se especifica el nuevo puerto que se va a utilizar que es el 8883 el cual garantiza una comunicación TCP y está destinado para el uso del protocolo MQTT seguro también se establece la ruta donde están guardados los certificados y llaves y se establece la versión TLS que se utilizará como se muestra en la Figura 15.

```
  GNU nano 5.4                    /etc/mosquitto/test.conf
#listener 1883
listener 8883

allow_anonymous true

cafile /etc/mosquitto/certs/ca.crt
keyfile /etc/mosquitto/certs/server.key
certfile /etc/mosquitto/certs/server.crt
tls_version tlsv1.2
```

Figura 15. Configuración de archivo test.conf

Se guarda todos los cambios realizados y se reinicia el servicio de Mosquitto con el comando que se observa en la Figura 16.

```
carlos@raspberrypi:~ $ sudo service mosquitto restart
```

Figura 16. Comando para reiniciar Mosquitto.

Se ejecuta Mosquitto con el nuevo archivo de configuración con el comando que se muestra en la Figura 17 y enseguida se puede observar la versión de Mosquitto y el puerto con el que está funcionando tal y como se configuró en el archivo test.conf.

```
carlos@raspberrypi:~ $ mosquitto -c /etc/mosquitto/test.conf -v
1680138305: mosquitto version 2.0.11 starting
1680138305: Config loaded from /etc/mosquitto/test.conf.
1680138305: Opening ipv4 listen socket on port 8883.
1680138305: Opening ipv6 listen socket on port 8883.
1680138305: mosquitto version 2.0.11 running
```

Figura 17. Comando para ejecutar Mosquitto con el nuevo archivo de configuración.

4.3.9 Propuesta de una arquitectura IOT segura orientada a Pymes

En el protocolo MQTT/TLS la capa de transporte es la encargada de enviar los datos encriptados que fueron recolectados por la capa de sensores. La encriptación y desencriptación se realiza con ayuda de los certificados y llaves de autoridad de certificación. Una vez que el bróker desencripta los mensajes y los analiza para tomar decisiones con el objetivo de automatizar cierto sistema publica los resultados a través de la capa de red. Los resultados pueden ser observados por medio de la capa de nube que contiene una interfaz gráfica comprensible para el usuario como se muestra en la Figura 18.

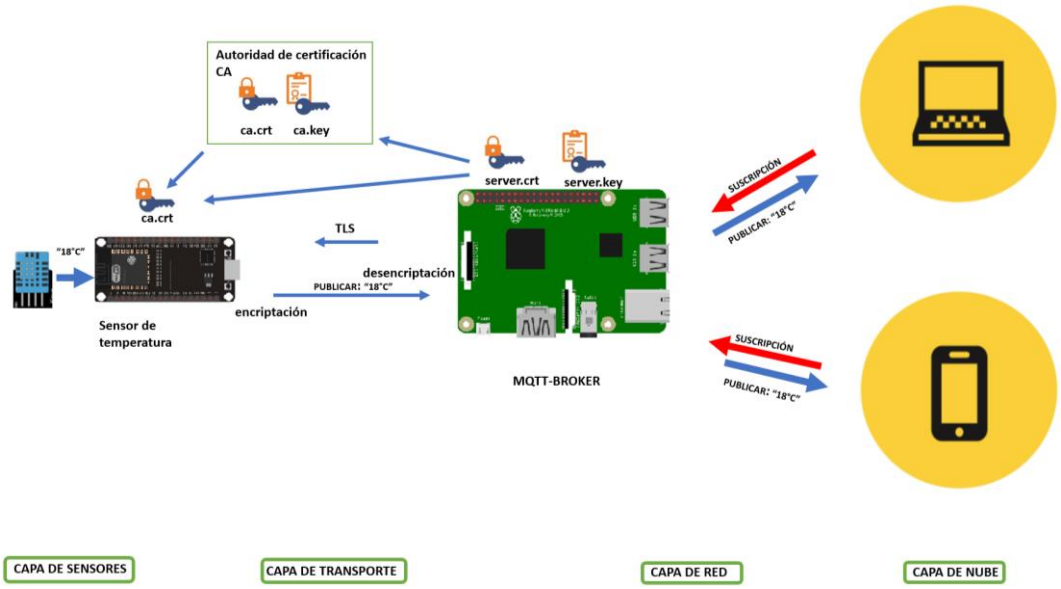

Figura 18. Propuesta de una arquitectura IoT segura orientada a Pymes.

4.3.10 Simulación de un prototipo con una arquitectura de ciberseguridad en una infraestructura de IoT orientado a las Pymes.

En este documento se implementó un prototipo de infraestructura IoT haciendo uso de una Raspberry Pi como bróker y dos dispositivos ESP32 como clientes.

4.3.11 Configuración de Raspberry Pi como bróker MQTT/TSL

- En la página web oficial de Raspberry pi es necesario descargar e instalar una imagen estable en una SD de décima generación que sea mayor a 8GB.
- Se conecta un monitor, un teclado, ratón y la tarjeta SD con la imagen estable de Rasbian instalada.
- El sistema de configuración avanzado de Raspberry Pi le guiarán en los primeros pasos como el establecimiento del nombre del usuario, contraseñas, país, entre otros.
- Con los comandos mostrados en la Tabla 6 se procede a instalar y configurar Mosquitto.

- Se genera los certificados y llaves electrónicas como se mostró anteriormente y se configura el archivo test.conf.

4.3.12 Instalación de Node red

- Con la línea de comando que se muestra en la Figura 19 es posible instalar o actualizar una nueva versión de Node red en raspberry pi.

```
bash <(curl -sL https://raw.githubusercontent.com/node-red/linux-installers/master/deb/update-nodejs-and-nodered)
```

Figura 19. Comando de instalación de Node red.

- Se ejecuta el comando de la Figura 20 para ejecutar Node red automáticamente en el arranque del bróker.

```
sudo systemctl enable nodered.service
```

Figura 20. Comando para establecer Node red como servicio.

- En un buscador de internet se ingresa la IP del bróker seguido de ":8080" y se obtiene acceso al programa de Node red para su programación como se muestra en la Figura 21.

Figura 21. Acceso a la interfaz de programación de Node red.

4.3.13 Programación de módulos ESP32 con el protocolo MQTT/TLS

- En el certificado ca.crt generado dar doble clic y dirigirse a la pestaña detalles como se observa en la Figura 22.

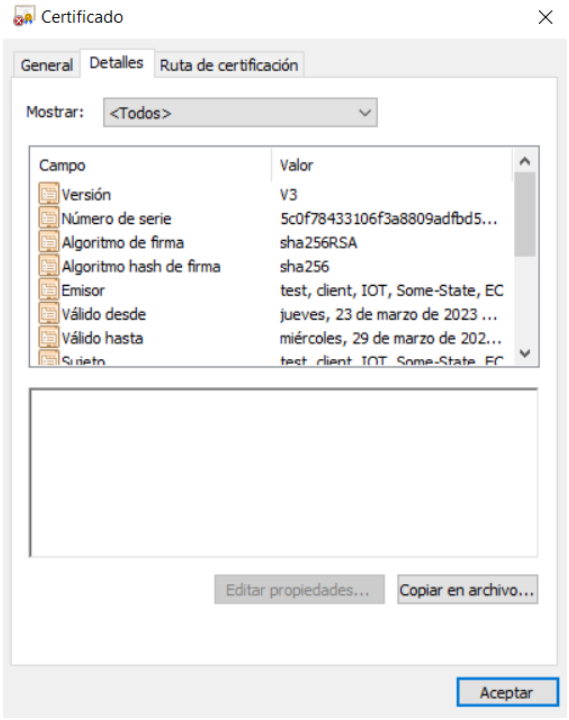

Figura 22. Detalles del certificado ca.

- Seleccionar algoritmo hash de firma y dar clic en copiar archivo, se desplegará una ventana en donde se debe escoger la opción que se visualiza en la Figura 23, escoger una ruta y un nombre donde se desea guardar los cambios.

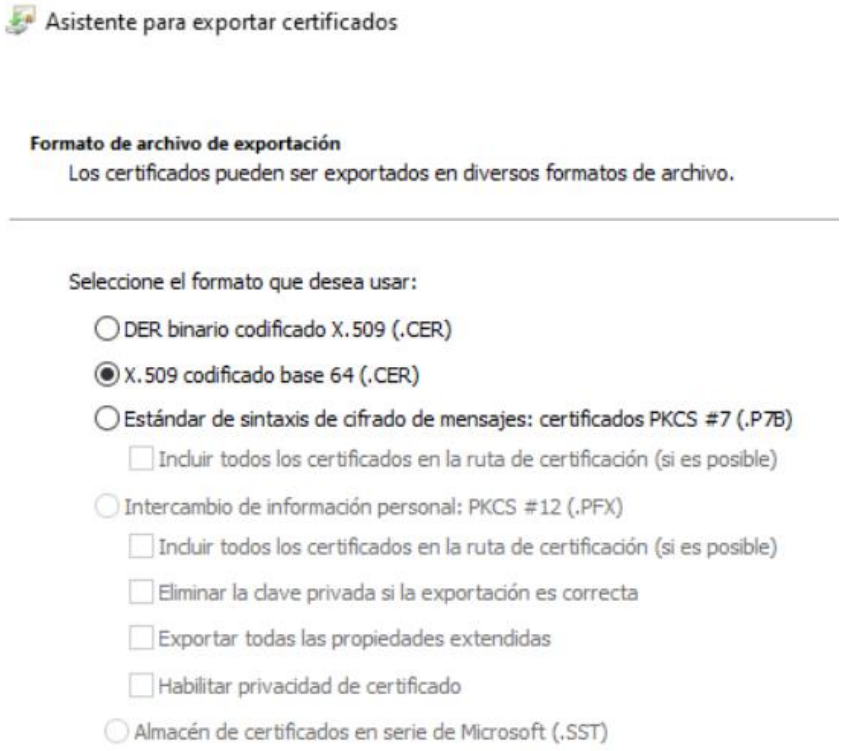

Figura 23. Ventana de diálogo de exportación de certificado.

- Se abre el archivo generado con un editor de texto como se muestra en la Figura 24 y se copia todo el texto para utilizar en la programación de los módulos ESP32.

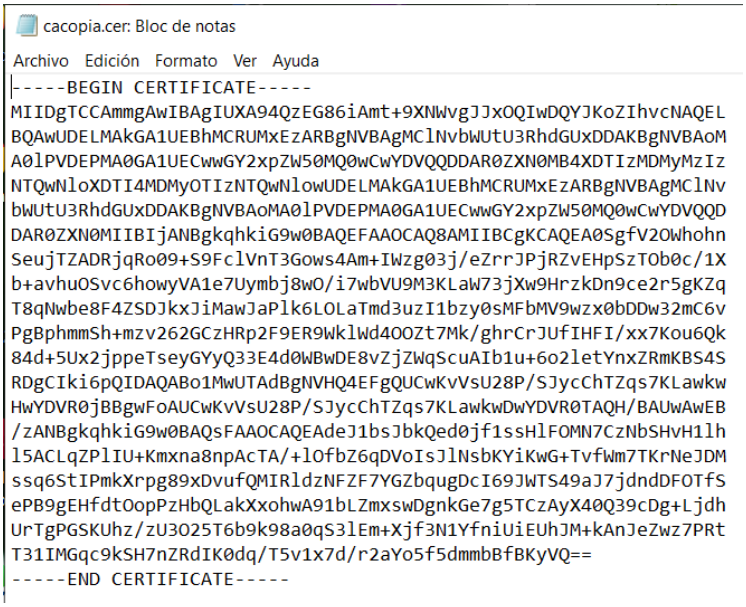

Figura 24. Certificado ca que será implementado en la programación de los módulos ESP32.

- Se carga la programación que se muestra en el anexo 1 en donde se incluye el certificado ca de la Figura 24, como se observa en la Figura 25.

```
#include "Arduino.h"
#include <WiFi.h>
#include "esp_log.h"
#include "esp_system.h"
#include "esp_event.h"
#include "mqtt_client.h"

//#define SECURE_MQTT //

#ifdef SECURE_MQTT
#include "esp_tls.h"

// certificado CA
static const unsigned char DSTroot_CA[] PROGMEM = R"EOF(
-----BEGIN CERTIFICATE-----
MIIDSjCCAjKgAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/
MSQwIgYDVQQKExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMT
DkRTVCBSb290IENBIFgzMB4XDTAwMDkzMDIxMTIxOVoXDTIxMDkzMDE0MDExNVow
PzEkMCIGA1UEChMbRGlnaXRhbCBTaWduYXR1cmUgVHJ1c3QgQ28uMRcwFQYDVQQD
Ew5EU1QgUm9vdCBDQSBYMzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AN+v6ZdQCINXtMxiZfaQguzH0yxrMMpb7NnDfcdAwRgUi+DoM3ZJKuM/IUmTrE4O
rz5Iy2Xu/NMhD2XSKtkyj4zl93ewEnu1lcCJo6m67XMuegwGMoOifooUMM0RoOEq
OLl5CjH9UL2AZd+3UWODyOKIYepLYYHsUmu5ouJLGiifSKOeDNoJjj4XLh7dIN9b
xiqKqy69cK3FCxolkHRyxXtqqzTWMIn/5WgTe1QLyNau7Fqckh49ZLOMxt+/yUFw
7BZylSbsOFU5Q9D8/RhcQPGX69Wam40dutolucbY38EVAjqr2m7xPi71XAicPNaD
aeQQmxkqtilX4+U9m5/wAl0CAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMSnsaR7LHH62+FLkHX/xBVghYkQMA0GCSqG
SIb3DQEBBQUAA4IBAQCjGiybFwBcqR7uKGY3Or+Dxz9LwwmglSBd49lZRNI+DT69
ikugdB/OEIKcdBodfpga3csTS7MgROSR6cz8faXbauX+5v3gTt23ADqlcEmv8uXr
AvHRAosZy5Q6XkjEGB5YGV8eAlrwDPGxrancWYaLbumR9YbK+rlmM6pZW87ipxZz
R8srzJmwN0jP41ZL9c8PDHIyh8bwRLtTcmlD9SZImlJntlir/md2cXjbDaJWFBM5
JDGFoqgCWjBH4d1QB7wCCZAA62RjYJsWvIjJEubSfZGL+T0yjWW06XyxV3bqxbYo
Ob8VZRzI9neWagqNdwvYkQsEjgfbKbYK7p2CNTUQ
-----END CERTIFICATE-----
)EOF";
#endif // SECURE_MQTT

esp_mqtt_client_config_t mqtt_cfg;
esp_mqtt_client_handle_t client;

const char* WIFI_SSID = "CELERITY_SOFY";
const char* WIFI_PASSWD = "$%Thepolice";

const char* MQTT_HOST = "192.168.1.57";
#ifdef SECURE_MQTT
```

Figura 25. Implementación del certificado ca en el módulo ESP32.

- Se carga la programación que está en el anexo 2 en el segundo dispositivo ESP32, y se incluye en la programación el mismo certificado ca que se utilizó en la Figura 25.

4.3.14 Adquisición de mensajes en Node red

Para poder probar que se está recibiendo los mensajes de los dispositivos ESP32 se hará uso de Node red.

- Se coloca en el área de trabajo un nodo MQTT in para la suscripción de mensajes y un nodo MQTT out para la publicación de mensajes, se los coloca un nodo debug para poder observar los mensajes, como se muestra en la Figura 26.

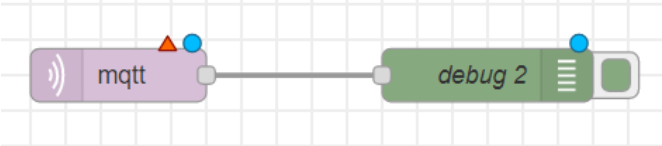

Figura 26. Implementación de nodo MQTT in para suscripción de mensajes.

- Se da doble clic en el nodo para proceder a la configuración del protocolo, se da clic en el lápiz y se configura la IP del bróker, el puerto seguro 8883 y el uso de TLS como se muestra en la Figura 27.

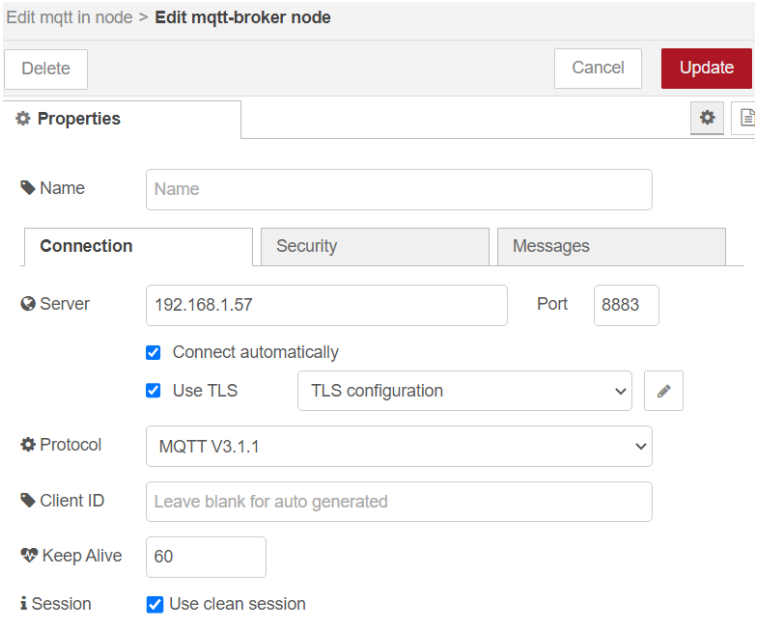

Figura 27. Configuración del protocolo MQTT in.

- Se da clic en el lápiz y se coloca la ruta en donde están guardados los certificados y llaves como se observa en la Figura 28.

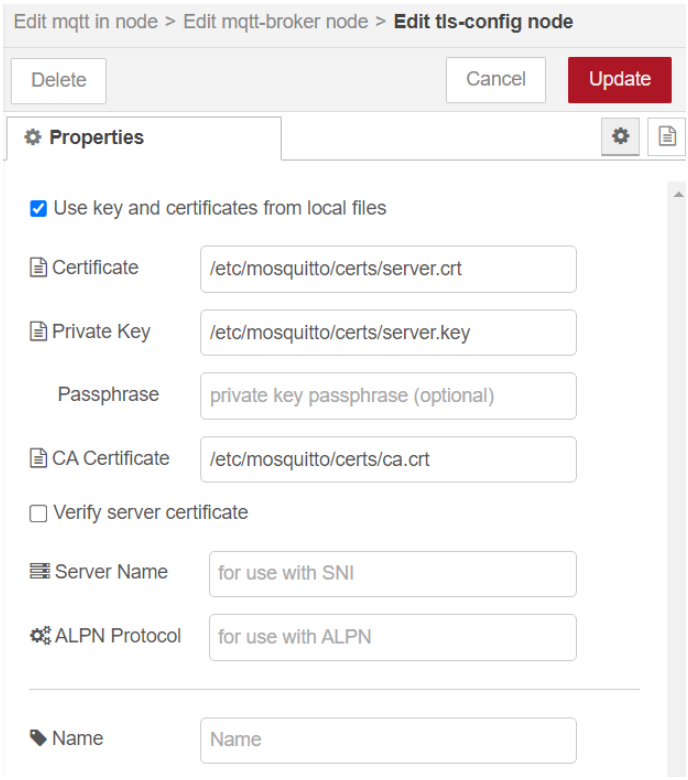

Figura 28. Configuración TLS en el modo MQTT in.

- Se da clic en update y se escribe el tema al cual se desea suscribir, en este caso se ha colocado el símbolo de numeral con el cual se indica que se desea observar todos los mensajes que llegan al bróker como se observa en la Figura 29.

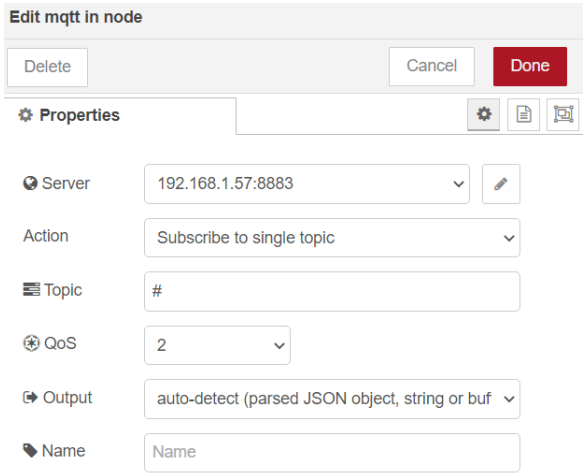

Figura 29. Suscripción para poder observar todos los mensajes que llegan al bróker.

- A continuación, se da clic en Done y en Deploy para poder ver todos los mensajes como se muestra en la Figura 30, donde se puede observar que se obtiene los mensajes de los dos ESP32 dispositivos programados.

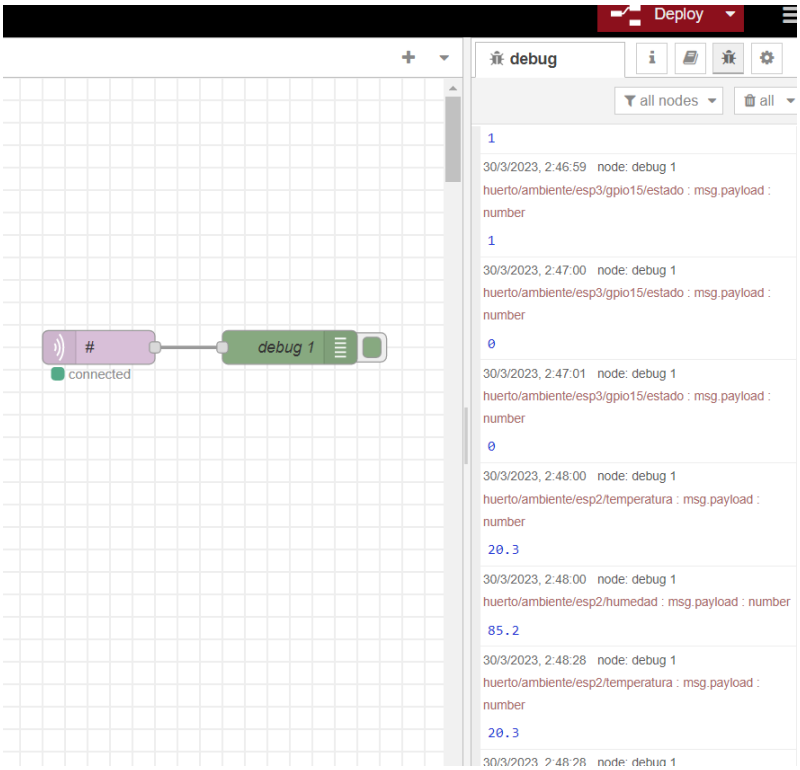

Figura 30. Mensajes de los dispositivos ESP32.

Mediante la utilización de Openhab es posible utilizar una interfaz gráfica amigable que pueda ser utilizada con un protocolo https desde cualquier parte del mundo.

- Se crea una interfaz gráfica capaz de obtener los mensajes de los dispositivos ESP32, como se muestra en la Figura 31.

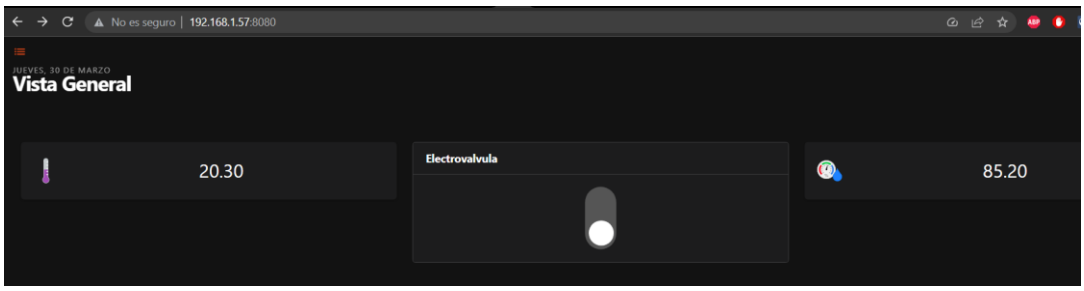

Figura 31. Creación de interfaz gráfica en Openhab.

- En un terminal de la Raspberry Pi se ingresa a las siguientes rutas que se muestran en la Tabla 7.

Tabla 7

Rutas de almacenamiento de claves para utilizar Myopenhab.

sudo nano /var/lib/openhab/openhabcloud/secret
Sudo nano /var/lib/openhab/uuid

- En un buscador se ingresa a myopenhab y se coloca un mail y las credenciales obtenidas en la Figura 32 y enseguida se puede ingresar a la interfaz gráfica con el protocolo https desde cualquier lugar del mundo, como se muestra en la Figura 33.

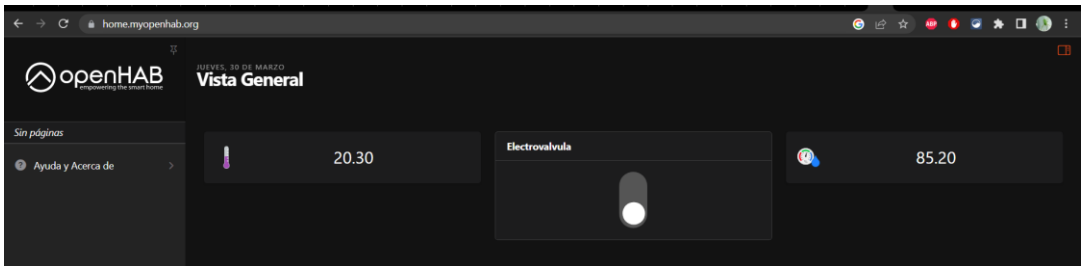

Figura 32. Ingreso a Myopenhab.org con protocolo https.

5. Viabilidad económica de la ciberseguridad en IoT para pymes

La seguridad en el Internet de las cosas (IoT) se ha convertido en un tema de gran importancia para las pequeñas y medianas empresas (Pymes) debido a que cada vez más dispositivos están conectados a la red, lo que aumenta el riesgo de ataques cibernéticos. La ciberseguridad en IoT se refiere a la protección de los dispositivos conectados y los datos que se transmiten y almacenan en ellos, con el objetivo de evitar el acceso no autorizado, el robo de información o la interrupción del funcionamiento de los dispositivos.

Para las Pymes, la ciberseguridad en IoT es especialmente importante, ya que a menudo tienen recursos limitados para implementar medidas de seguridad avanzadas. Sin embargo, estas empresas también tienen una gran responsabilidad, ya que pueden ser el objetivo de ciberdelincuentes que buscan aprovechar las vulnerabilidades de los dispositivos conectados para acceder a información valiosa.

En consecuencia, es fundamental que las Pymes comprendan la importancia de la ciberseguridad en IoT y adopten medidas de seguridad para proteger sus dispositivos y datos. Esto puede incluir la implementación de contraseñas fuertes, la actualización regular del firmware de los dispositivos, la monitorización constante de la red y la realización de copias de seguridad de los datos importantes. Además, es importante que los empleados de la empresa estén capacitados para identificar posibles amenazas y evitar prácticas inseguras en la red.

Sin embargo, la implementación de una arquitectura de ciberseguridad puede ser costosa y compleja, especialmente para las pymes con presupuestos y recursos limitados. Por lo tanto, es crucial analizar los costos involucrados en la implementación de una solución de ciberseguridad y determinar la factibilidad económica de esta inversión.

5.1 Factores principales por considerar para implementar la ciberseguridad en IoT para pymes

- Identificación de riesgos: Es importante identificar los riesgos potenciales para los dispositivos IoT y las redes empresariales antes de implementar cualquier solución de ciberseguridad. Esto ayudará a entender qué medidas de seguridad son necesarias para proteger los activos empresariales.
- Protección de dispositivos IoT: Los dispositivos IoT deben ser protegidos de manera adecuada para evitar posibles brechas de seguridad. Es importante implementar medidas de seguridad como el cifrado de datos, contraseñas seguras, y actualizaciones regulares del software.
- Monitoreo de red: La implementación de una herramienta de monitoreo de red puede ayudar a detectar posibles amenazas cibernéticas en tiempo real. También puede ayudar a identificar patrones de actividad sospechosos en la red, lo que puede ser útil para prevenir posibles ataques.
- Educación y conciencia: Es importante que los empleados de la Pyme comprendan la importancia de la ciberseguridad y estén capacitados en cómo proteger los dispositivos IoT y la red empresarial. Esto puede incluir la educación sobre el uso de contraseñas seguras, la identificación de correos electrónicos de phishing y la prevención de la descarga de software malicioso.
- Política de seguridad: La Pyme debe implementar una política de seguridad clara y detallada que aborde la ciberseguridad de los dispositivos IoT y la red empresarial. Esto debe incluir la definición de roles y responsabilidades, la definición de medidas de seguridad específicas y la creación de un plan de respuesta a incidentes.

5.2 Factores que influyen en el costo de implementación de la ciberseguridad en IoT para pymes

Algunos de los principales factores de costos involucrados en la implementación de una solución de seguridad de IoT en pymes son:

- Infraestructura: La implementación de ciberseguridad en IoT puede requerir la adquisición de nueva infraestructura, como hardware y software especializado, lo que podría aumentar los costos.
- Personal capacitado: Es esencial contar con personal capacitado en ciberseguridad para administrar y mantener la infraestructura de seguridad, lo que puede generar costos adicionales en capacitación y salarios.
- Actualizaciones de seguridad: Los costos de mantener y actualizar las soluciones de ciberseguridad en IoT también deben tenerse en cuenta, ya que se requiere una inversión continua para mantener la seguridad de los sistemas.
- Auditorías de seguridad: Las auditorías de seguridad regulares también son importantes para garantizar la eficacia de las soluciones de ciberseguridad implementadas, lo que puede generar costos adicionales.

5.3 Dispositivos esenciales para la implementación de ciberseguridad en IoT para pymes

La implementación de ciberseguridad en IoT para pymes requiere una combinación de medidas técnicas, de gestión y de concienciación para los empleados. A continuación, se presentan algunos dispositivos y soluciones que pueden ser esenciales para la implementación de ciberseguridad en IoT para pymes:

- FirewalL

Indicadores	Fortinet FortiGate 30E	Sophos XG 106	Palo Alto Networks PA-220
GAMA	Baja	Media	ALTA
MARCA	FORTINET	SOPHOS	PALO ALTO NETWORKS
Ofrece	protección básica y es adecuado para pequeñas empresas.	Amplia gama de funcionalidades.	protección completa contra amenazas de seguridad. Es adecuado para empresas grandes y organizaciones gubernamentales.
Característica	- Firewall de próxima generación - VPN SSL - Gestión centralizada - Control de aplicaciones - Control de acceso - Filtrado de URL	- Firewall de próxima generación - VPN SSL y Ipsec - Control de aplicaciones y acceso - Protección web y contra amenazas avanzadas - Gestión centralizada	- Firewall de próxima generación - VPN SSL y IPsec - Gestión centralizada - Control de aplicaciones y acceso - Protección contra amenazas avanzadas - Integración con servicios en la nube - Análisis y reportes de seguridad
Precio	$350	$1,000	$3,500

- Antivirus

Indicadores	Avast Free Antivirus	Kaspersky Anti-Virus	McAfee AntiVirus Plus
GAMA	Baja	Media	ALTA
MARCA	Avast	Kaspersky	McAfee
Ofrece	protección de los sistemas informáticos contra virus y otros tipos de programa maligno.		
Característica	- Protección antivirus y antispyware, red doméstica y de navegación web,	- Protección antivirus y antispyware, de correo electrónico, de	- Protección antivirus y antispyware, de correo electrónico, de

	de correo electrónico y contraseñas - Escaneo inteligente - Actualizaciones automáticas - Modo de juego	navegación web, pagos y compras en línea y de contraseñas. - Escaneo inteligente - Actualizaciones automáticas	navegación web, de pagos y compras en línea, de identidad y de dispositivos móviles - Escaneo inteligente - Actualizaciones automáticas
Precio	$30 anuales para un dispositivo.	$40 anuales para un dispositivo.	$50 anuales para un dispositivo.

- DMZ

Indicadores	**TP-Link TL-R600VPN**	**Ubiquiti UniFi Security Gateway**	**Fortinet FortiGate**
GAMA	Baja	Media	ALTA
MARCA	TL-R600VPN	UniFi Security Gateway	FortiGate
Característica	- Permite hasta 20 túneles VPN IPsec con un ancho de banda de hasta 100Mbps. - Incluye un firewall integrado con filtrado de URL y control de acceso. - Soporta múltiples protocolos VPN, incluyendo PPTP, L2TP y IPsec. - Incluye la limitación de velocidad y la priorización de tráfico. - compatible con las tecnologías de red IPv4 e IPv6.	- Proporciona funciones avanzadas de firewall y VPN, incluyendo soporte para redes DMZ. - Permite la configuración de políticas de seguridad avanzadas. - Incluye un controlador UniFi. - Permite la configuración remota y la supervisión del dispositivo a través de la plataforma UniFi. - Compatible con las tecnologías de red IPv4 e IPv6.	- Proporcionan funciones avanzadas de seguridad, como firewall, VPN, prevención de intrusiones, antivirus, filtrado web y control de aplicaciones. - procesamiento de alto - Incluyen una interfaz de gestión unificada. - Ofrecen integración con otros productos de seguridad de Fortinet, como FortiAnalyzer y FortiManager.
Precio	$60	$100	$1500

- DLP

Los dispositivos DLP (Data Loss Prevention) son herramientas de seguridad que ayudan a prevenir la pérdida o fuga de datos sensibles de una empresa.

Indicadores	**Endpoint Protector**	**Symantec Data Loss Prevention**	**McAfee Total Protection for DLP**
GAMA	Baja	Media	ALTA
MARCA	Endpoint Protector	Symantec DLP	McAfee
Ofrece	Proporciona características básicas de prevención de pérdida de datos y es compatible con Windows, Mac y Linux.	Proporciona características avanzadas de prevención de pérdida de datos, como análisis de contenido en tiempo real y la capacidad de bloquear la transferencia de datos sensibles.	Características avanzadas de prevención de pérdida de datos, como monitoreo continuo, análisis de contenido en tiempo real y la capacidad de bloquear la transferencia de datos sensibles. También ofrece integración con otras soluciones de seguridad de McAfee.
Característica	- Monitoreo y control de dispositivos de almacenamiento externos, como USB y discos duros externos. - Protección de datos en la nube a través de integraciones con servicios de almacenamiento. - Análisis de contenido en tiempo real.	- Identificación y clasificación de datos sensibles - Prevención de la pérdida de datos - Monitorización y auditoría - Integración con otros productos de seguridad	- Identificación y clasificación de datos sensibles - Prevención de la pérdida de datos - Monitorización y auditoría - Integración con otros productos de seguridad - Protección de dispositivos móviles

	- Generación de informes y registros.		
Precio	$3 por usuario por mes.	$20 por usuario por mes.	$60 por usuario por mes.

- Antispam

Indicadores	**MailWasher**	**SonicWALL Email Security**	**Symantec Messaging Gateway**
GAMA	Baja	Media	ALTA
MARCA	MailWasher	SonicWALL	Symantec
Característica	- MailWasher escanea y filtra los mensajes de correo electrónico entrantes. - Función de "Lista negra" que permite a los usuarios bloquear automáticamente el correo electrónico de remitentes específicos. - Configuración avanzada para personalizar la forma en que se manejan los mensajes de spam.	- Filtro antispam y antivirus avanzado. - Protección contra phishing y malware. - Soporte para la autenticación de correo electrónico basada en DKIM, SPF y DMARC. - Integración con otros dispositivos de seguridad de SonicWALL.	- Filtro antispam y antivirus. - Control de contenido. - Prevención de la pérdida de datos (DLP) para garantizar el cumplimiento de las políticas de seguridad y privacidad de datos. - Interfaz de usuario basada en web. - Herramientas de informes y análisis.
Precio	MailWasher Pro es de $29.95 por dispositivo, y la versión Lifetime Pro tiene un precio de $89.95 por dispositivo.	$1,000 por una licencia básica.	$5,000 por una licencia básica.

- Gestores de contraseñas

Indicadores	**KeePass**	**Dashlane**	**CyberArk Vault**

GAMA	Baja	Media	ALTA
MARCA	KeePass	Dashlane	McAfee
Característica	- Almacenamiento seguro de contraseñas. - Generador de contraseñas - Integración del navegador - Compatible con múltiples plataformas - Soporte para grupos y etiquetas - Extensiones y complementos	- Almacenamiento seguro de contraseñas - Generador de contraseñas - Autenticación de dos factores - Monitoreo de la dark web - Compartir contraseñas seguras - Autofill y autologin - Compatible con múltiples plataformas	- Almacenamiento seguro de contraseñas - Administración de cuentas privilegiadas - Monitoreo y alertas - Integración con múltiples plataformas - Control de acceso y permisos
Precio	No se encuentra disponible los costos.	$11.99 USD por mes.	No se encuentra disponible los costos, solo cotización.

- Sistema de control de acceso basados en la biometría

Los sistemas de control de acceso basados en la biometría utilizan características físicas únicas de los usuarios, como la huella dactilar o el escaneo de la retina, para permitir el acceso a los sistemas y dispositivos de IoT.

Indicadores	**ZKTeco Biosecurity Lite**	**Suprema BioEntry W2**	**HID Biometric Reader**
GAMA	Baja	Media	ALTA
MARCA	ZKTeco	Suprema	HID Global
Ofrece	- identificación de huellas dactilares. - Tarjeta RFID y contraseña. - Puede ser utilizado en pequeñas	- identificación de huellas dactilares. - Reconocimiento facial. - Tarjeta RFID - Puede ser utilizado en pequeñas y	- Múltiples modalidades de autenticación biométrica, incluyendo huella dactilar. - Reconocimiento facial.

	empresas y hogares	medianas empresas	- Reconocimiento de iris y de voz - Es adecuado para empresas grandes y organizaciones gubernamentales
Precio	$200	$600	$2000

5.4 Toma de decisiones para la implementación de ciberseguridad en IoT

Para tomar decisiones informadas sobre la implementación de ciberseguridad en IoT, es útil contar con la siguiente información:

- Análisis de riesgos: Un análisis detallado de los riesgos de seguridad cibernética a los que están expuestos los dispositivos IoT. Esto permitirá identificar los puntos críticos que necesitan protección y entender los riesgos asociados con cada uno.
- Soluciones disponibles: Conocer las diferentes soluciones de ciberseguridad disponibles en el mercado para proteger los dispositivos IoT. Esto incluye software, hardware, soluciones de seguridad gestionadas externamente, entre otros.
- Costos asociados: Tener una comprensión clara de los costos asociados con la implementación de soluciones de ciberseguridad. Esto incluye el costo de adquisición y configuración de la solución, así como el costo de mantenimiento y actualización.
- Retorno de inversión: Entender el retorno de inversión (ROI) de la implementación de una solución de ciberseguridad. Esto puede incluir el ahorro en costos de reparación de dispositivos IoT en caso de una violación de seguridad cibernética, así como el aumento en la confianza de los clientes y la mejora de la reputación de la empresa.

- Evaluación de escalabilidad: Evaluar la escalabilidad de la solución de ciberseguridad, es decir, si puede ser implementada y adaptada a medida que la empresa crece y se expande.
- Políticas y regulaciones: Conocer las políticas y regulaciones relevantes relacionadas con la ciberseguridad en el sector agrícola, incluyendo las leyes y regulaciones de protección de datos.

5.5. Implementación de ciberseguridad en IoT para pymes

Para la implementación de una infraestructura de ciberseguridad con IoT para pymes L o primero que se debe hacer es evaluar las necesidades de ciberseguridad de la empresa y establecer un presupuesto adecuado. Es importante considerar los riesgos de seguridad específicos de la empresa y cómo pueden abordarse de manera efectiva.

En lugar de comprar soluciones individuales de seguridad, es recomendable buscar soluciones integrales que ofrezcan múltiples capas de protección en una sola herramienta. Por ejemplo, un paquete de software de seguridad que incluya antivirus, firewall y control de acceso puede ser más efectivo y rentable que comprar cada herramienta por separado.

Las herramientas de seguridad deben ser fáciles de usar y administrar para que el personal de la empresa pueda entender cómo utilizarlas sin problemas. Si las herramientas son complicadas de usar, la empresa puede terminar pagando por una solución que no se utiliza de manera efectiva.

es importante asegurarse de que el proveedor de la herramienta de seguridad ofrezca soporte técnico confiable y actualizaciones regulares para protegerse de nuevas amenazas de seguridad, es así como las herramientas de ciberseguridad deben ser efectivas, pero también accesibles en términos de costo y complejidad.

Por último, Es importante recordar que cada empresa tiene necesidades de seguridad únicas, por lo que es importante evaluar cuidadosamente las necesidades específicas de la empresa antes de seleccionar herramientas de ciberseguridad. Además, es importante asegurarse de que todas las herramientas estén actualizadas regularmente para garantizar la protección contra las últimas amenazas de seguridad.

6. Resultados y discusión

Mediante kali linux se realizó una comprobación del estado el puerto 1883 el cual es utilizado para el protocolo MQTT sin TLS, se pudo comprobar que el puerto se encuentra cerrado con lo cual podemos asegurar que el prototipo está funcionando con el puerto seguro 8883 como se muestra en la Figura 33.

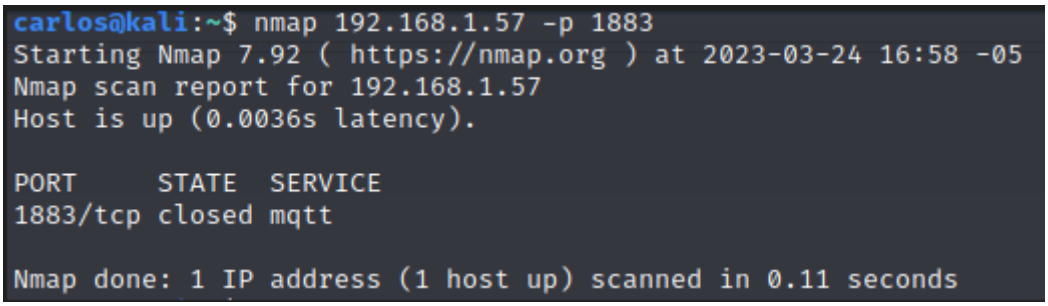

Figura 33. Estado del puerto 1883.

Se tomo una muestra del tráfico que existe en la red y se guardó en un archivo con el nombre de dump.pcap este archivo se lo ejecuto con wireshark como se observa en la Figura 34.

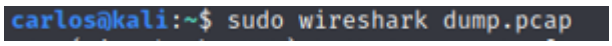

Figura 34. Captura de tráfico de red.

Los resultados mostraron que se está trabajando con el protocolo MQTT/TLS en el puerto seguro 8883 y que los mensajes están cifrados y no son posibles de leer ni manipular como se muestra en la Figura 35.

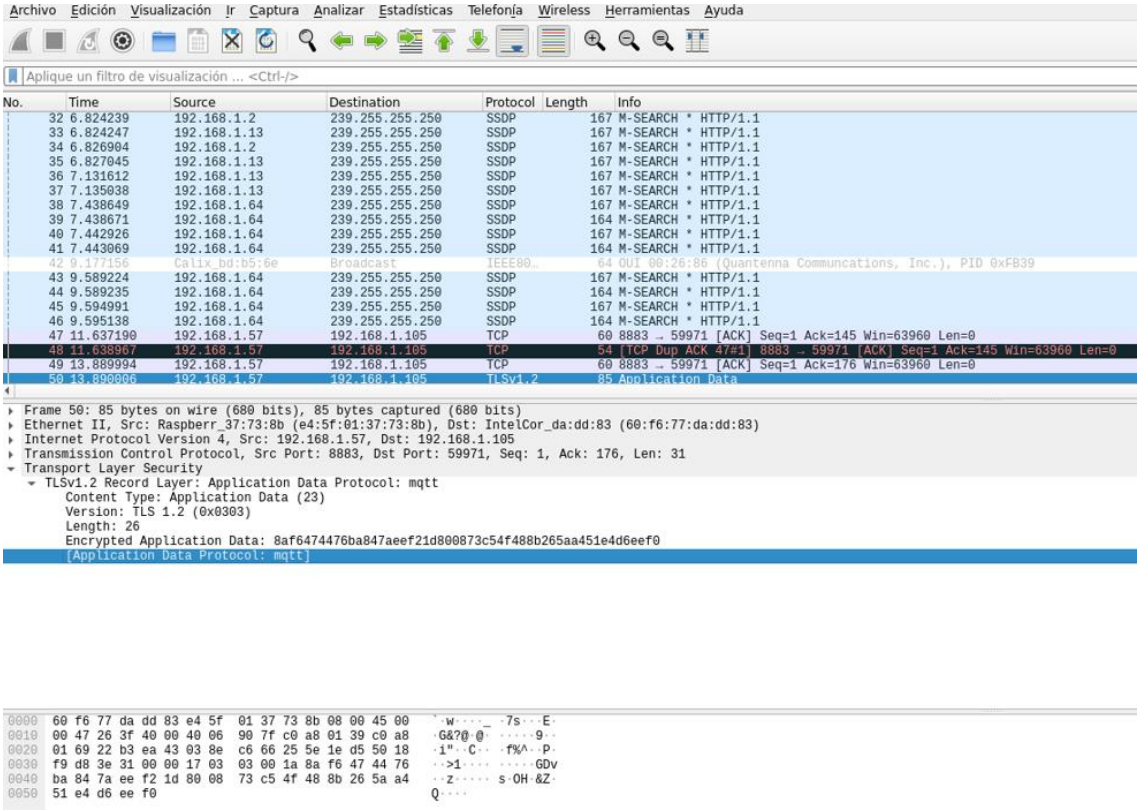

Figura 35. Mensajes encriptados.

Ventajas	Desventajas
El uso de firmas electrónicas permite el intercambio seguro de llaves de encriptación entre bróker y clientes.	La programación en los Esp32 utiliza más recursos de memoria flash y memoria dinámica. aproximadamente un 20% más.
Los certificados de autenticación permiten una encriptación eficiente del tráfico de mensajes.	Utilizar Mqtt/TLS en los Esp32 implica tener un aumento considerable en el consumo de

	energía, cerca de 15% más comparado con un protocolo no cifrado.
El protocolo utiliza el puerto 8883 para su comunicación, el cual está destinado de manera estándar para una conexión segura.	Puede existir una sobrecarga de comunicación debido a los dispositivos que no son diseñados para trabajos de computación intensa.
Es un protocolo ligero que utiliza poco ancho de banda.	

Esta arquitectura se ha diseñado tomando como referencia una pyme orientada a la elaboración de sistemas de riego IoT para huertos caseros, en donde se hace uso del protocolo Mqtt no cifrado.

Mqtt al ser un protocolo que fue diseñado sin tomar en cuenta la seguridad de la información es extremadamente vulnerable a ataques “Man in the Middle” lo cual para una Pyme podría se perjudicial ya que la información puede ser leída o incluso alterada poniendo en riesgo toda la operación de la Pyme, por esta razón es importante utilizar MQTT/TLS ya que mediante este protocolo se asegura una vía de comunicación cifrada que es segura y utiliza el puerto 8883 el cual está destinado exclusivamente por la Internet Assigned Numbers Authority (IANA) para el uso del protocolo MQTT seguro a través de TLS.

Para una Pyme que dispone de una arquitectura IoT el poder monitorear los dispositivos desde cualquier parte del mundo es de gran utilidad, para lo cual en este documento se propone el uso de Openhab, ya que permite utilizar el protocolo MQTT/SSL y también proporciona una VPN privada segura, gratuita que permite al

usuario de la Pyme interactuar con la arquitectura IoT de manera segura desde cualquier lugar del mundo.

7. Conclusiones

- El análisis del estado del arte de las arquitecturas de ciberseguridad en las infraestructuras IoT ha dejado en claro la importancia de abordar los desafíos de seguridad que enfrentan las pymes en la actualidad. Las soluciones de ciberseguridad deben ser diseñadas y adaptadas para satisfacer las necesidades específicas de cada organización, y deben ser actualizadas y monitoreadas constantemente para garantizar una protección adecuada contra las amenazas cibernéticas.
- La arquitectura propuesta demostró que el protocolo MQTT/TLS permite una comunicación encriptada entre clientes y bróker cumpliendo con los principios de autenticación de dispositivos, encriptación de mensajes e integridad que son los principios del protocolo. La utilización del puerto 8883 que es el puerto seguro para el uso del protocolo permitió cerrar el puerto 1883 evitando de esta manera que exista un ataque por este puerto.
- Se logró implementar un prototipo para llevar a cabo pruebas de vulnerabilidad en donde se logró demostrar que los mensajes de los clientes enviados al bróker llegan encriptados y no es posible acceder al bróker ni suscribirse o publicar mensajes sin tener las llaves y certificados de seguridad necesarios. Este tipo de arquitectura puede ser utilizada en cualquier infraestructura IoT.
- Las herramientas básicas para ciberseguridad de pymes son esenciales para proteger los sistemas y datos de la empresa de los riesgos cibernéticos. Es importante que las empresas implementen estas herramientas y adopten buenas prácticas de seguridad para reducir el riesgo de ser víctimas de ciberataques y proteger la información de la empresa.

Referencias

Caiza Narváez, J. J., Márceles Villalba, K., & Amador Donado, S. (2021). Arquitectura basada en tecnologías emergentes y tecnología de monitoreo de tráfico de red. Investigación e Innovación En Ingenierías, 9(3), 18-31. https://doi.org/10.17081/invinno.9.3.5340

Chulde, L., & Défaz, H. (2021). Diseño del Modelo de Ciberseguridad IADI para el Sistema de Gestión Académica Ignug del Instituto Superior Tecnológico Yavirac. Ecuadorian Science Journal, 5(3), 272-292. https://doi.org/10.46480/esj.5.3.160

Cisco. (2018). Elementos esenciales de seguridad en las Pymes.

Guzmán Y Valle, E., Mater, A., Magisterio, D., Facultad, N., Ciencias, D. E., Delgado, Q., & Milagros, F. (2019). Software Libre.

HaddadPajouh, H., Khayami, R., Dehghantanha, A., Choo, K. K. R., & Parizi, R. M. (2020). AI4SAFE-IoT: an AI-powered secure architecture for edge layer of Internet of things. Neural Computing and Applications, 32(20), 16119-16133. https://doi.org/10.1007/s00521-020-04772-3

Iavarone Gisella Paula. (2012). Costos por órdenes de producción: su aplicación a la INDUSTRIA PAULA GISELLA IAVARONE.

Instituto Nacional de ESPaña de Ciberseguridad Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. Https://Www.Incibe.Es/Protege-Tu-Empresa/Blog/El-Pentesting-Auditando-Seguridad-Tus-Sistemas.

Jhordany Serna Valdivia, E., & Mejia Miranda, J. (2020). Propuesta de un Agente Inteligente para el Manejo y Mitigación de Riesgos de Ciberseguridad en Entornos IoT. Applications in Software Engineering - Proceedings of the 9th International Conference on Software Process Improvement, CIMPS 2020, 158. https://doi.org/10.1109/CIMPS52057.2020.9390153

Kali.org. (2022). What is Kali Linux? Https://Www.Kali.Org/Docs/Introduction/What-Is-Kali-Linux/#kali-Linux-Features.

Lawal, M. A., Shaikh, R. A., & Hassan, S. R. (2020). An anomaly mitigation framework for iot using fog computing. Electronics (Switzerland), 9(10), 1-24. https://doi.org/10.3390/electronics9101565

Lombardi, J., & Arevalo, C. (2020). «Diseño de una Arquitectura de ciberseguridad para los servicios de plataformas IoT en el área de TI dentro de la empresa Pacífico Seguros».

Maggi Murillo Paul, & Gomez Omar. (2021a). Estudio preliminar sobre conocimiento de Ciberseguridad Pymes Riobamba.

Maggi Murillo Paul, & Gomez Omar. (2021b). Estudio preliminar sobre conocimiento de Ciberseguridad Pymes Riobamba.

Ministerio de Telecomunicaciones. (2021). Acuerdo-No.-006-Anexo-Politica-de-Ciberseguridad.

Ministerio de Telecomunicaciones, & Ministro de Telecomunicaciones. (2021). Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.

Morales Suárez, A. C., Díaz Ávila, S. S., & Leguizamón Páez, M. Á. (2019). Mecanismos de seguridad en el internet de las cosas. Revista Vínculos, 16(2), 288-297. https://doi.org/10.14483/2322939x.15758

Muñoz Santiago. (2018). Resolución N° SB-CGPMC-2018-004 Super Intendencia de Bancos Bases legales Seguridad de la información.

Naciones Unidas. (2020). Boletín FAL No 382. La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad.

Normas ISO 27001. (2022). Norma ISO 27001. Https://Normaiso27001.Es/#h1.

Peralta Marco, & Aguilar Daniela. (2021). La Ciberseguridad y su concepción en las Pymes de Cuenca, Ecuador.

Pinzón Iraldo. (2014). Gestion del riesgo en seguridad informatica.

Ramírez Bravo Pía. (2006). UNIVERSIDAD DE CHILE METODOLOGÍA ITIL.

Rodríguez-Mendoza, R., & Aviles-Sotomayor, V. (2020). Las Pymes en Ecuador un análisis necesario. 593 Digital Publisher CEIT, 5-1(5), 191-200. https://doi.org/10.33386/593dp.2020.5-1.337

Romo Santiago. (2022). Hacking Ético: Nociones y Conceptos. Entendiendo el Hacking Ético.

Rose, K., Eldridge, S., & Chapin, L. (2015). Internet de las cosas IoT - Breve reseña.

Tanenbaum, A. S., & Wetherall, D. J. (2012). Redes de computadoras. Pearson Educación.

Valderrama Jhon Edinson. (2017). Pentesting Prueba de penetración para la identificación de Vuñnerabilidades. 20-29.

Velásquez Contreras, A. (2007). La Organización, el sistema y su dinámica: una versión desde Niklas Luhmann. http://www.epsilones.com/paginas/i-figurasimp.html#figimp-ambiguedadanimal

Zuña Edgar, Arce ángel, Romero Wilson, & Soledispa César. (2019). Análisis de la seguridad informática en las PYMES de la ciudad de Milagro. 4. https://orcid.org/0000-0002-9316-1262

Anexos

Anexo 1 Programación del módulo uno

```
#include <WiFi.h>
//#include <WiFiClientSecure.h>
#include "src/dependencies/WiFiClientSecure/WiFiClientSecure.h"
#include <time.h>
#include <PubSubClient.h>
//#include "secrets.h"
#include "DHT.h"
float h;
float t;
const int DHTPin =4;
#define DHTTYPE DHT11
DHT dht(DHTPin,DHTTYPE);
#ifndef SECRET
  const char ssid[] = "CELERITY_SOFY";
  const char pass[] = "$%Thepolice";

  #define HOSTNAME "esp2"

  const char *MQTT_HOST = "192.168.1.57";
  const int MQTT_PORT = 8883;
  const char *MQTT_USER = "";
  const char *MQTT_PASS = "";

  const char* local_root_ca = R"EOF(
    -----BEGIN CERTIFICATE-----
MIIDgTCCAmmgAwIBAgIUXA94QzEG86iAmt+9XNWvgJJxOQIwDQYJKoZIhvcNAQEL
BQAwUDELMAkGA1UEBhMCRUMxEzARBgNVBAgMClNvbWUtU3RhdGUxDDAKBgNVBAoM
A01PVDEPMA0GA1UECwwGY2xpZW50MQ0wCwYDVQQDDAR0ZXN0MB4XDTIzMDMyMzIz
NTQwNloXDTI4MDMyOTIzNTQwNlowUDELMAkGA1UEBhMCRUMxEzARBgNVBAgMClNv
bWUtU3RhdGUxDDAKBgNVBAoMA01PVDEPMA0GA1UECwwGY2xpZW50MQ0wCwYDVQQD
DAR0ZXN0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0SgfV2OWhohn
SeujTZADRjqRo09+S9FclVnT3Gows4Am+IWzg03j/eZrrJPjRZvEHpSzTOb0c/lX
b+avhuOSvc6howyVAle7Uymbj8wO/i7wbVU9M3KLaW73jXw9HrzkDn9ce2r5gKZq
T8qNwbe8F4ZSDJkxJiMawJaPlk6LOLaTmd3uzIlbzy0sMFbMV9wzx0bDDw32mC6v
PgBphmmSh+mzv262GCzHRp2F9ER9WklWd4OOZt7Mk/ghrCrJUfIHFI/xx7Kou6Qk
84d+5Ux2jppeTseyGYyQ33E4d0WBwDE8vZjZWqScuAIblu+6o2letYnxZRmKBS4S
RDgCIki6pQIDAQABolMwUTAdBgNVHQ4EFgQUCwKvVsU28P/SJycChTZqs7KLawkw
HwYDVR0jBBgwFoAUCwKvVsU28P/SJycChTZqs7KLawkwDwYDVR0TAQH/BAUwAwEB
/zANBgkqhkiG9w0BAQsFAAOCAQEAdeJlbsJbkQed0jflssHlFOMN7CzNbSHvHllh
l5ACLqZPlIU+Kmxna8npAcTA/+lOfbZ6qDVoIsJlNsbKYiKwG+TvfWm7TKrNeJDM
ssq6StIPmkXrpg89xDvufQMIRldzNFZF7YGZbqugDcI69JWTS49aJ7jdndDFOTfS
ePB9gEHfdtOopPzHbQLakXxohwA9lbLZmxswDgnkGe7g5TCzAyX40Q39cDg+Ljdh
UrTgPGSKUhz/zU3O25T6b9k98a0qS3lEm+Xjf3NlYfniUiEUhJM+kAnJeZwz7PRt
T3lIMGqc9kSH7nZRdIK0dq/T5vlx7d/r2aYo5f5dmmbBfBKyVQ==
    -----END CERTIFICATE-----)EOF";

#endif
```

Elaborado por: Carlos Cuaical e Israel De La Torre

```
49  const char MQTT_SUB_TOPIC[] = "test/" HOSTNAME "/in";
50  const char MQTT_PUB_TOPIC[] = "test/"HOSTNAME"/out";
51
52  WiFiClientSecure net;
53  PubSubClient client(net);
54
55  time_t now;
56  unsigned long lastMillis = 0;
57
58  void mqtt_connect()
59  {
60      while (!client.connected()) {
61      Serial.print("Time:");
62      Serial.print(ctime(&now));
63      Serial.print("MQTT connecting");
64      if (client.connect(HOSTNAME, MQTT_USER, MQTT_PASS)) {
65        Serial.println("connected");
66        client.subscribe(MQTT_SUB_TOPIC);
67      } else {
68        Serial.print("failed, status code =");
69        Serial.print(client.state());
70        Serial.println("try again in 5 seconds");
71        /* Wait 5 seconds before retrying */
72        delay(5000);
73      }
74    }
75
76  }
77
78  void receivedCallback(char* topic, byte* payload, unsigned int length) {
79    Serial.print("Received [");
80    Serial.print(topic);
81    Serial.print("]: ");
82    for (int i = 0; i < length; i++) {
83      Serial.print((char)payload[i]);
84    }
85  }
86
87  void setup()
88  {
89    Serial.begin(115200);
90    dht.begin();
91    Serial.print("Attempting to connect to SSID: ");
92    Serial.println(ssid);
93    WiFi.setHostname(HOSTNAME);
94    WiFi.mode(WIFI_AP_STA);
95    WiFi.begin(ssid, pass);
```

Elaborado por: Carlos Cuaical e Israel De La Torre

```
  WiFi.begin(ssid, pass);
  while (WiFi.status() != WL_CONNECTED)
  {
    Serial.print(".");
    delay(1000);
  }
  Serial.println();
  Serial.print("Connected to ");
  Serial.println(ssid);

  Serial.print("Setting time using SNTP");
  configTime(-5 * 3600, 0, "pool.ntp.org", "time.nist.gov");
  now = time(nullptr);
  while (now < 1510592825) {
    delay(500);
    Serial.print(".");
    now = time(nullptr);
  }
  Serial.println("");
  struct tm timeinfo;
  gmtime_r(&now, &timeinfo);
  Serial.print("Current time: ");
  Serial.print(asctime(&timeinfo));

  net.setCACert(local_root_ca);
  client.setServer(MQTT_HOST, MQTT_PORT);
  client.setCallback(receivedCallback);
  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())
```

Elaborado por: Carlos Cuaical e Israel De La Torre

```
    {
      mqtt_connect();
    }
    else
    {
      client.loop();
    }
  }

  if (millis() - lastMillis > 5000) {
    lastMillis = millis();
    //client.publish(MQTT_PUB_TOPIC, ctime(&now), false);
   // h=dht.readHumidity();
    //t=dht.readTemperature();
    h= 85.2;
    t= 20.3;
    float f = dht.readTemperature(true);
    float hic=dht.computeHeatIndex(t,h,false);
    static char temperatureTemp[7];
    dtostrf(t,6,2,temperatureTemp);
    static char humidityTemp[7];
    dtostrf(h,6,2,humidityTemp);
    client.publish("huerto/ambiente/esp2/temperatura",temperatureTemp);
    client.publish("huerto/ambiente/esp2/humedad",humidityTemp);
    Serial.println(h);
    Serial.println(t);
  }
}
```

Elaborado por: Carlos Cuaical e Israel De La Torre

Anexo 2 Programación del módulo dos

```
#include <WiFi.h>
//#include <WiFiClientSecure.h>
#include "src/dependencies/WiFiClientSecure/WiFiClientSecure.h"
#include <time.h>
#include <PubSubClient.h>
//#include "secrets.h"
int gpio0 = 0;
#ifndef SECRET
  const char ssid[] = "CELERITY_SOFY";
  const char pass[] = "$%Thepolice";

  #define HOSTNAME "test2"

  const char *MQTT_HOST = "192.168.1.57";
  const int MQTT_PORT = 8883;
  const char *MQTT_USER = ""; // leave blank if no credentials used
  const char *MQTT_PASS = ""; // leave blank if no credentials used

  const char* local_root_ca = R"EOF(
    -----BEGIN CERTIFICATE-----
MIIDgTCCAmmgAwIBAgIUXA94QzEG86iAmt+9XNWvgJJxOQIwDQYJKoZIhvcNAQEL
BQAwUDELMAkGA1UEBhMCRUMxEzARBgNVBAgMClNvbWUtU3RhdGUxDDAKBgNVBAoM
A01PVDEPMA0GA1UECwwGY2xpZW50MQ0wCwYDVQQDDAR0ZXN0MB4XDTIzMDMyMzIz
NTQwNloXDTI4MDMyOTIzNTQwNlowUDELMAkGA1UEBhMCRUMxEzARBgNVBAgMClNv
bWUtU3RhdGUxDDAKBgNVBAoMA01PVDEPMA0GA1UECwwGY2xpZW50MQ0wCwYDVQQD
DAR0ZXN0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0SgfV2OWhohn
SeujTZADRjqRo09+S9FclVnT3Gows4Am+IWzg03j/eZrrJPjRZvEHpSzTOb0c/lX
b+avhuOSvc6howyVAle7Uymbj8wO/i7wbVU9M3KLaW73jXw9HrzkDn9ce2r5gKZq
T8qNwbe8F4ZSDJkxJiMawJaPlk6LOLaTmd3uzIlbzy0sMFbMV9wzx0bDDw32mC6v
PgBphmmSh+mzv262GCzHRp2F9ER9WklWd4OOZt7Mk/ghrCrJUfIHFI/xx7Kou6Qk
84d+5Ux2jppeTseyGYyQ33E4d0WBwDE8vZjZWqScuAIblu+6o2letYnxZRmKBS4S
RDgCIki6pQIDAQABo1MwUTAdBgNVHQ4EFgQUCwKvVsU28P/SJycChTZqs7KLawkw
HwYDVR0jBBgwFoAUCwKvVsU28P/SJycChTZqs7KLawkwDwYDVR0TAQH/BAUwAwEB
/zANBgkqhkiG9w0BAQsFAAOCAQEAdeJlbsJbkQed0jflssHlFOMN7CzNbSHvHllh
l5ACLqZPlIU+Kmxna8npAcTA/+lOfbZ6qDVoIsJlNsbKYiKwG+TvfWm7TKrNeJDM
ssq6StIPmkXrpg89xDvufQMIRldzNFZF7YGZbqugDcI69JWTS49aJ7jdndDFOTfS
ePB9gEHfdtOopPzHbQLakXxohwA91bLZmxswDgnkGe7g5TCzAyX40Q39cDg+Ljdh
UrTgPGSKUhz/zU3O25T6b9k98a0qS3lEm+Xjf3NlYfniUiEUhJM+kAnJeZwz7PRt
T3lIMGqc9kSH7nZRdIK0dq/T5vlx7d/r2aYo5f5dmmbBfBKyVQ==
    -----END CERTIFICATE-----)EOF";

#endif

const char MQTT_SUB_TOPIC[] = "huerto/ambiente/esp3/gpio15/estado";

WiFiClientSecure net;
PubSubClient client(net);
```

Elaborado por: Carlos Cuaical e Israel De La Torre

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

void mqtt_connect()
{
    while (!client.connected()) {
    Serial.print("Time:");
    Serial.print(ctime(&now));
    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("]: ");
  String messageOpenhab;
  for (int i = 0; i < length; i++) {
    Serial.print((char)payload[i]);
    messageOpenhab += (char)payload[i];
  }
  Serial.println("");
  if(messageOpenhab == "1"){digitalWrite(gpio0, HIGH);} else if (messageOpenhab == "0"){digitalWrite(gpio0,LOW);}
}

void setup()
{
  pinMode(gpio0, OUTPUT);
  digitalWrite(gpio0,LOW);
  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);
```

Elaborado por: Carlos Cuaical e Israel De La Torre

```
  while (WiFi.status() != WL_CONNECTED)
  {
    Serial.print(".");
    delay(1000);
  }
  Serial.println();
  Serial.print("Connected to ");
  Serial.println(ssid);
  Serial.print("Setting time using SNTP");
  configTime(-5 * 3600, 0, "pool.ntp.org", "time.nist.gov");
  now = time(nullptr);
  while (now < 1510592825) {
    delay(500);
    Serial.print(".");
    now = time(nullptr);  }
  Serial.println("");
  struct tm timeinfo;
  gmtime_r(&now, &timeinfo);
  Serial.print("Current time: ");
  Serial.print(asctime(&timeinfo));
  net.setCACert(local_root_ca);
  client.setServer(MQTT_HOST, MQTT_PORT);
  client.setCallback(receivedCallback);
  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(); }
}
```

Elaborado por: Carlos Cuaical e Israel De La Torre