**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| Programa de formación | Implementación de seguridad en Internet de las cosas |
| --- | --- |

| Competencia | 220501110 - Implementar el sistema de seguridad de la información según modelo y estándares técnicos. | Resultado de aprendizaje | 220501110-03 - Desplegar las estrategias de seguridad en IoT de acuerdo a planeación realizada. |
| --- | --- | --- | --- |

| Número del componente formativo | 02 |
| --- | --- |
| Nombre del componente formativo | Control de amenazas en IoT |
| Breve descripción | En la actualidad, las empresas, hogares y demás instituciones recurren a la seguridad de sus datos, para mejorar su productividad y aumentar la rentabilidad, a través de procesos ágiles y de calidad; por ello, es imprescindible adoptar medidas que contribuyan a la seguridad en IoT, identificando agujeros de seguridad en los dispositivos que conforman la red IoT y posibles controles. |
| Palabras clave | Activo de información, amenazas, ciberseguridad, estándar, metodología, riesgo |

| Área ocupacional | 2 - Ocupaciones en Ciencias Naturales, aplicadas y relacionadas |
| --- | --- |
| Idioma | Español |

1. **TABLA DE CONTENIDO**

**Introducción**

**1. Protocolos de comunicación IoT**

1.1. MQTT

1.2. Seguridad en MQTT

**2. MOSQUITTO**

**3. Evaluación de seguridad MQTT**

1. **INTRODUCCIÓN**

Se da la bienvenida al componente formativo denominado “Control de amenazas en IoT”, que hace parte del programa de formación complementario “Implementación de seguridad en Internet de las cosas”. La temática a conocer está basada en MQTT, que es el protocolo principal del denominado Internet de las cosas (IoT); este es un servicio de mensajería donde los mensajes se envían de forma directa desde el servidor a los dispositivos móviles, como teléfonos inteligentes o tabletas, y aplicaciones de escritorio.

Para conocer un poco más se invita a observar el siguiente video:



1. **DESARROLLO DE CONTENIDOS**
2. **Protocolos de comunicación IoT**

Los **protocolos de comunicación** son descripciones formales de formatos y reglas de mensajes digitales, se consideran también como el conjunto de normas de mensajes digitales que deben cumplir los dispositivos y programas que intercambian comunicación de datos; sin estas reglas la comunicación resultaría caótica y por tanto, imposible.

Los protocolos de comunicaciones abarcan la autenticación, detección y corrección de errores y señalización, además pueden evidenciar la sintaxis, la semántica y la sincronización de las comunicaciones analógicas y digitales. La implementación de los protocolos se realiza en *hardware* y *software*, pues todas las comunicaciones analógicas como las digitales los utilizan. Existen algunos como:

* Protocolo de Información Industrial (DNP).
* Protocolo de Internet (IP).
* Protocolo de Información de Transmisión (TCP).

Estos generan conexiones entre todos los dispositivos enlazados.

* 1. **MQTT**

Sus siglas significan *Message Queuing Telemetry Transport*, es un protocolo muy sencillo usado para para transmitir mensajes cortos provenientes de cualquier dispositivo, desde o hacia una red de sensores / actuadores; su comunicación es de mensajería ligera y está diseñado para telemetría M2M (máquina a máquina), en entornos de ancho de banda bajo. La forma de comunicación trabaja como un sistema de publicar y suscribirse, los dispositivos publican mensajes sobre un tópico específico, todos los dispositivos que están suscritos a ese tópico reciben el mensaje; por ello, se considera que su modelo de comunicación que está basado en el productor - consumidor.

Con el protocolo MQTT es posible que los dispositivos de IoT envíen o publiquen información con recursos limitados a un servidor que funciona como un agente de mensajes MQTT, acerca de un tema determinado.

Entre las principales aplicaciones MQTT se incluye el envío de mensajes a salidas de control, leer y publicar datos desde sensores y otras muchas más aplicaciones. MQTT se usa actualmente en autos inteligentes, casas inteligentes, fábricas, ciudades inteligentes, productos de consumo, etc.

Hay varias versiones de MQTT ¿sabe cuáles son? Esta es su oportunidad para que se actualice y se contextualice al respecto:

* MQTT v3.1.0.
* MQTT v3.1.1 - en uso común.
* MQTT v4 uso limitado.
* MQTT SN.

En MQTT no es necesario que el dispositivo que publica y el dispositivo que recibe mensajes estén conectados o sincronizados al mismo tiempo, puesto que el *Broker* es capaz de guardar los mensajes de los clientes, a diferencia de aplicaciones industriales donde los mensajes son consumidos en tiempo real, todo depende del requerimiento puntual a resolver, es decir, las bases del protocolo MQTT son de alguien que publica un mensaje usando un *topic* específico y el *Broker* distribuye el mensaje a todos los clientes (aplicaciones o dispositivos) que están suscritos a ese *topic,* esos clientes reciben y consumen los datos de esos mensajes.

**Figura 1**

*MQTT*

| Diagrama  Descripción generada automáticamente con confianza media | Observando la figura, existe un dispositivo que publica un mensaje, este dispositivo no requiere conocer nada de otro u otros componentes que consumen esos mensajes, diferente a las redes TCP/IP en la que sí es necesario conocer la dirección IP origen e IP destino, además del puerto usado. Con MQTT solo se necesita conocer una sola dirección y es la del Broker, ver figura. |
| --- | --- |

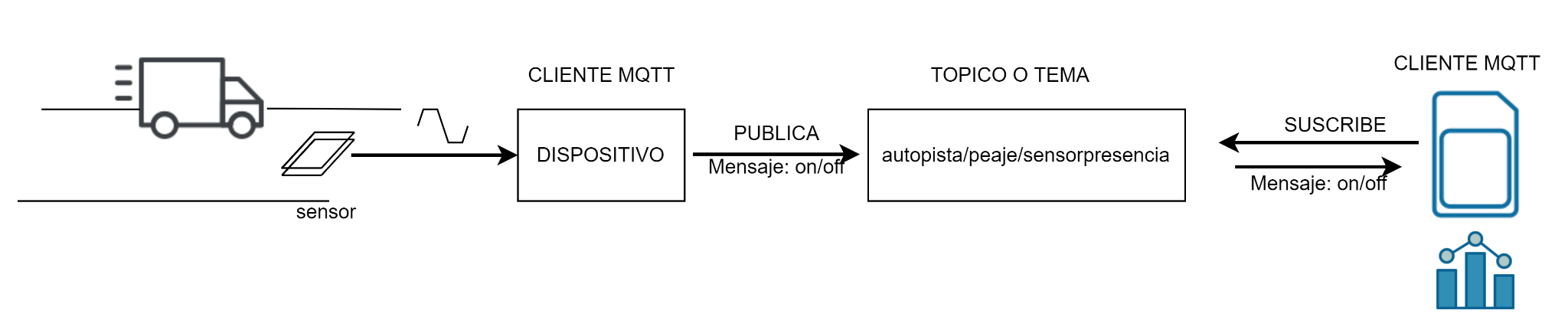
Para adentrarse en el mundo de MQTT se deben conocer algunos conceptos relacionados:



Para ejemplificar lo mencionado anteriormente, observe la siguiente arquitectura:

**Figura 2**

*Detección vehicular*



Se puede interpretar que:

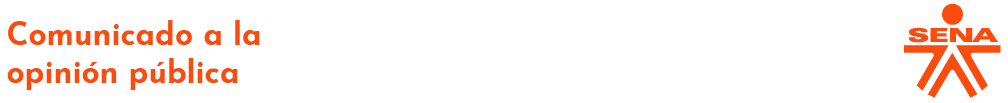
1. El sensor detecta la presencia de un vehículo y envía una señal, el cliente MQTT la procesa y envía el mensaje sobre el tópico autopista/peaje/sensorpresencia.
2. También existe un dispositivo que necesita obtener información del sensor y debe subscribirse a autopista/peaje/sensorpresencia.
3. autopista/peaje/sensorpresencia, carretera y peaje son los niveles del tópico.

**Envíos de mensajes MQTT**

Los clientes MQTT inicialmente se conectan con el protocolo TCP/IP con el *Broker* MQTT, la misión de este *Broker* es tener almacenada la información de los clientes y de los usuarios emisores y consumidores, la conexión entre cliente y *Broker* estará disponible hasta que el dispositivo cliente termine su labor. El protocolo MQTT usa el puerto 1883 para conexión básica no segura y el puerto 8883 cuando usa una capa de seguridad TLS.

Vea, entonces, las fases de los envíos de mensajes y lo que representan:



**Estructura de un mensaje MQTT**

La potencia del protocolo MQTT está en la definición y tipología de los mensajes, en su sencillez radica su potencialidad. Cada mensaje consta de tres partes:



Si desea conocer los diferentes tipos de mensajes y códigos de control que se envían en el protocolo MQTT, a través de la siguiente tabla lo puede hacer:



**Calidad del servicio (QoS)**

MQTT tiene capacidad de gestionar la calidad del servicio o QoS de acuerdo con las necesidades del proyecto, el hecho de que la calidad del servicio se resuelva en la capa de protocolo proporciona ventajas para el desarrollo de aplicaciones de Internet de las cosas y se blinda de fallos de cualquier fuente.

MQTT posee tres niveles QoS, pero ¿cuáles son? Véalas:



* 1. **Seguridad en MQTT**

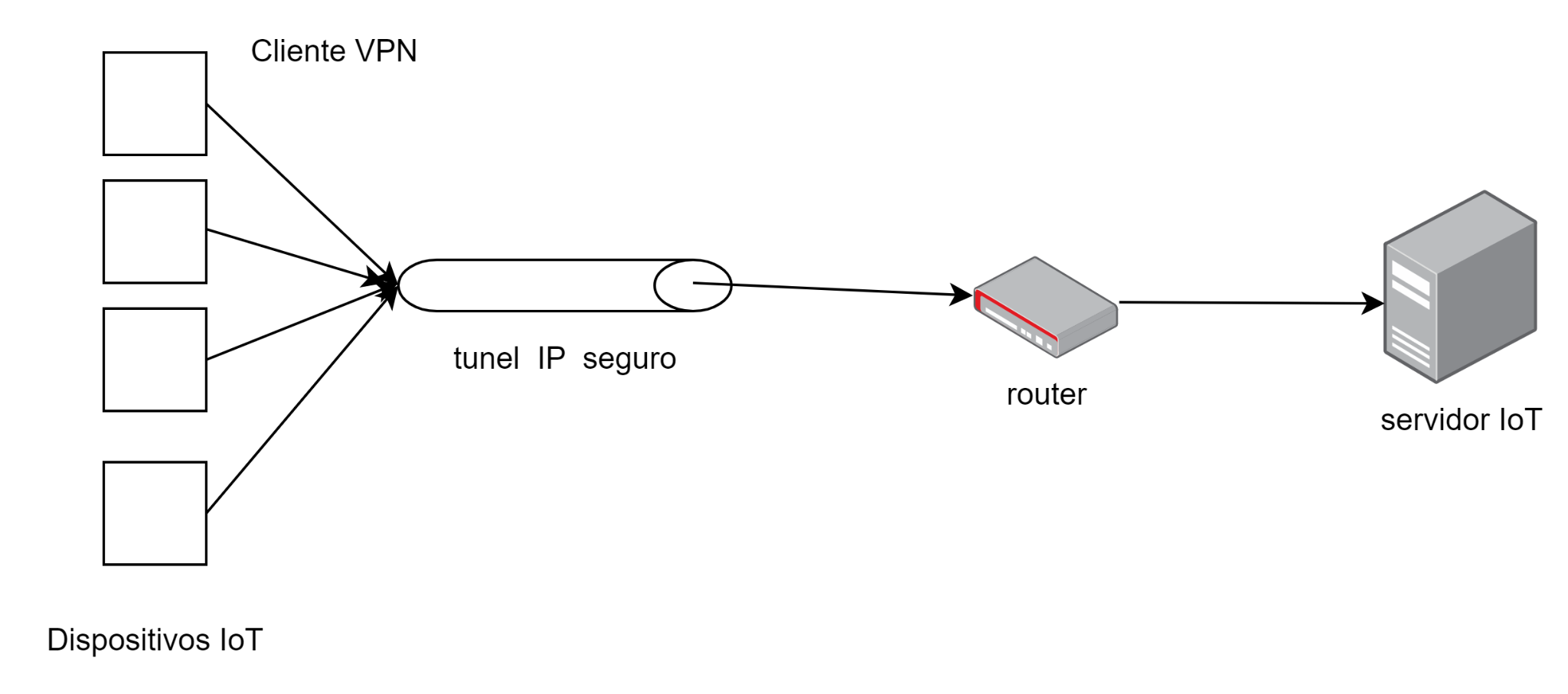
Cuando se habla de ciberseguridad se hace referencia a asegurar que la comunicación entre clientes solo se realice entre ellos y nadie más que esté autorizado, es importante que cada vez que se evalúa un protocolo IoT se revisen sus propiedades y características en materia de seguridad.

En el caso de MQTT, no cuenta con una propiedad de seguridad específica, por tanto, es conveniente implementar seguridad adicional en la arquitectura, lo más común es usar el protocolo de transporte como es TLS / SSL (Transport Layer Security / Secure Sockets Layer) o capa de seguridad de transporte y capa de *socket* seguro. Este protocolo hace que la información se vaya por un canal encriptado y seguro ante posibles ataques como *“the man in the middle*”.

Una forma alterna en la capa de red es implementar una red privada virtual (VPN) entre el *Broker* y los dispositivos IoT, esto hace un túnel seguro entre el dispositivo y el servidor principal, ver figura.

**Figura 3**

*Seguridad MQTT*



Es algo complejo de implementar en aplicaciones IoT, pues hablar de dispositivos IoT es difícil porque son muy pocos los que ofrecen cliente VPN.

Para garantizar la seguridad es necesario apegarse a tres niveles de seguridad que ha definido IBM y que puede de alguna forma constatar revisando el estándar del protocolo, así se tiene:



Se puede identificar un dispositivo a través de los siguientes atributos:



Hasta aquí, identificando cliente ID y usuario más contraseña, en el *payload* se tienen problemas de seguridad, puesto que se consigue establecer una conexión en la que se transmite la información en texto plano y cualquier persona que conozca la trama del protocolo podrá acceder a la información, por tanto, se requiere un transporte encriptado y usar protocolos TLS /SSL con puertos 8883, por defecto sin encriptación el puerto es 1883.

**MQTT + TLS /SSL:** son los acrónimos para Seguridad capa de transporte y Capa de puertos seguros, ambos son protocolos de criptografía, basados en encriptación asimétrica, que proporciona comunicación segura entre los dispositivos conectados a un servidor.

La encriptación asimétrica se basa en la codificación de la información basada en dos claves:



Se requiere el par de claves o llaves para desencriptar los mensajes transportados. Ahora bien, para saber si la llave pertenece a un dispositivo, la respuesta radica en los siguientes certificados públicos:



**Vulnerabilidades y vectores de ataque**

El protocolo MQTT puede ser atacado con ataques mediante MQTT malaria que se basa en la simulación de varios clientes llamados mosquitos que publican mensajes a grandes velocidades, ataques de denegación de servicio, botones a través de MQTT, *man in the middle*, ataques de fuerza, los cuales fueron descritos anteriormente.

Entre las recomendaciones está el decir que deben realizarse actualizaciones y parches, autenticación, control de accesos y administración, evitar contraseñas por defecto, uso de protocolos seguros TLS/SSL y bloquear puertos inactivos.

**2. MOSQUITTO**

Ya conoce cómo funciona el protocolo MQTT, ahora aprenderá a implementarlo y para ello, buscará un servicio o implementación del Broker MQTT. Existen varias opciones para instalar en cualquier sistema operativo tales como Mosquitto, HiveMQ y VernMQ; también se encuentran servicios de Broker MQTT listos para desarrolladores IoT en la nube, por ejemplo, AWS IoT e IBM Bluemix.



El objetivo básicamente es estudiar el servidor mosquitto, sus vulnerabilidades y posibles vectores de ataque.



El protocolo MQTT se puede complementar con una buena base de datos que puede ser InfluxDB, orientada al almacenamiento de series de datos temporales, es de código abierto y diseñado para soportar una gran carga de escrituras y lecturas; debido a esto es una herramienta muy útil para guardar los datos de los dispositivos IoT y se caracteriza por enviar muchos datos en un breve intervalo de tiempo.

**MOSQUITO con TLS y SSL**

Para usar TLS entre el *Broker* y el cliente se deben generar y desplegar un conjunto de claves y certificados y, realizar ajustes de configuración en el archivo de configuración del *Broker* y el almacén de claves cliente/servidor. El protocolo MQTT funciona en la capa de aplicación y se encarga de organizar la información y enviarlos a través de una red TCP, la cual es un protocolo de la capa de transporte, es de aclarar que TCP por defecto no usa una comunicación cifrada, por eso se puede usar TLS si se está enviando información como usuario y contraseña, además de información sensible dependiendo del requerimiento de diseño.

El protocolo MQTT tiene estandarizado para su conexión segura el puerto 8883, reservado exclusivamente para MQTT a través de TLS, el nombre estandarizado en IANA es *secure-mqtt.*

Como se mencionó anteriormente, SSL/TLS son protocolos de encriptación que son usados para asegurar que las comunicaciones web se realicen con integralidad, seguridad y resistencia contra manipulación no autorizada. El *Transport Layer Security* (TLS) y *Secure Sockets Layer* (SSL), proveen un canal de transporte seguro entre un cliente y un servidor. TLS y SSL usan un mecanismo de intercambio de información negociando varios parámetros para crear una conexión segura entre el cliente y un servidor, en el caso de IoT un *Broker* después de que la comunicación inicial se completa se establece una comunicación completamente encriptada entre clientes y *Broker*, y así ningún atacante como *“the man in the middle”* entenderá lo que se transmitió.

**Figura 4**

*Mosquito-TSL/SSL*

Diagrama

Descripción generada automáticamente

PKI usa el protocolo TLS para establecer conexiones seguras entre clientes y servidores sobre TCP, asegurando que la información enviada sea imposible de leer por terceras personas.

1. **Evaluación de seguridad MQTT**

La seguridad es bien importante en cualquier dispositivo que esté disponible en ambientes en producción. En el sector industrial o empresarial protocolos como MQTT realizan una función secundaria de monitoreo en muchos casos, pero es posible que algún usuario conceda acceso a otros servicios esenciales comprometiendo la seguridad de la empresa.

La metodología para evaluar la seguridad de una comunicación MQTT es muy parecida a la de un ataque de penetración clásico y se deben ejecutar las siguientes fases:



Las medidas de seguridad son sencillas de aplicar si se añade a MQTT la capa TLS, con el fin de encriptar la información y proteger el *Broker* de ataques masivos. El protocolo MQTT también se usa en dispositivos de nuestros hogares como la domótica, enchufes inteligentes, cámaras IP, sensores y actuadores, si un *hacker* entra a una red sin seguridad puede comprometer seriamente la red del hogar y extraer información importante como claves bancarias, correos, etc.

1. **SÍNTESIS**

Con el fin de relacionar el contenido de este componente formativo se presenta el siguiente cuadro de síntesis:



1. **ACTIVIDAD DIDÁCTICA**

| Descripción de la actividad didáctica | |
| --- | --- |
| Nombre de la actividad | Seguridad digital |
| Objetivo de la actividad | Reconocer las diferentes formas de ataque en redes IoT y sus posibles soluciones. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexo2\_CF02\_ActividadDidactica |

1. **MATERIAL COMPLEMENTARIO**

| Tema | Referencia APA del Material | Tipo de material  (Video, capítulo de libro, artículo, otro) | Enlace del Recurso o  Archivo del documento o material |
| --- | --- | --- | --- |
| MQTT | Llamas, L. (2019). *¿Qué es MQTT? Su importancia como protocolo IoT*. <https://www.luisllamas.es/que-es-mqtt-su-importancia-como-protocolo-iot/> | Artículo | <https://www.luisllamas.es/que-es-mqtt-su-importancia-como-protocolo-iot/> |
| MQTT | Crespo, E. (2020). *Aprendiendo Arduino.* <https://aprendiendoarduino.wordpress.com/2018/11/19/mqtt/> | Blog | <https://aprendiendoarduino.wordpress.com/2018/11/19/mqtt/> |
| Seguridad en MQTT | Server World. (2020). *FTP: Vsftpd Over SSL/TLS*. <https://www.hivemq.com/hivemq/mqtt-broker/> | Artículo | <https://www.hivemq.com/hivemq/mqtt-broker/> |
| Seguridad en MQTT | Server World. (2020). *Apache2: Configure SSL/TLS*. <https://www.server-world.info/en/note?os=Ubuntu_20.04&p=httpd&f=3> | Artículo | <https://www.server-world.info/en/note?os=Ubuntu_20.04&p=httpd&f=3> |
| Seguridad en MQTT | Server World. (2020). *OpenSSH: Password Authentication*. <https://www.server-world.info/en/note?os=Ubuntu_20.04&p=ssh&f=1> | Artículo | <https://www.server-world.info/en/note?os=Ubuntu_20.04&p=ssh&f=1> |
| MOSQUITTO | Mosquito.org. (2020). *Documentación sobre mosquitto.* <https://mosquitto.org/documentation/> | Sitio web | <https://mosquitto.org/documentation/> |
| Evaluación de seguridad | HiveMQ Team. (2015*). TLS/SSL - MQTT Security fundamentals.* <https://www.hivemq.com/blog/mqtt-security-fundamentals-tls-ssl/> | Artículo | <https://www.hivemq.com/blog/mqtt-security-fundamentals-tls-ssl/> |

1. **GLOSARIO**

| TÉRMINO | SIGNIFICADO |
| --- | --- |
| CA | Sus siglas aplican para autoridad certificadora, emite certificados digitales (claves públicas firmadas de forma electrónica) de alta confianza. |
| IoT | Red de objetos físicos que pueden llevar sensores, *software* y varias tecnologías, con el fin de conectarse y compartir información con otros dispositivos y sistemas a través de Internet. |
| *Malware* | Programa dañino que se instala en dispositivos y que puede generar daños o pérdida de información. |
| MQTT | Protocolo de transporte de mensajería publicación - suscripción de cliente - servidor, liviano, abierto y simple. |
| Riesgo | Es la probabilidad de que una amenaza se materialice, generando alguna consecuencia negativa. |
| SSL | Se refiere a Secure Sockets Layer, asegura la comunicación entre servidor y cliente mediante el cifrado, haciendo que los mensajes no puedan ser intervenidos. |
| TLS | Se refiere a Transport Layer Security, protocolo de cifrado y comunicación, reemplazará al SSL usando un solo puerto para la conexión segura como para la no protegida. |

1. **REFERENCIAS BIBLIOGRÁFICAS**

Almagro, L. (2019). *Ciberseguridad marco NIST. Un abordaje integral de la ciberseguridad*.

AUDEA. (2020). *Fuga de información ¿Qué es y cómo se puede prevenir?* <https://www.audea.com/fuga-de-informacion-que-es-y-como-se-puede-prevenir/>

Castro, M. (2016). *Internet de las cosas. Privacidad y seguridad*. Universidad de Jaén. Departamento de Informática.

IBM Cloud Education. (2021). *Redes*. <https://www.ibm.com/co-es/cloud/learn/networking-a-complete-guide#toc-trminos-y--ZhqcZz4r>

INCIBE. (2017). *Control de acceso, políticas de seguridad para la pyme*. INCIBE. <https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/control-de-acceso.pdf>

INCIBE. (2020). *¿Qué son y para qué sirven los SIEM, IDS e IPS?* INCIBE. <https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips>

Instituto Nacional de Seguridad. (2020). *Seguridad en la instalación y uso de dispositivos IoT: Una guía de aproximación para el empresario*. INCIBE.

ISO. (2018). *ISO 31000:2018(es). Gestión del riesgo — Directrices*.<https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es>

ISO. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. <https://www.iso.org/standard/54534.html>

ISO / IEC JTC 1 / SC 27. (2018). *Seguridad de la información, ciberseguridad y protección de la privacidad*. *ISO / IEC 27005: 2018*. <https://www.iso.org/standard/75281.html>

ISO / IEC JTC 1 / SC 27. (2013). *Seguridad de la información, ciberseguridad y protección de la privacidad*. ISO / IEC 27001: 2013. <https://www.iso.org/standard/54534.html>

ISO / IEC JTC 1 / SC 27. (2013). *Seguridad de la información, ciberseguridad y protección de la privacidad*. ISO / IEC 27002: 2013. <https://www.iso.org/standard/54533.html>

Oracle Corporation and/or its affiliates. (2010). *Modelo de referencia OSI*.<https://docs.oracle.com/cd/E19957-01/820-2981/ipov-8/index.html>

Portas, L. (2021). *Evaluación de la seguridad de sistemas IoT basados en MQTT*. Universidade da Coruña. Facultad de Informática.

1. **CONTROL DEL DOCUMENTO**

|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| --- | --- | --- | --- | --- |
| Autor (es) | Héctor Henry Jurado Soto | Experto temático | Regional Cauca – Centro de Teleinformática y Producción Industrial | Marzo de 2022 |
| Caterine Bedoya Mejía | Diseñadora instruccional | Regional Distrito Capital – Centro de Gestión Industrial | Marzo de 2022 |
| Andrés Felipe Velandia Espitia | Asesor metodológico | Regional Distrito Capital – Centro de Diseño y Metrología | Marzo de 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo desarrollo curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura | Marzo de 2022 |
|  | Julia Isabel Roberto | Correctora de estilo | Regional Distrito Capital – Centro de Diseño y Metrología | Marzo de 2022 |

1. **CONTROL DE CAMBIOS**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

|  | Nombre | Cargo | Dependencia | Fecha | Razón del Cambio |
| --- | --- | --- | --- | --- | --- |
| Autor (es) |  |  |  |  |  |