ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

# “PLAN DE DISEÑO DE CIBERSEGURIDAD A EQUIPOS IOT BASADOS EN CONTROL DE ACCESO DE INGRESO VEHICULAR EN LAS URBANIZACIONES DE LA CIUDAD DE GUAYAQUIL.”

**TRABAJO DE TITULACIÓN**

Previo a la obtención del título de:

**MAESTRÍA EN SEGURIDAD INFORMÁTICA**

**APLICADA**

Presentado por:

**ING ELOY EFREN ALVARADO CABRERA**

**ING XIMENA STEFANIA CHICA BLACIO**

GUAYAQUIL – ECUADOR

2024

# AGRADECIMIENTO

Quiero expresar mi agradecimiento a Dios porque me permitió llegar hasta este momento de mi vida y lograr una meta más, a mi mamá que es mi pilar fundamental, a mi papá porque gracias a él pude lograr muchas metas en mi vida, a mis hermanas que son ese apoyo incondicional en todas circunstancias.

**Ximena Stefania Chica Blacio**

# AGRADECIMIENTO

Por medio de estas líneas, quiero expresar mi más profundo y sincero agradecimiento a mi familia, cuya presencia constante y apoyo inquebrantable han sido la luz guía en cada paso de este arduo camino. Su amor incondicional, paciencia infinita y fé en mis capacidades me han brindado la fortaleza necesaria para enfrentar cada desafío y persistir en la búsqueda de mis sueños. A ustedes, que han compartido conmigo noches de desvelo y momentos de incertidumbre, les debo no solo el éxito de esta tesis, sino también el crecimiento personal y profesional que me ha permitido llegar hasta aquí.

**Eloy Efren Alvarado Cabrera**

# DEDICATORIA

Me gustaría dedicar esta Tesis a mi familia, mi esposo que es la persona que me apoya en cada una de las metas que me propongo, el que me ánima a no desmayar en el intento, quien ha entendido y sacrificado todo este tiempo que he tenido que dedicarme para lograr este objetivo. A mis padres Isabel y Edilberto, por su apoyo incondicional en todo momento en cada una de las cosas que me propongo y por todos los valores que me han inculcado y sembrado en mi para hacer una mujer de bien.

**Ximena Stefania Chica Blacio**

# DEDICATORIA

A mi querida familia, por su inquebrantable apoyo y constante aliento en cada paso de este camino. Gracias por creer en mí y por ser mi mayor fuente de motivación. A la empresa Telconet, por brindarme la oportunidad de crecer profesionalmente, permitiéndome enriquecer mis conocimientos y habilidades en un entorno tan dinámico y retador. Este logro es tanto suyo como mío, y lo dedico a todos ustedes con profunda gratitud.

**Eloy Efren Alvarado Cabrera**

# TRIBUNAL DE GRADUACCIÓN

Firmado electrónicamente por:
LENIN EDUARDO
FREIRE COBO

**Mgs. Lenin Eduardo Freire Cobo**

**TUTOR**

Firmado electrónicamente por:
JUAN CARLOS GARCIA
PLUA

**Mgs. Juan C. García**

**REVISOR**

# DECLARACIÓN EXPRESA

La responsabilidad del contenido de esta Tesis de Grado nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral.

Firmado electrónicamente por:
**ELOY EFREN ALVARADO CABRERA**

ING. ELOY EFREN ALVARADO CABRERA

Firmado electrónicamente por:
**XIMENA STEFANIA CHICA BLACIO**

ING. XIMENA STEFANIA CHICA BLACIO

# RESUMEN

Hoy en día debido a tanta inseguridad que posee el país las empresas de seguridad ofrecen servicios de control de acceso de ingreso vehicular a las garitas mediante equipos IOT como cámaras de seguridad, intercomunicador, barreras de protección para el paso vehicular y el software de registro en el que se detalla el ingreso y salida de garita.

Estos dispositivos IOT debido a su conectividad constante, son vulnerables a ataques cibernéticos que puedan comprometer la seguridad, la falta de medidas adecuadas de ciberseguridad en esos sistemas podría dar lugar a consecuencias graves, como accesos no autorizados, robo de datos, interrupciones en el funcionamiento de los sistemas y la exposición a ataques más amplios en la red.

El plan de diseño de ciberseguridad para equipos IoT en sistemas de control de acceso vehicular en las urbanizaciones de Guayaquil busca asegurar la integridad, confidencialidad y disponibilidad de los datos y operaciones, proporcionando una protección robusta contra amenazas cibernéticas. El plan de diseño exitoso no solo fortalecerá la seguridad de las urbanizaciones, sino que también mejorará la confianza de los residentes en la tecnología utilizada para gestionar el acceso vehicular.

# ÍNDICE GENERAL

# ABREVIATURAS

| | |
|---|---|
| CCTV | Circuito cerrado de Televisión |
| ASIC | Application Specific Integrated Circuit |
| HTTP | Hypertext Transfer Protocol |
| ITU | Unión Internacional de Telecomunicaciones |
| TIC | Tecnologías de la Información y Comunicación |
| OWASP | Open Web Application Security Project |
| DVR | Digital Video Record |
| RFID | Radio Frequency Identification |
| SBC | Session Border Controller |
| FTTH | Fiber To The Home |
| POTS | Plain Old Telephone Service |
| SOHO | Small Office/Home Office |
| ONT | Optical Network Terminal |
| VOIP | Voice Over Internet Protocol |
| QR | Quick Response Cod |

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# INTRODUCCIÓN

En la actualidad la era digital, la conectividad y la automatización están transformando la forma en que se interactúa una amplia variedad de tecnologías, dispositivos y aplicaciones con el mundo que nos rodea a través de internet se denomina IOT

La evolución de dispositivos IOT ha experimentado un rápido avance, planteando importantes preocupaciones relacionadas con la seguridad de los datos y la infraestructura. Estos equipos, al estar conectados a la red, se vuelven susceptibles a amenazas cibernéticas que podrían comprometer la privacidad y la integridad de los sistemas.

Las empresas que ofrecen servicios de control de acceso vehicular mediante estos dispositivos IOT no son la excepción, estos poseen información muy importante de permisos para residentes o visitantes en base a la tecnología implementada. Por lo tanto, con la realización de este trabajo de titulación se busca desarrollar un Plan de Diseño de Ciberseguridad sólido y efectivo que garantice la protección de estos equipos.

Este plan se enfocará en identificar, prevenir y mitigar posibles amenazas cibernéticas que puedan afectar los equipos IOT utilizados en el control de

acceso vehicular en las urbanizaciones de Guayaquil. Nuestra principal misión es salvaguardar la integridad de estos sistemas, garantizar la continuidad de los servicios y proteger la información sensible de los usuarios. Para lograrlo, se requerirá una estrategia integral que abarque desde la evaluación de riesgos hasta la implementación de medidas de seguridad robustas.

Para enfrentar los desafíos de la ciberseguridad en el ámbito de control de acceso vehicular con Equipos IOT, se necesitará en este proyecto abordar aspectos críticos de la ciberseguridad para poder proponer soluciones y establecer las mejores prácticas que permitan garantizar la protección de estos sistemas y adicional brindar la tranquilidad de los habitantes de las urbanizaciones de la ciudad.

Este Plan de Diseño de Ciberseguridad servirá como una guía esencial para garantizar la protección de los sistemas de control de acceso vehicular basados en Equipos IOT en Guayaquil que a su vez contribuirá en mantener la seguridad y la calidad de vida de los residentes en nuestras urbanizaciones.

# CAPITULO I.

# GENERALIDADES

## 1.1. Antecedentes

La empresa que provee servicios de seguridad física privada ubicada en la ciudad de Guayaquil cuenta con alrededor de 10 años de trayectoria sus inicios empezaron en el 2010 con exmilitares de la Legión extranjera francesa, quienes ingresaron con tecnología de calidad e innovadora que brindan soluciones integrales de sistemas de CCTV, control de acceso, detección de incendio mediante un sistema de desarrollo propio.

El sistema aparte de ser un gestor de configuraciones para cada dispositivo también tiene un módulo de monitoreo donde se tiene recepción de señal de alerta y visibilidad de las operaciones que se realizan de cada punto en tiempo real. Además, cuentan con profesionales que diseñan soluciones basándose en la situación del problema planteado por el cliente con el objetivo de brindar el servicio de seguridad que se adapte a sus necesidades.

La tecnología en la organización es parte importante y esencial dependiendo de la forma en que se utilice ya que se debe tener en cuenta los riesgos que se pueden dar al manipular información y esta no estar protegida, por este motivo es primordial que se tome medidas necesarias para actuar de manera adecuada ante cualquier incidencia de seguridad que se pueda presentar en la organización.

En la actualidad la empresa de seguridad cuenta con equipos IOT para brindar protección y seguridad al momento del ingreso de los vehículos a los residentes de las urbanizaciones de guayaquil, mediante el sistema de control de acceso se valida la información correcta para permitir o restringir el ingreso.

Debido al crecimiento y demanda de dispositivos IOT conectados a la nube, la empresa de seguridad ha tenido la necesidad de fortalecer su diseño actual basado en tecnología de seguridad informática que permita realizar una mejor

gestión en términos de ciberseguridad para proteger los equipos IOT.

La empresa de seguridad de la ciudad de Guayaquil no cuenta con la debida protección de la información que se manipula en sus equipos IOT instalados en las urbanizaciones los cuales ocasionan vulnerabilidades y amenaza al no contar con un dispositivo que brinda seguridad como firewalls que permitan llevar el control y permisos adecuados con el objetivo de disminuir las brechas de seguridad informática existentes.

### 1.2. Descripción del Problema

Una empresa de seguridad de guayaquil que ofrece servicios de control de acceso de ingreso vehicular a las garitas mediante equipos IOT como cámaras de seguridad, intercomunicador, barreras de protección para el paso vehicular y el software de registro en el que se detalla el ingreso y salida de garita.

Estos dispositivos IOT debido a su conectividad constante, son vulnerables a ataques cibernéticos que puedan comprometer la seguridad de las urbanizaciones, los residentes y sus propiedades. La falta de medidas adecuadas de ciberseguridad en esos sistemas podría dar lugar a consecuencias graves, como accesos no autorizados, robo de datos, interrupciones en el funcionamiento de los sistemas y la exposición a ataques más amplios en la red.

La falta de una infraestructura de ciberseguridad sólida en la mayoría de las urbanizaciones de Guayaquil plantea un riesgo latente para la privacidad y seguridad de los residentes, así como para la integridad de los sistemas de control de acceso. Los dispositivos IOT, si no se protegen adecuadamente, pueden convertirse en puntos de entrada para ataques dirigidos o botnets, lo que puede tener graves consecuencias para la comunidad.

Los beneficios de resolver este problema es reducir los riesgos de ciberseguridad, protección de la inversión en los dispositivos IOT y mejorar el nivel confianza de los residentes, pero para poderlo lograr es necesario evaluar e identificar los posibles riesgos potenciales asociados con la seguridad y la privacidad.

La tecnología IOT también llamado como el Internet de las cosas son dispositivos informáticos no estándar (objetos, elementos cotidianos, dispositivos, sensores o actuadores) conectados a una red cableada o inalámbrica, que tienen la capacidad de transmitir y/o recibir datos, recibir instrucciones e incluso actuar basados en los datos que recogen. [1]

Esta propuesta es viable de ser ejecutada debido a que existe disponibilidad de tecnología para implementar medidas de ciberseguridad y es compatible con los dispositivos IOT existentes en las urbanizaciones, sin dejar a un lado que se tiene el conocimiento técnico y las habilidades necesarias para implementar medidas de seguridad de manera efectiva.

## 1.3. Solución Propuesta

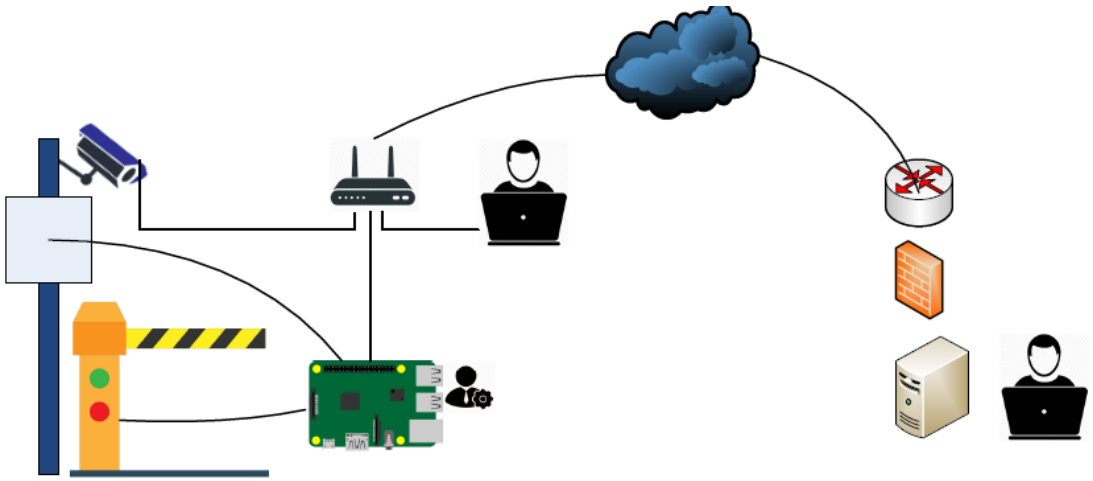


***FIGURA 1.1: ESQUEMA ACTUAL FÍSICO IMPLEMENTADO EN URBANIZACIONES***

***FUENTE: AUTOR***

En este gráfico se puede observar el diseño actual de la red donde se visualiza dispositivos conectados en una placa de control de acceso, que permite autorizar o denegar el ingreso del vehículo de los clientes de manera automática mediante la configuración realizada en el sistema.

Además, las garitas poseen un modem de internet, el cual tiene conectado una cámara de video vigilancia, la placa de control de acceso y la PC que administrará el software de la placa que a su vez se conecta mediante el internet para poder llegar al servidor que está en matriz que recolecta la información de los logs y de los perfiles configurados localmente. Cabe indicar

que la empresa de seguridad posee con 50 garitas con el mismo modelo como se observa en el grafico anterior, Incluyendo sus propias garitas locales.

Se propone a una empresa de seguridad de la ciudad de Guayaquil diseñar un modelo de solución usando las herramientas tecnológicas FortiNAC y Fortigate que se explicara de manera breve los conceptos y características a continuación:

FortiNAC es una herramienta perteneciente al ecosistema de dispositivos Fortinet que da una solución de confianza cero cuya finalidad es proteger y supervisar los activos digitales que se encuentren conectados a la red corporativa de la empresa. Esta herramienta proporciona visibilidad, control y respuesta automatizada para todos los dispositivos que se encuentran conectados a la red y ofrece protección contra amenazas de IOT.

Las principales características que definen a FortiNAC son las siguientes.

- Permite controlar y gestionar el acceso de los usuarios y dispositivos a la red.
- Puede autenticar y autorizar a los usuarios antes de permitirles acceder a los recursos de red. Esto ayuda a garantizar que solo los dispositivos y usuarios autorizados puedan acceder a la red y los recursos correspondientes.

- Tiene la capacidad de detectar y descubrir dispositivos conectados a la red, aquellos que son nuevos o no autorizados. Proporciona información detallada sobre los dispositivos, como direcciones IP, fabricante, tipo de dispositivo, sistema operativo, historial de conexión, etc. Esto permite una mejor visibilidad y control sobre los dispositivos en la red.

El equipo FortiNAC ayuda a garantizar el cumplimiento de las políticas de seguridad de la red. Pueden aplicar políticas de seguridad predefinidas o personalizadas para diferentes tipos de dispositivos y usuarios. Esto incluye la verificación de parches, la configuración del sistema operativo, la presencia de software antivirus, el cumplimiento de políticas de contraseña, entre otros criterios.

También desempeña un papel en la seguridad de la red al proporcionar protección contra amenazas. Puede detectar y responder a amenazas en tiempo real, como dispositivos comprometidos, programa maligno o actividades sospechosas en la red. Además, puede integrarse con otras soluciones de seguridad de Fortinet para una defensa más completa. [2]

El equipo fortigate es una poderosa combinación de software y hardware basada en el uso de “Circuitos Integrados de Aplicación Específica”, conocidos

por sus siglas en inglés como ASIC, a través de la cual es capaz de ofrecer el procesamiento y análisis del contenido del tráfico de la red sin que ello suponga ningún impacto en el rendimiento de las comunicaciones. La tecnología incluye el Procesador FortiASICTM y el Sistema Operativo FortiOSTM los cuales forman el núcleo de los equipos FortiGate y son la base del alto rendimiento ofrecido por los equipos.

La línea de soluciones de seguridad de amenazas a series FortiGate ofrece a las empresas un sencillo despliegue, al permitir su instalación sin problemas en redes de última generación.[3]

De acuerdo con las soluciones presentadas como FortiNAC y Fortigate se presenta a continuación el esquema de la solución que se diseñó para mejorar la red actual que posee el cliente con la finalidad de lograr brindar seguridad a los dispositivos IOT.

## 1.4. Objetivos

### 1.4.1. Objetivo General

- ✓ Diseñar un modelo de solución integral para la ciberseguridad a equipos de IOT usando tecnologías inmersas en la actualidad que brindaran

seguridad al sistema de control de acceso para el ingreso vehicular de los residentes de las urbanizaciones de la ciudad de Guayaquil.

### 1.4.2. Objetivos Específicos

- ✓ Identificar las vulnerabilidades comunes en los sistemas de control de acceso IOT en urbanizaciones de Guayaquil.
- ✓ Evaluar la infraestructura de control de acceso vehicular IOT en urbanizaciones y realizar un análisis de riesgos para identificar las posibles amenazas y vulnerabilidades que podrían afectar a estos sistemas.
- ✓ Diseñar una solución de seguridad que contengan: firewalls, sistemas de detección de intrusiones y actualizaciones de firmware seguras, para proteger los dispositivos IOT.

## 1.5. Metodología

El alcance de trabajo de titulación es principalmente descriptivo puesto que los dispositivos del control de acceso vehicular necesitan brindar seguridad a los residentes de las urbanizaciones para lo cual es necesario realizar un análisis de diversos aspectos claves y demostrar las vulnerabilidades existentes en estos dispositivos IOT.

Para garantizar la seguridad de los dispositivos y sistemas IOT basándonos primero en un testing de amenazas o vulnerabilidades, los cuales nos ayudarán a proponer medidas de seguridad como por ejemplo actualización de firmware, contraseñas fuertes, capacitación a usuarios, entre otras.

En base al análisis o testing el cual ayudará a saber que problemas de seguridad existen en la infraestructura actual, se generará el plan a seguir del diseño que conllevará medidas de seguridad.

El proyecto cuenta con un muestreo no probabilístico por convivencia ya que se va a escoger un área determinada de la empresa para realizar el estudio, mediante la herramienta de Google la cual ayuda a elaborar formularios de preguntas con respuestas para obtener la información necesaria.

El tipo de muestra que se va a usar en el proyecto será por convivencia ya que se tiene un área identificada en la que se va a desarrollar y recopilar la información necesaria para la evaluación. El departamento de LAN de la organización será el objeto presente para el estudio y este cuenta con 30 profesionales de los cuales solo se va a seleccionar 15 profesionales para el estudio y análisis previo a una encuesta.

# CAPITULO II.

# MARCO TEÓRICO

En este capítulo se describe los conceptos teóricos necesarios para el desarrollo del presente proyecto como conceptos básicos que se debe conocer acerca del Internet de las cosas, ventajas y desventajas de IOT, equipos que se usan para la seguridad en urbanizaciones de guayaquil.

## 2.1. IOT

### 2.1.1. Origen y definición de IOT

En 1926 Nikola Tesla preparo las bases de las comunicaciones, después en el año 1990 Berners-Lee creo HTTP estas son las bases donde posteriormente en el año 1999 Kevin Ashton fue la persona que utilizo por primera vez la expresión de IOT en una conferencia, desde entonces comenzó a ser normal referirse al sistema de conexión de cosas a internet. [4]

Kevin Asthon Trabajaba en Procter & Gamble (P&G) tenía 28 años en ese momento estaba en problemas porque los productos que manejaba no estaban disponibles en las tiendas, se dio cuenta de cuál era el problema de información, por lo tanto, se le ocurrió una idea de colocar sensores a los productos para saber cuándo dejaran de estar en stock, el trato de convencer a P&G para poder implementar la idea que tenía.

Asthon asegura que “entendió que la palabra “internet” podría atraer la atención de esta compañía porque en 1998 los gerentes pensaban que la red era lo más importante y buscaban nuevos proyectos. Después la palabra “cosas” se comenzó a usar por la idea de empotrar las computadoras en las mesas y cada vez los equipos llegaban más económicos y pequeños, la idea era confusa, pero era lo suficiente para que comenzara a investigar sobre IOT. [4]

En 2005 ITU (International Telecommunications Unión) realizo el primer estudio sobre el tema, ellos afirmaron lo siguiente “Una nueva dimensión se ha agregado al mundo de las tecnologías de información y la comunicación (TIC): a cualquier hora, en cualquier lugar, se tiene conectividad para cualquier cosa. Las conexiones se multiplican y crearán una nueva red dinámica de redes con redes, Internet de las Cosas”.

En el año 2008 un grupo de empresas crearon una alianza para promover el uso de protocolos de internet de objetos inteligentes comenzaron a trabajar en ello para que se hiciera realidad esta idea. La Alliance IPSO tiene empresas involucradas actualmente como Google, Bosch, Motorola, Toshiba, etc... Primero comenzaron con el proyecto de desarrollo del protocolo IPV6.En el año 2009 comenzó a ser más escuchada esa palabra IOT, en 2011 fue lanzado como tal el protocolo IPV6 y otros fabricantes anunciaron sus proyectos, después se inició la adopción de estándares para IOT a escala global. [4]

En actualidad la IOT continúa expandiéndose a medida que se integra en una amplia variedad de industrias y aplicaciones, desde la agricultura inteligente y la atención médica hasta la movilidad urbana y la fabricación. Los avances en la inteligencia artificial, el aprendizaje automático y la analítica de datos están impulsando aún más la IOT, permitiendo un mayor análisis y aprovechamiento de los datos generados por los dispositivos.

El Internet de las Cosas (IOT) contribuye a una nueva revolución tecnológica que impacta a la sociedad. IOT es un paradigma que permite componer sistemas a partir de objetos (cosas) únicamente direccionables equipados con comportamientos de identificación, detección o actuación y capacidades de procesamiento que pueden comunicarse y cooperar para alcanzar una meta. [5]

## 2.2. Definición de IOT

La IOT se puede definir como un sistema de dispositivos físicos conectados a través de internet, que pueden recopilar y compartir datos automáticamente sin la necesidad de intervención humana directa. Estos dispositivos pueden variar desde electrodomésticos y sensores industriales hasta vehículos conectados, dispositivos de salud, cámaras de seguridad y mucho más. Los datos recopilados por estos dispositivos pueden ser utilizados para tomar decisiones informadas, mejorar la eficiencia, automatizar procesos y proporcionar una amplia gama de servicios útiles en diversos sectores, como la industria, la salud, la agricultura, el transporte, la energía y el hogar inteligente, entre otros.

El paradigma IOT será considerado en su ámbito de desarrollo como la cuarta revolución industrial, ya que actuará en campos como la industria y automatización, transporte, salud, ciudades inteligentes, casas inteligentes y

actividades de la comunidad. IOT es la interconexión en red de todos los objetos que se encuentran equipados con algún tipo de inteligencia, IOT es una verdadera evolución por su interconectividad dando manejo de la información y servicios inteligentes (Silvestre, 2016) afirma: IOT ofrece grandes oportunidades en diferentes campos, mejorando continuamente la gestión y dando cambio radical en la vida cotidiana ofreciendo nuevas oportunidades en los datos y otros servicios, se puede explorar nuevos modelos de negocio por medio de los dispositivos interconectados. [4]

Con IOT se espera que las cosas sean capaces de interactuar y comunicarse entre ellas por la interconexión basada en estándares de protocolos de comunicación, IOT permitirá comunicarse desde cualquier lugar del mundo a través de diferentes tecnologías de información y comunicaciones con el objetivo de permitir el control y monitorización en tiempo real y de manera automática.[4]

## 2.3. Ventajas y desventajas de IOT

### 2.3.1 Ventajas:

- ✓ Detección y defensa de la infraestructura de red de IOT de ataques DDoS y detección de dispositivos maliciosos de IOT.[6]

- ✓ Configuración, instalación y acuerdo de claves para autenticar la comunicación entre los dispositivos y la autoridad de autenticación de IOT y lograr la integridad de los datos de IOT.[6]

### 2.3.2 Desventajas:

- ✓ En la seguridad para dispositivos IOT [6] no existe un diseño único o esquema general sobre la arquitectura de IOT ya que se proponen diferentes arquitecturas de IOT basados en el servicio que ofrece el equipo como en el caso de las cámaras de video vigilancia que se necesita que esté conectado a la nube para recopilar la dato de los videos y tener el respaldo de los mismos o en otros casos en una red tradicional se debe constar con el DVR central que contenga un disco de respaldo pero sin embargo este equipos puede ser robado o roto, las imágenes de vídeo podrían perderse o verse comprometidas; o el vídeo puede sobrescribirse. Además, estos [7] dispositivos suelen estar conectados a Internet; por lo tanto, son potencialmente vulnerables a la infiltración.
- ✓ Se necesita una inversión tecnológica.
- ✓ La complejidad del IOT puede ser una limitante ya que los usuarios pueden tener dificultades para entender y manejar dispositivos complejos.

## 2.4. Funcionamiento de dispositivos de ingreso vehicular

Los dispositivos de ingreso vehicular se utilizan para controlar el acceso de vehículos a áreas privadas o restringidas, como estacionamientos, comunidades cerradas, garajes, instalaciones industriales y más. Estos dispositivos permiten autorizar o denegar la entrada de vehículos de manera automatizada o remota por medio de:

### 2.4.1. Cámara de seguridad

Los dispositivos de ingreso vehicular basados en cámaras se utilizan para capturar, analizar imágenes de vehículos y matrículas. Estos sistemas se utilizan para controlar y gestionar el acceso de vehículos a áreas restringidas, como estacionamientos, garajes, comunidades cerradas, o cualquier lugar que requiera autorización de ingreso. [8]

A continuación, se describen funcionamiento de las cámaras y beneficios que estos poseen cuando se añaden a un desarrollo capaz de analizar reconocimiento de data para que el sistema tome una decisión en base a su algoritmo.

Captura de imágenes:

- ✓ Las cámaras de video están instaladas en ubicaciones estratégicas donde puedan capturar imágenes de los vehículos que se aproximan o intentan ingresar al área restringida.
- ✓ Las cámaras están configuradas para capturar imágenes de alta calidad, lo que permite la identificación de matrículas de vehículos con precisión.

Detección de vehículos:

- ✓ Los sistemas de cámaras pueden incorporar tecnología de detección de vehículos que identifica cuándo un vehículo se encuentra en el área de enfoque de la cámara.
- ✓ Esto suele realizarse mediante algoritmos de detección de movimiento que registran la presencia de un vehículo en el campo de visión de la cámara.

Captura de matrículas:

- ✓ Una vez que se detecta un vehículo, la cámara captura una imagen de su matrícula.
- ✓ Las cámaras de reconocimiento de matrículas utilizan lentes específicos y tecnología de procesamiento de imagen para enfocarse en la matrícula y capturarla de manera clara y legible.

Procesamiento y análisis:

- ✓ Las imágenes de las matrículas capturadas se envían a un sistema de procesamiento y análisis de imágenes.
- ✓ Este sistema utiliza algoritmos de reconocimiento de caracteres (OCR) para convertir la imagen de la matrícula en texto legible y reconocible.

Verificación y autorización:

- ✓ El texto de la matrícula se compara con una base de datos de matrículas autorizadas.
- ✓ Si la matrícula coincide con una matrícula autorizada en la base de datos, el sistema autoriza el acceso del vehículo.

Acceso y registro:

- ✓ Si el sistema verifica que el vehículo está autorizado, se activa la apertura de una barrera, puerta o se permite el acceso de alguna otra manera.
- ✓ El sistema registra la entrada del vehículo en una base de datos, lo que permite llevar un registro de quién entra y sale del área restringida.

Alarmas y notificaciones:

- ✓ En caso de que el sistema detecte una matrícula no autorizada o algún comportamiento inusual, puede generar alarmas o notificaciones para alertar a los operadores de seguridad.

Las cámaras de seguridad ofrecen muchas ventajas como se indica en los párrafos anteriores como complemento al circuito cerrado para el paso vehicular, pero en la empresa que se realizó el levantamiento de información, solo son usadas para grabar y guardarla los videos o imágenes en la central a través del internet

### 2.4.2. Barreras de acceso:

- ✓ Barreras físicas, como brazos o puertas, bloquean el acceso al área.
- ✓ Controladas por un motor eléctrico, hidráulico o neumático que permite que la barrera se abra y se cierre de forma controlada.
- ✓ Se pueden controlar de manera manual a través de un panel de control, con tarjetas de acceso, control remoto, o de forma automática mediante sensores, lectores de tarjetas, u otros dispositivos de entrada.
- ✓ Los sensores de seguridad, como fotocélulas y detectores de presencia, se utilizan para evitar accidentes y garantizar la seguridad de los vehículos y las personas.

### 2.4.3. Lectores de tarjetas o identificación:

- ✓ Los vehículos autorizados tienen una tarjeta de acceso o un dispositivo de identificación, como un tag RFID o una etiqueta con códigos de barras.

- ✓ El lector de tarjetas o el sistema de identificación captura la información de la tarjeta o del dispositivo y verifica si el vehículo está autorizado para el acceso.
- ✓ Si la autorización es válida, se activa la apertura de la barrera o puerta, permitiendo la entrada.

Software de gestión y control:

- ✓ Los dispositivos de ingreso vehicular suelen estar conectados a un software de gestión que administra las autorizaciones, registros de acceso y configuraciones.
- ✓ El software permite a los administradores autorizar o revocar permisos de acceso, realizar un seguimiento de las actividades de entrada y salida, y generar informes sobre el uso del sistema.

# CAPITULO III.

# IDENTIFICACIÓN DE LAS VULNERABILIDADES

## 3.1. Identificación de los activos de información

Este proyecto tiene algunos activos de información que permiten conocer los dispositivos y el software que se usa para el control de acceso a urbanizaciones de la ciudad de guayaquil. A continuación, se describe los equipos:

### 3.1.1. Cámara Hikvision DS-2CD1653G0-IZ2.8-12MM

Esta cámara tiene propiedades importantes que cumplen con la función de análisis profundo cruce de líneas, intrusión, entrada y salida de región.

Posee alarma de excepción de temperatura para prevención de incendios, permite que se vea en la noche y vigile su propiedad con la cámara bala de red para exteriores con visión nocturna. La cámara captura video a resoluciones de hasta 2550 x 1920 y tienen un alcance de 30 metros en visión nocturna.


***FIGURA 3.1: CÁMARA HIKVISION***

***FUENTE: HTTPS://WWW.HIKVISION.COM/ES-LA/PRODUCTS/IP-PRODUCTS/NETWORK-CAMERAS/PRO-SERIES-EASYIP-/DS-2CD2027G2-L-U-/***

### 3.1.2. Raspberry

Es un ordenador mini u ordenador de placa simple conocida por sus siglas Single Board Computer (SBC), que tienen bajo costo su tamaño es como de una tarjeta de crédito.

Se ha convertido en una herramienta de enseñanza de programación y es útil plataforma para el diseño de aficionados y para usos informáticos generales como creación digital, robótica. La evolución que ha tenido ha permitido que mejoren el consumo energético, usa sistema operativo Linux, lenguaje de programación como Scratch y Python, tiene la habilidad de interactuar con el mundo exterior.

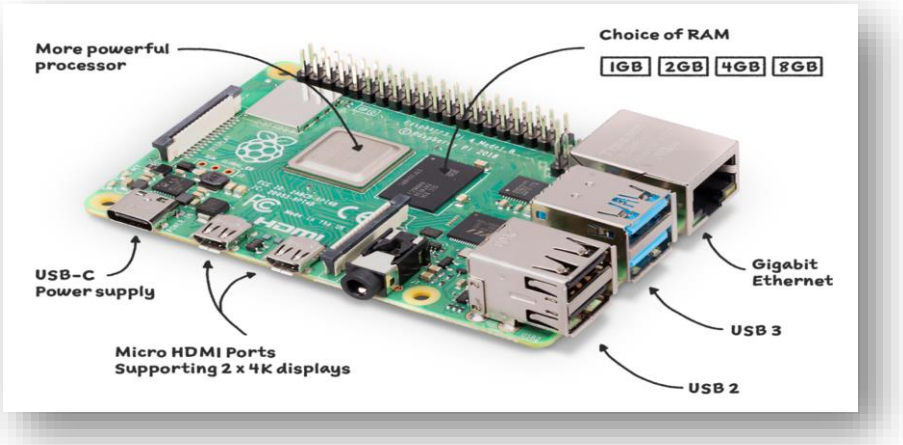



***FIGURA 3.2: TARJETA RASPBERRY***

***FUENTE:HTTPS://WWW.RASPBERRYPI.COM/PRODUCTS/RASPBERRY-PI-4-MODEL-B/***

### *3.1.3. Huawei*

Huawei EG8145V5 es un terminal dual band que funciona en las dos bandas, banda de 5G y 2.4G, en la banda de 5G dispone de WIFI IEEE 802.11 a/n/ac y en la banda 2.4G dispone de IEEE 802.11 b/g/n. Posee antenas externas y es MIMO 2*2 en ambas bandas.

Son dispositivos de usuario en las soluciones FTTH (fibra hasta la vivienda) de Huawei; admiten el acceso a banda ultra ancha para usuarios residenciales o pequeñas empresas (SOHO) que utilizan tecnologías GPON. Los ONT de la serie EchoLife EG poseen puertos POTS y puertos Ethernet de negociación automática FE/GE, lo que permite contar con capacidades de transmisión de alto rendimiento.

***FIGURA 3.3: HUAWEI EG8145V5***

***FUENTE: HTTPS://E.HUAWEI.COM/ES/PRODUCTS/OPTICAL-TERMINAL/ECOLIFE-EG8145V5***

### *3.1.4. Switch Trendnet 8 puertos Gigabit POE*

El switch PoE+ Gigabit de 8 puertos modelo TPE-TG83, permite reducir los costos de equipo y de instalación al suministrar datos y alimentación eléctrica a través de cables ethernet ya existentes. Este switch cuenta con ocho puertos gigabit PoE+ con una potencia PoE total disponible de 65W, permite conectar en red dispositivos PoE como puntos de acceso wireless, cámaras IP, teléfonos VoIP, codificadores de vídeo IP y controles de acceso, entre otros. No tiene ventilador, y tiene una cómoda opción de montaje en pared.


***FIGURA 3.4: SWITCH TRENDNET 8 PUERTOS***

***FUENTE: HTTPS://WWW.TRENDNET.COM/LANGSP/PRODUCTS/POE-SWITCH/8-PORT-GIGABIT-POEPLUS-SWITCH-TPE-TG83***

### *3.1.5. NVR 8CH Capacidad 40mb Bandeja 1hdd*

Nvr 8Ch Capacidad 40Mb Bandeja 1Hdd 8Ch 8Mp Hasta 16 Cámaras Ip Simultaneas H.265+/H2.65/H.264/H2.264+/Hdmi/Vga Salida De Video Hdmi 4K (348X2160) 1Hdds 6Tb Tpc/Ip 10/100/1000 Mbps Incluye Fuente 110Vac.


***FIGURA 3.5: NVR HIKIVISION***

***FUENTE: HTTPS://WWW.HIKVISION.COM/ES-LA/PRODUCTS/IP-PRODUCTS/NETWORK-VIDEO-RECORDERS/PRO-SERIES/DS-7608NI-Q1-8P/***

### *3.1.6. Barra de acceso Zkteco*

Controla el acceso de vehículos no autorizados en zonas restringidas, posee un dispositivo de control de acceso, lector de tarjetas de largo alcance o un sistema de reconocimiento de placas.

Tiene sensor de masa que evita el cierre a destiempo debido a que se bajará automáticamente después de que el vehículo haya accedido, sin dejar de

tomar en cuenta que la barrera se puede manipular manualmente mediante el uso de control remoto. La barrera está equipada con un sensor que detecta algún obstáculo durante el cierre.

***FIGURA 3.6: BARRA DE ACCESO ZKTECO***

***FUENTE: HTTPS://ZKTECOLATINOAMERICA.COM/CATEGORIA-PRODUCTO/ACCESO-VEHICULAR/BARRERA-VEHICULAR/***

## 3.2. Recolección de información

Se requiere recolectar datos para determinar un muestreo del departamento encargado de administrar los enlaces que se encuentran ubicados en distintas urbanizaciones para identificar cuanto conocimiento poseen acerca de la seguridad de los dispositivos de acceso vehicular y el control seguro que estos brindan. A continuación, las preguntas de la encuesta:

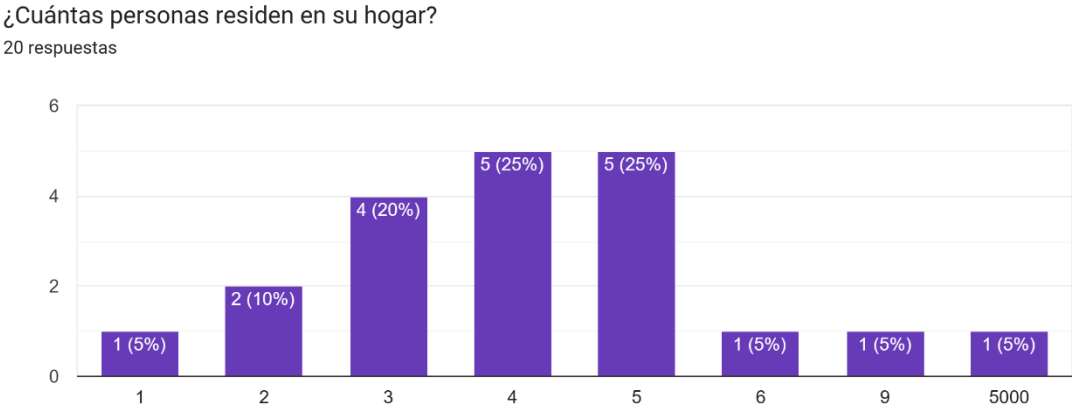



***FIGURA 3.7: DATOS ESTADÍSTICOS PREGUNTA 1***

***FUENTE: AUTOR***

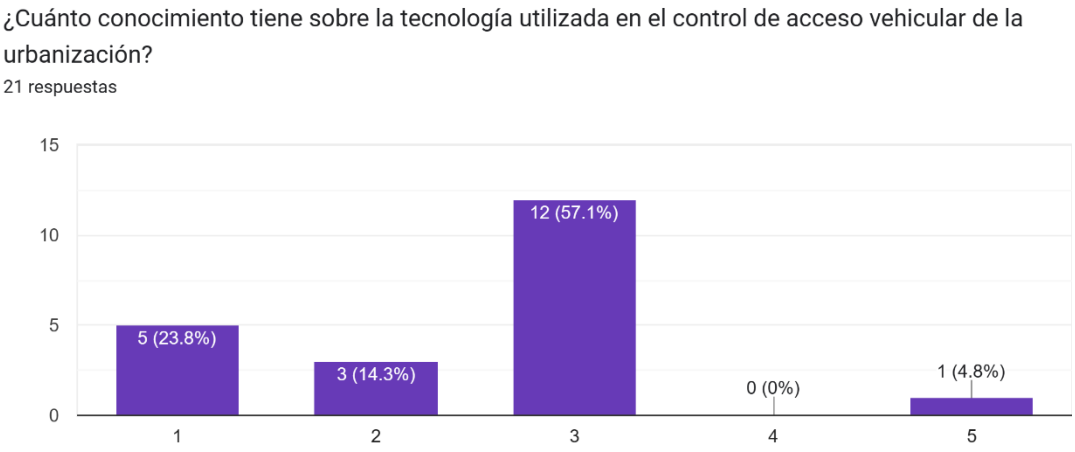



***FIGURA 3.8: DATOS ESTADÍSTICOS PREGUNTA 2***

***FUENTE: AUTOR***

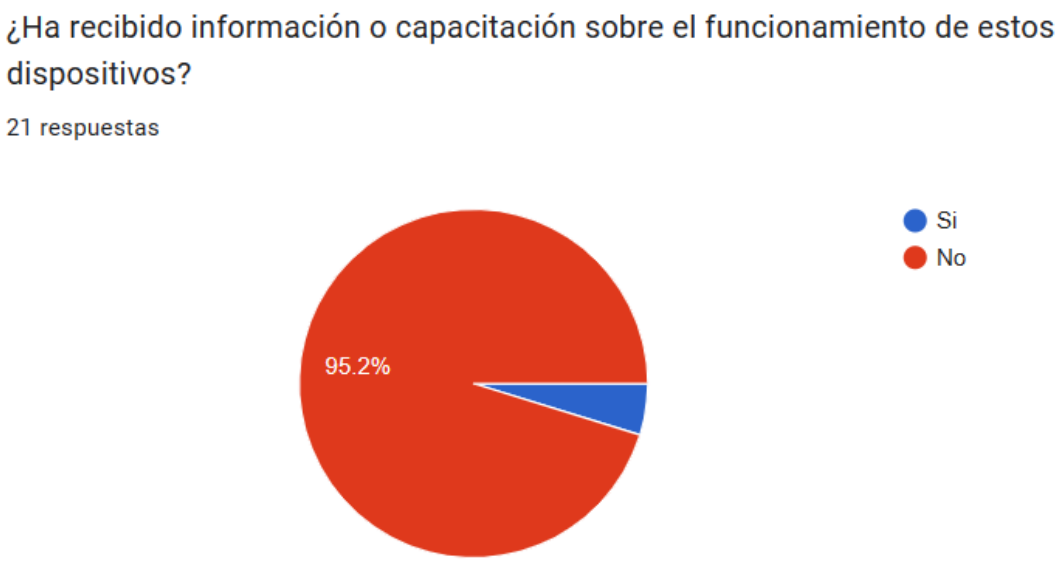



***FIGURA 3.9: DATOS ESTADÍSTICOS PREGUNTA 3***

***FUENTE: AUTOR***

La encuesta revela que solo el 4.8% de las 21 personas encuestadas han recibido información o capacitación sobre el funcionamiento de los dispositivos de control de acceso vehicular en la residencia. Este dato indica una brecha significativa en la conciencia y comprensión de la tecnología de seguridad entre los residentes. La abrumadora mayoría, el 95.2%, no ha recibido ninguna información, lo que sugiere la necesidad de implementar programas educativos para mejorar la comprensión y el uso efectivo de estos sistemas. Este hallazgo destaca la importancia de fortalecer la conciencia y la formación en seguridad informática para garantizar una implementación eficaz de los controles de acceso vehicular.

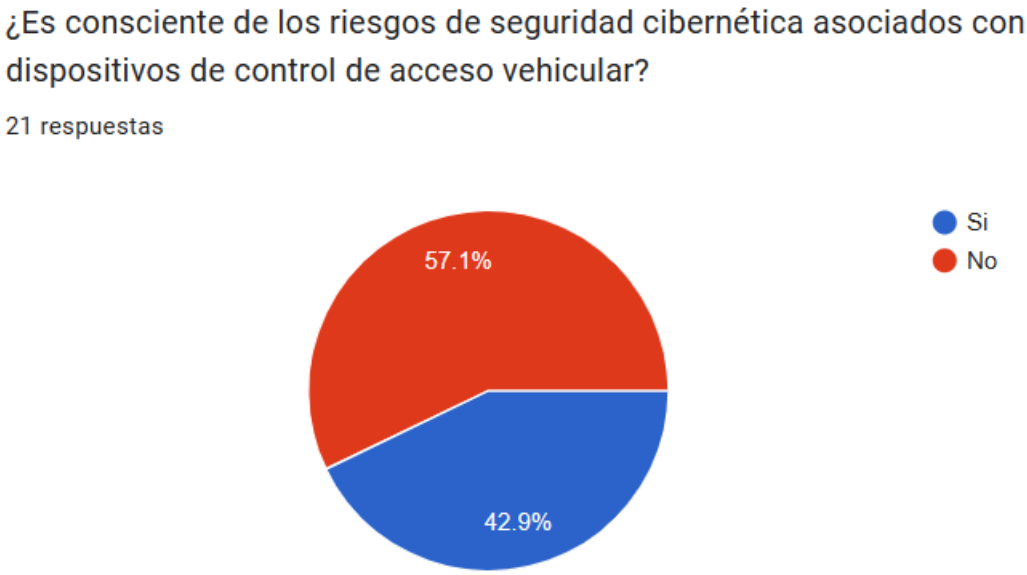



***FIGURA 3.10: DATOS ESTADÍSTICOS PREGUNTA 4***

***FUENTE: AUTOR***

La encuesta revela que el 42.9% de las 21 personas encuestadas son conscientes de los riesgos de seguridad cibernética asociados con los dispositivos de control de acceso vehicular en la residencia. Sin embargo, la mayoría, el 57.1%, no muestra esta conciencia, indicando una brecha significativa en la comprensión de los posibles riesgos digitales. Este resultado destaca la necesidad de aumentar la concienciación sobre las amenazas cibernéticas relacionadas con los sistemas de acceso vehicular, subrayando la importancia de la educación en seguridad informática para garantizar la protección integral de la residencia.

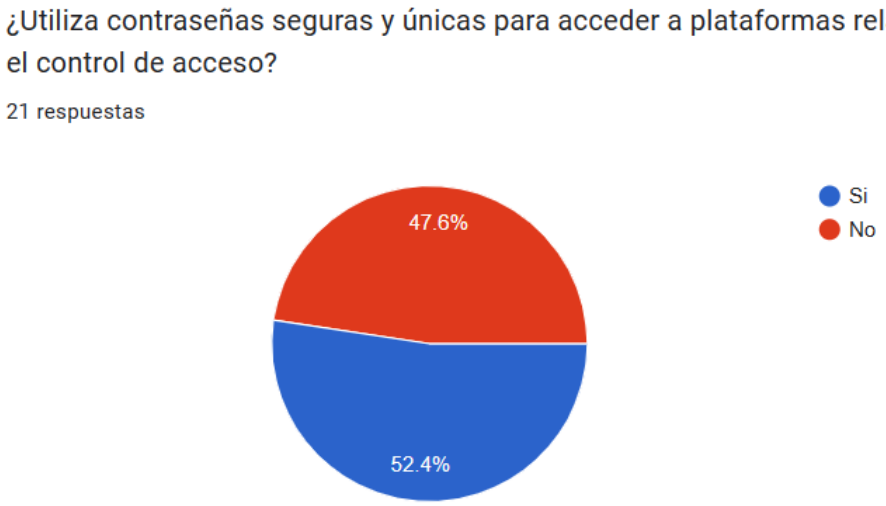



***FIGURA 3.11: DATOS ESTADÍSTICOS PREGUNTA 5***

***FUENTE: AUTOR***

La encuesta indica que el 52.4% de las 21 personas encuestadas utilizan contraseñas seguras y únicas para acceder a plataformas relacionadas con el control de acceso vehicular en la residencia. Sin embargo, el 47.6% no sigue esta práctica, lo que sugiere un riesgo potencial para la seguridad. Este hallazgo destaca la necesidad de fomentar el uso de contraseñas robustas y distintas para garantizar la protección adecuada de los sistemas de acceso vehicular. Se recomienda implementar medidas educativas y de concienciación sobre buenas prácticas de seguridad para fortalecer la postura de protección en la comunidad residencial.


***FIGURA 3.12: DATOS ESTADÍSTICOS PREGUNTA 6***

***FUENTE: AUTOR***

La encuesta revela que solo el 28.6% de las 21 personas encuestadas cambian regularmente sus contraseñas en plataformas relacionadas con el control de acceso vehicular en la residencia. Sin embargo, una preocupante mayoría del 71.4% no sigue esta práctica, lo que puede aumentar el riesgo de vulnerabilidades de seguridad. Este hallazgo destaca la necesidad de promover la conciencia sobre la importancia de la rotación frecuente de contraseñas como una medida esencial para mitigar posibles amenazas cibernéticas y fortalecer la seguridad de los sistemas de acceso vehicular en la comunidad residencial. Se sugiere implementar programas educativos para fomentar esta buena práctica entre los residentes.

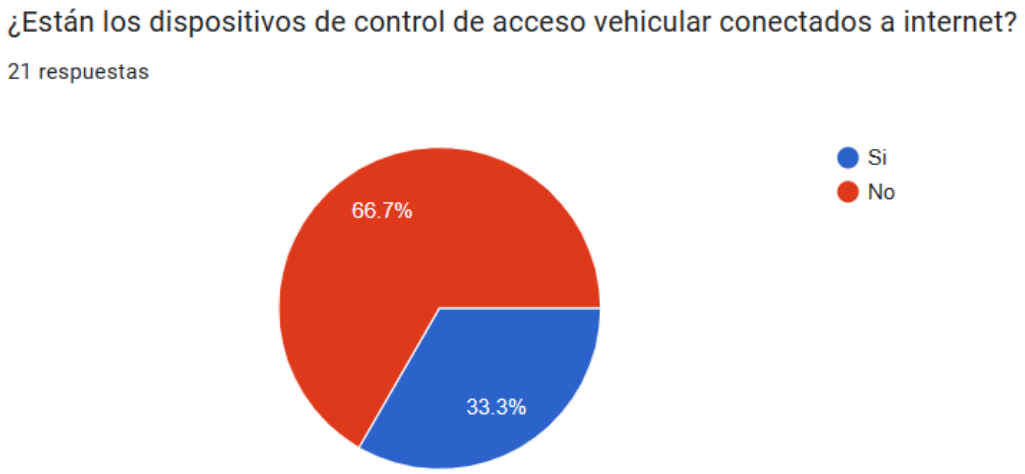



***FIGURA 3.13: DATOS ESTADÍSTICOS PREGUNTA 7***

***FUENTE: AUTOR***

La encuesta indica que el 33.3% de las 21 personas encuestadas son conscientes de que los dispositivos de control de acceso vehicular en la residencia están conectados a Internet. Sin embargo, la mayoría, el 66.7%, no tiene conocimiento de esta conexión, lo que sugiere una falta de conciencia sobre la exposición potencial a amenazas cibernéticas. Este resultado subraya la necesidad de educar a los residentes sobre la conectividad de estos dispositivos y promover medidas de seguridad adicionales para mitigar posibles riesgos de ataques en línea. Se recomienda implementar programas de concienciación para mejorar la comprensión de la interconexión de los sistemas de acceso vehicular con Internet.


***FIGURA 3.14: DATOS ESTADÍSTICOS PREGUNTA 8***

***FUENTE: AUTOR***

La encuesta revela que solo el 5% de las 20 personas encuestadas están al tanto de la implementación de medidas de seguridad para proteger la conexión de los dispositivos de control de acceso vehicular en la residencia. En contraste, el 95% no tiene conocimiento de tales medidas, indicando una potencial falta de conciencia sobre la importancia de salvaguardar la conexión de estos sistemas. Este resultado destaca la necesidad crítica de reforzar las medidas de seguridad y llevar a cabo iniciativas educativas para mejorar la comprensión y la implementación de prácticas seguras en relación con la conectividad de los dispositivos de acceso vehicular en la comunidad residencial.

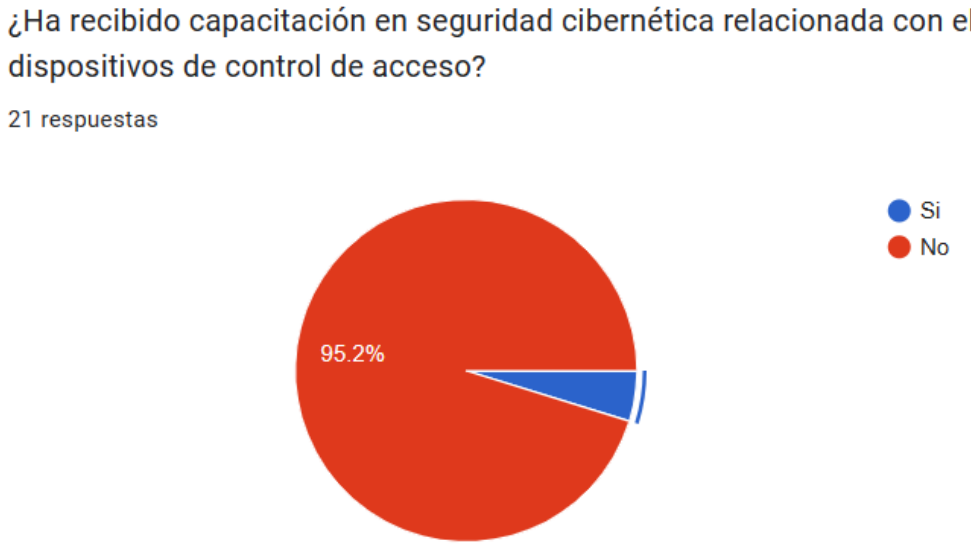



***FIGURA 3.15: DATOS ESTADÍSTICOS PREGUNTA 9***

***FUENTE: AUTOR***

La encuesta refleja que únicamente el 4.8% de las 21 personas encuestadas han recibido capacitación en seguridad cibernética relacionada con el uso de dispositivos de control de acceso vehicular en la residencia. Sin embargo, la abrumadora mayoría, el 95.2%, no ha recibido esta capacitación, indicando una brecha significativa en la preparación de los residentes ante posibles amenazas digitales. Este hallazgo resalta la urgencia de implementar programas de formación en seguridad cibernética para fortalecer la conciencia y competencia de los usuarios, garantizando así una utilización más segura y eficaz de los sistemas de control de acceso vehicular en la comunidad residencial.

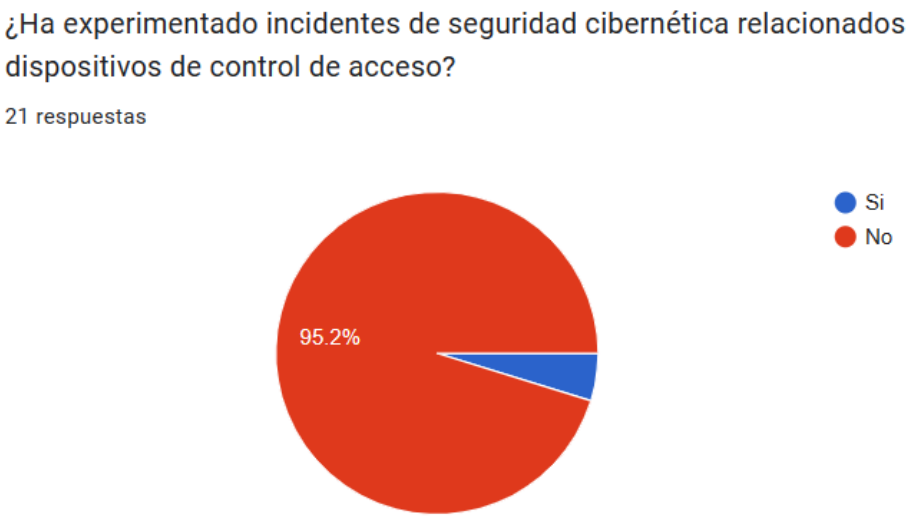



***FIGURA 3.16: DATOS ESTADÍSTICOS PREGUNTA 10***

***FUENTE: AUTOR***

La encuesta revela que solo el 4.8% de las 21 personas encuestadas han experimentado incidentes de seguridad cibernética relacionados con los dispositivos de control de acceso vehicular en la residencia. En contraste, el 95.2% no ha enfrentado este tipo de incidentes, indicando una aparente ausencia generalizada de problemas de seguridad. Aunque la proporción de afectados es baja, este resultado subraya la importancia de mantener la vigilancia y adoptar medidas proactivas para prevenir posibles amenazas cibernéticas en el futuro, a fin de garantizar la integridad y seguridad continua de los sistemas de control de acceso vehicular en la comunidad residencial.


***FIGURA 3.17: DATOS ESTADÍSTICOS PREGUNTA 11***

***FUENTE: AUTOR***

La encuesta indica que solo el 9.5% de las 21 personas encuestadas son conscientes de la existencia de un proceso claro de comunicación en caso de un incidente de seguridad cibernética relacionado con los dispositivos de control de acceso vehicular en la residencia. Sin embargo, el 90.5% no tiene conocimiento de dicho proceso, evidenciando una falta de claridad y comunicación efectiva en el manejo de situaciones de seguridad digital. Este resultado resalta la necesidad urgente de establecer y comunicar de manera transparente protocolos de respuesta a incidentes, asegurando que los residentes estén preparados y puedan colaborar eficazmente en la mitigación de amenazas cibernéticas.

¿Tiene algún comentario, sugerencia o preocupación adicional relacionada con la seguridad cibernética en la urbanización?

6 respuestas

| |
|---|
| no |
| NINGUNO |
| No |
| implementar circuito de cámaras |
| N/A |

***FIGURA 3.18: DATOS ESTADÍSTICOS PREGUNTA 12***

***FUENTE: AUTOR***

## 3.3. Análisis de la arquitectura de sistema

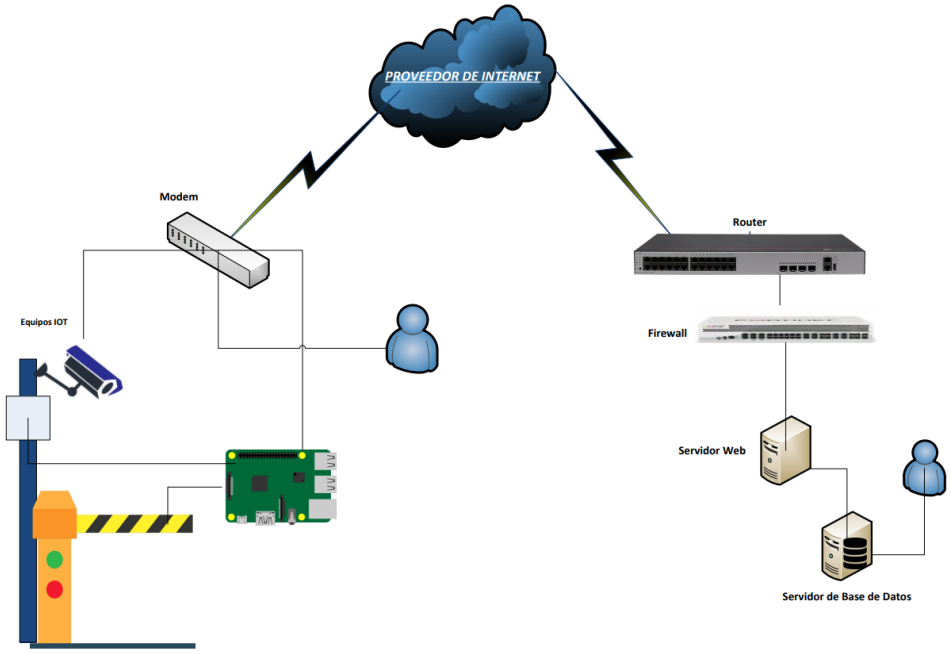



***FIGURA 3.19: ESQUEMA CLIENTE-SERVIDOR WEB***

***FUENTE: AUTOR***

Como se puede observar en el gráfico, la compañía cuenta con un sistema cliente-servidor web que permite controlar el acceso a los residentes mediante registro del usuario en la base de datos del sistema. El software también tiene integrado un módulo donde puede ver las cámaras mediante la web y el registro de los usuarios cuando entran y salen de la garita.

Las cámaras como el sotfware cliente están conectadas a un servicio de internet con ip pública fija donde se realizan DNAT de puertos con el objetivo de que el servidor de matriz pueda llegar a los dispositivos de las garitas para controlar y administrar.

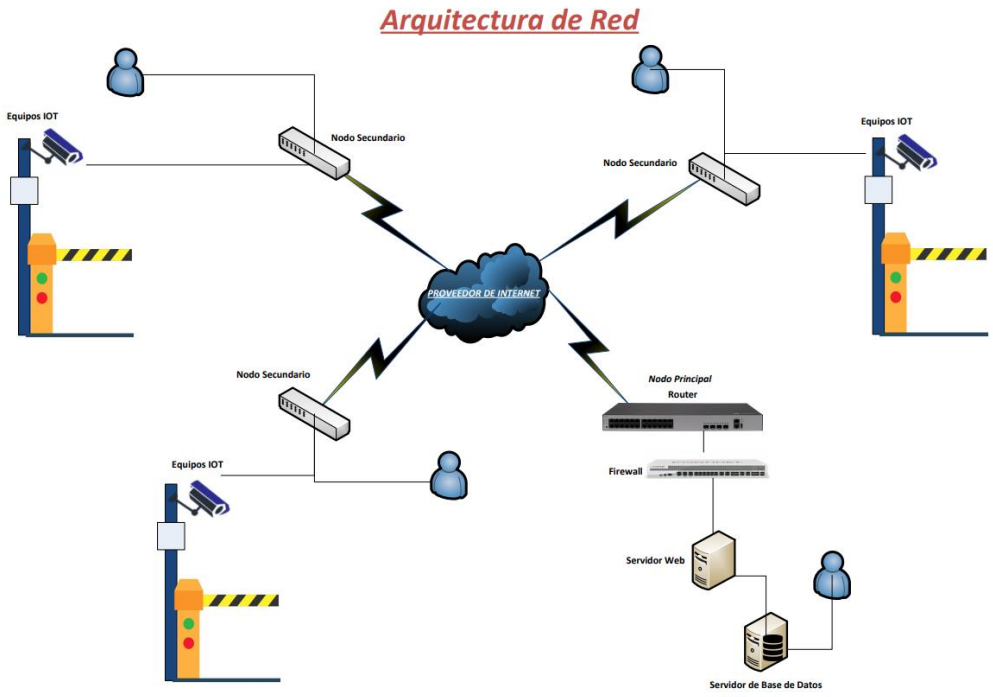



***FIGURA 3.20: ARQUITECTURA DE RED***

***FUENTE: AUTOR***

Esta arquitectura de red como se observa en el grafico anterior, actualmente posee en todas las garitas puntos de internet de hogar que se usan como medio de comunicación entre un nodo principal denominado matriz con sus nodos secundarios denominado urbanizaciones.

Los nodos secundarios cuentan con los activos de información conectados a un router el cual realiza reenvió de puertos para que el servidor de matriz pueda llegar a las cámaras locales y al sistema cliente de la urbanización.

El servidor Web con la Base de datos se encuentra conectado hacia un firewall el cual protege al servidor de Matriz y este a su vez se conecta al router de internet que le permite llegar a los dispositivos que están en las diferentes garitas de la ciudad de Guayaquil

### 3.4. Funcionamiento del servicio del control de acceso

Los dispositivos IOT que se encuentran dentro de Garita donde se vigilan y se controla el acceso a los vehículos cumplen con las siguientes funciones que se detallan a continuación con el objetivo de brindar seguridad a los visitantes y residentes de las urbanizaciones:

Una cámara inferior ubicada en la parte a 20 cm del piso para capturar la placa de los carros que ingresan y a 1 metro con 70 cm se encuentra otra cámara

superior para visualizar a los usuarios que están en la parte delantera del vehículo, se tiene otra cámara en la torre de color gris donde se puede observar al conductor de manera lateral o frontal cuando coloque los documentos y adicional se cuenta una cámara en la parte trasera a un metro para obtener las imágenes de placas de motos.

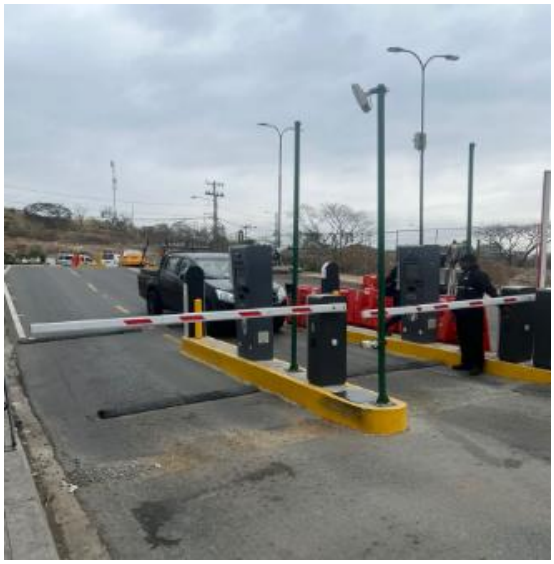


***FIGURA 3.21: INGRESO A GARITA***

***FUENTE: AUTOR***

El lector de documento se encuentra ubicado debajo de una pantalla de bienvenida que cuenta con 3 opciones de verificación antes de su ingreso como se observa en la imagen siguiente.


***FIGURA 3.22: SISTEMA INGRESO***

***FUENTE: AUTOR***

La opción código QR es para los residentes que tienen en sus celulares instalada la aplicación proporcionada por la empresa de seguridad que les permitirá escanear el código de la pantalla para saber si el usuario tiene permisos para acceder a su vivienda, en cambio sí se elige las opciones proveedores o visitantes, la pantalla le indicará “Coloque su identificación” para que el conductor o los visitantes ingresen la cedula en el recuadro donde se escanean los documentos como se observa en las siguientes imágenes:

***FIGURA 3.23: IDENTIFICACIÓN DEL VISITANTE***

***FUENTE: AUTOR***

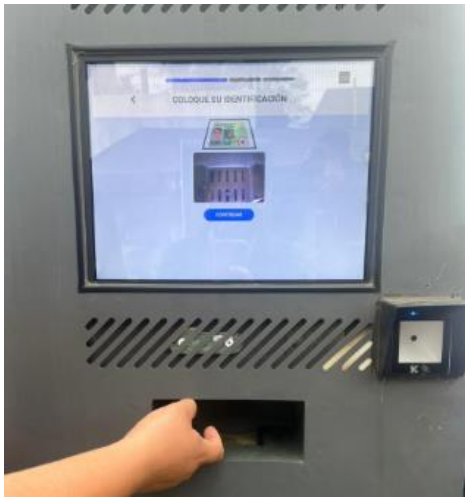



***FIGURA 3.24: ESCANEO DE LA DOCUMENTACIÓN***

***FUENTE: AUTOR***

Después de escanear su documento de identidad, la pantalla solicita que se ingrese el nombre de la persona a visitar para que el sistema se comunique con el residente y autorice al guardia mediante llamada el paso del vehículo.


***FIGURA 3.25: RESIDENTE ACCEDER***

***FUENTE: AUTOR***

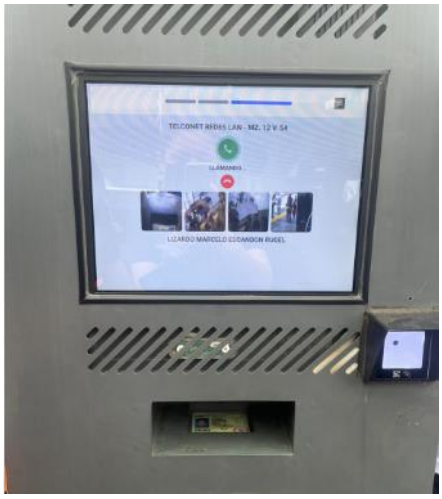


***FIGURA 3.26: LLAMADA AL RESIDENTE***

***FUENTE: AUTOR***

Dentro de la torre gris instalada se tiene un switch trendnet de 8 puertos donde llegan las cámaras, la tarjeta raspberry que permite controlar el momento en que se levanta la barra vehicular si la tarjeta lectora escanea el código QR que poseen los vehículos residentes ubicados en el parabrisa superior y además que coincidan con la base de datos como autorizados configurados en la memoria del chip que se encuentra en la raspberry, este permitirá el ingreso rápido de los residentes a comparación al de los visitantes que necesita al guardia para accionar la subida manualmente de la barrera vehicular para el paso de los no residentes después de escanear la identificación personal.

***FIGURA 3.27: TORRE DE ACCESO***

***FUENTE: AUTOR***

***FIGURA 3.28: TORRE DE ACCESO***

***FUENTE: AUTOR***

***FIGURA 3.29: TARJETA RASBERRY***

***FUENTE: AUTOR***

Se tiene un switch trendnet de 8 puertos ubicado dentro de la Torre Gris la cual conecta los cables de las 4 cámaras, la tarjeta raspberry y el modem de internet que está dentro de la garita y que a su vez se conecta con el servidor de matriz y con monitores para que los guardias mediante las cámaras puedan monitorear 24/7 si existen alguna anomalía del usuario, documentos falsos, o armas que puedan portar.

***FIGURA 3.30: SWITCH TRENDNET***

***FUENTE: AUTOR***

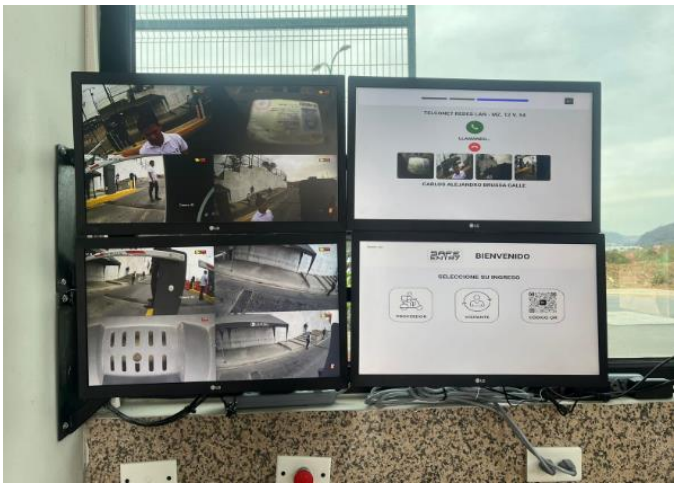



***FIGURA 3.31: MONITOREO EN GARITA***

***FUENTE: AUTOR***

## 3.5. Testeo ético de la arquitectura de red

Se realizará el testeo a uno de los nodos secundarios ya que, mediante el esquema mostrado en el punto anterior, son dispositivos conectados directamente al internet mostrando una visibilidad de que son los enlaces más vulnerables de esta infraestructura.

Para hacer esta prueba, se solicitó al personal de sistemas de la empresa de seguridad de Guayaquil los permisos necesarios y las ips públicas de uno de los router que están en las urbanizaciones para realizar el escaneo de puertos abiertos mediante las herramientas Nmap y Nessus.

Nessus es una herramienta de escaneo de vulnerabilidades que se utiliza para identificar y evaluar posibles debilidades en sistemas informáticos, redes y aplicaciones. Es importante destacar que el escaneo de puertos es solo una parte de la funcionalidad integral de Nessus, sus demás funciones se basan en identificar vulnerabilidades en sistemas y ayuda a los profesionales de seguridad informática y equipos de administración de sistemas que buscan mantener un entorno seguro y cumplir con los estándares de seguridad.

Se procede a instalar la herramienta Nessus dentro de una máquina virtual Kali, en la cual se creó una carpeta denominada Scan_IoT que permite ingresar la IP que se requiera escanear con el objetivo de encontrar vulnerabilidades como observará a continuación en las siguientes imágenes.

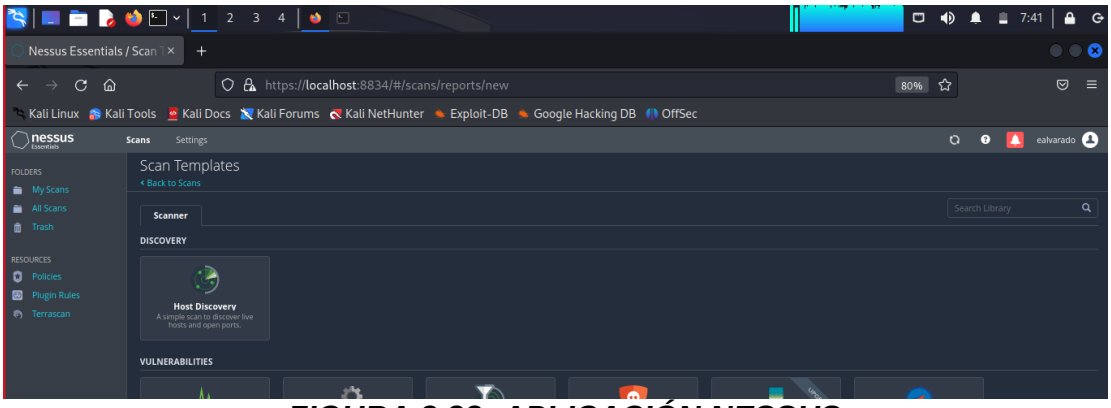



***FIGURA 3.32: APLICACIÓN NESSUS***

***FUENTE: AUTOR***

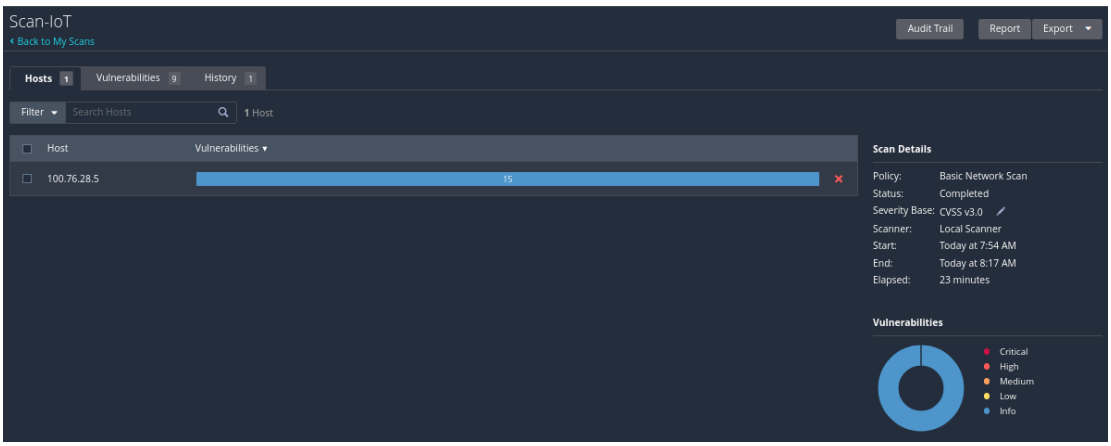



***FIGURA 3.33: ESCANEO DE PUERTOS***

***FUENTE: AUTOR***

En las imágenes anteriores, se verifica que en la herramienta Nessus en su versión gratuita que ayuda a encontrar puerto abiertos, lo cual nos da un indicio para saber que puertos pueden ser no seguros o vulnerables antes ataques comunes.

Nmap es una herramienta de código abierto que ayuda a los profesionales de seguridad y administradores de sistemas explorar redes, descubrir hosts y servicios proporcionando información detallada sobre los dispositivos conectados a una red, los servicios que están ejecutándose en esos dispositivos y los puertos abiertos como se observará en las siguientes imágenes:

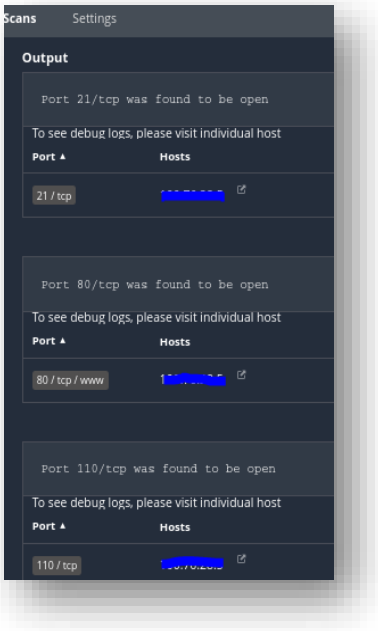



***FIGURA 3.34: PUERTOS VULNERABLES***

***FUENTE: AUTOR***

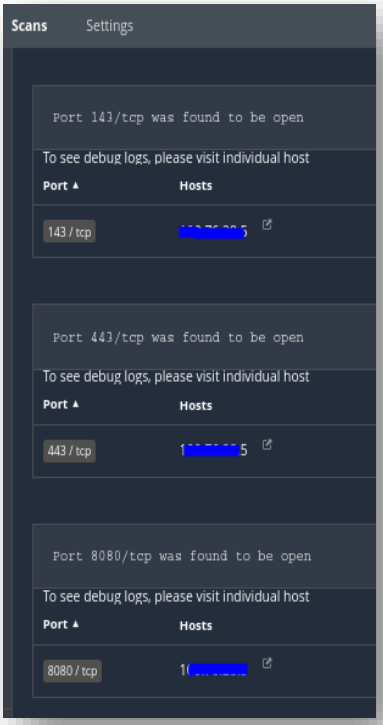



***FIGURA 3.35: PUERTOS VULNERABLES***

***FUENTE: AUTOR***

Esta herramienta es importante utilizarla de manera ética cumpliendo con los permisos necesarios como en este caso que se utilizará el permiso de la compañía la cual desea que sus servicios sean revisados con fines educativos para encontrar vulnerabilidades con las leyes y regulaciones locales al realizar escaneos en redes que no le pertenecen. Además, algunos escaneos pueden ser detectados por sistemas de seguridad y firewalls, por lo que su uso debe ser cuidadoso y respetar la privacidad y políticas de red.

Nmap es una herramienta de código abierto que ayuda a los profesionales de seguridad y administradores de sistemas explorar redes, descubrir hosts y servicios proporcionando información detallada sobre los dispositivos conectados a una red, los servicios que están ejecutándose en esos dispositivos y los puertos abiertos como se observará en las siguientes imágenes:

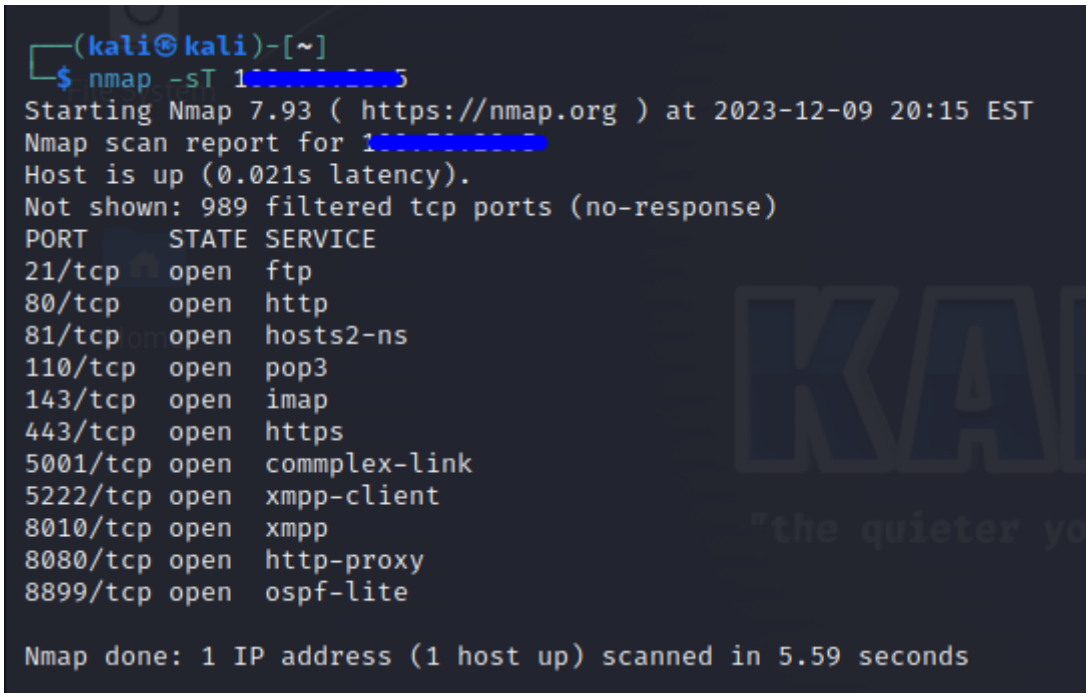



***FIGURA 3.36: ESCANEO DE PUERTOS***

***FUENTE: AUTOR***

Se ejecuto el comando nmpa -sT también conocido como escaneo TCP Connect porque se realiza un 3-way-handshake que es una conexión completa vía TCP.

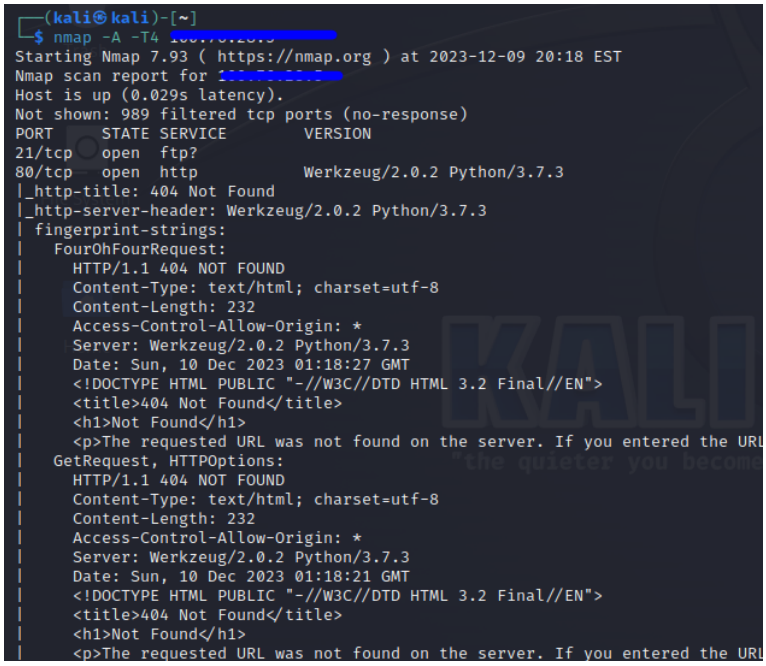



***FIGURA 3.37: ESCANEO DE PUERTOS***

***FUENTE: AUTOR***

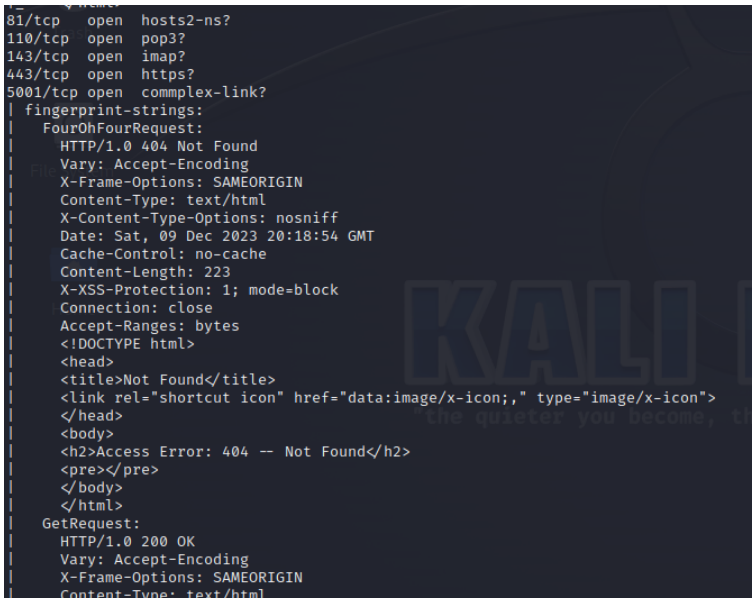



***FIGURA 3.38: ESCANEO DE PUERTOS***

***FUENTE: AUTOR***

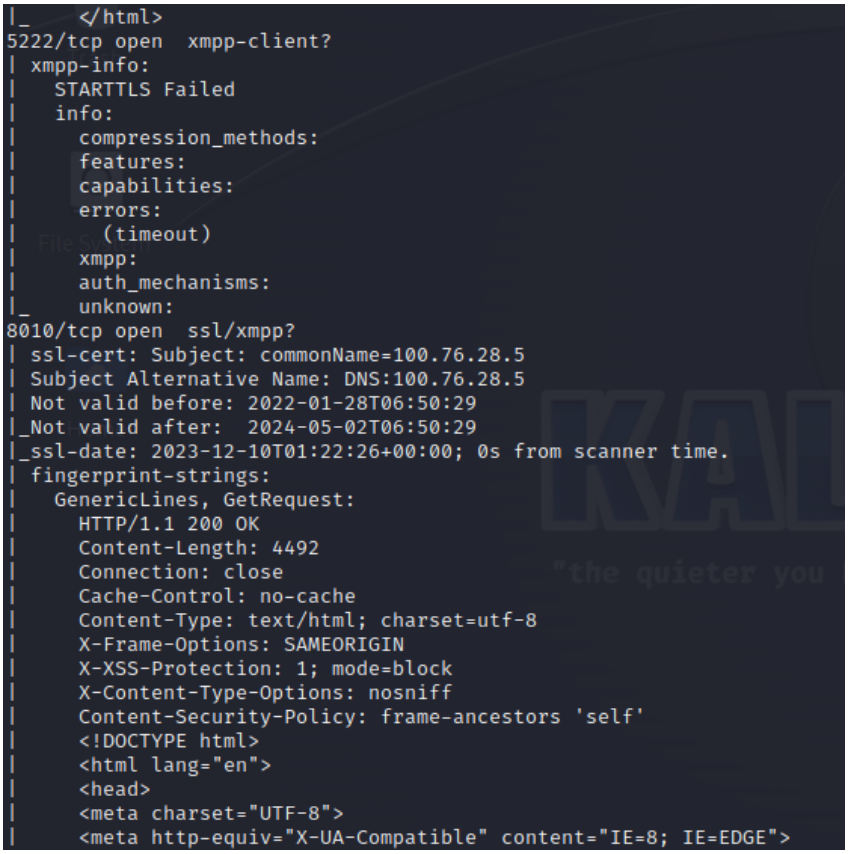



***FIGURA 3.39: ESCANEO DE PUERTOS***

***FUENTE: AUTO***

En las imágenes anteriores se ejecutó el comando nmap -A que muestra la versión del sistema operativo mediante un escaneo agresivo.

Estas herramientas se deben utilizar de manera ética cumpliendo con las leyes y regulaciones locales al realizar escaneo en redes que no le pertenecen porque el escaneo puede ser detectado por sistemas de seguridad y firewalls, por lo que su uso debe ser cuidadoso y respetar la privacidad y políticas de red.

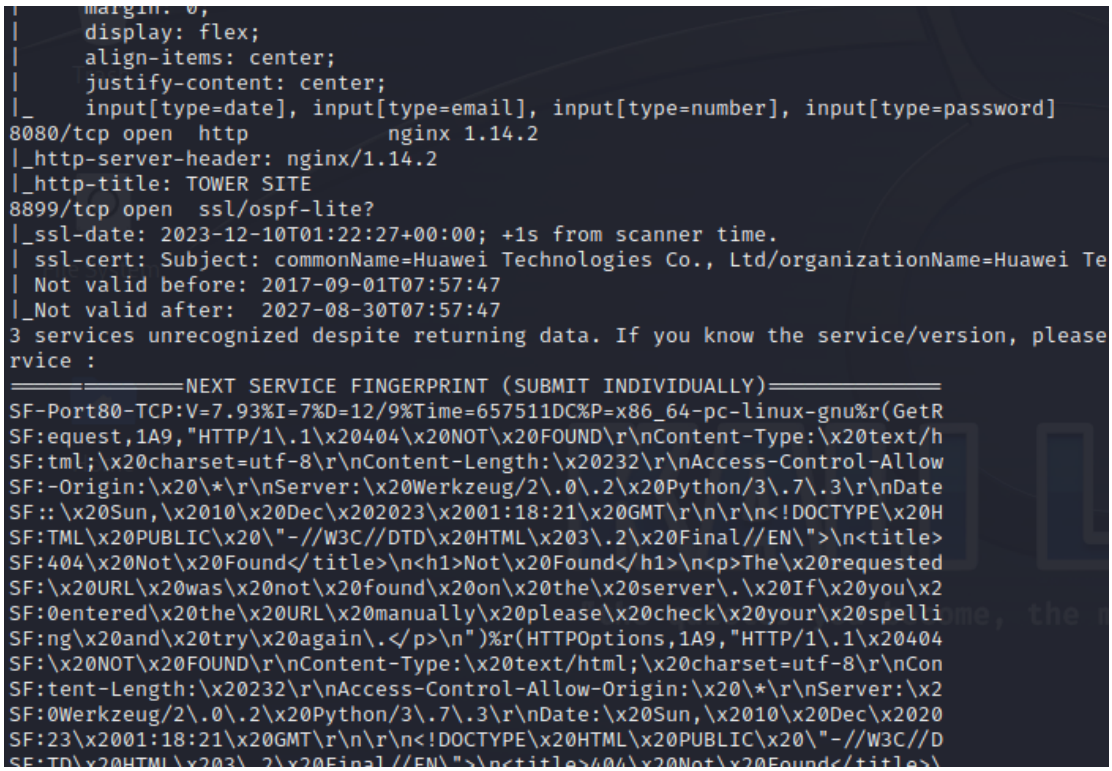



***FIGURA 3.40: ESCANEO DE PUERTOS***

***FUENTE: AUTOR***

# CAPITULO IV.

# EVALUACIÓN DE LA INFRAESTRUCTURA DE CONTROL DE ACCESO VEHICULAR IOT

## 4.1 Pruebas de Penetración

En base a la prueba de puertos realizados en el apartado 3.5, se identifica que existen puertos no seguros que se encuentran abiertos como el 80 y el 8080. En el escaneo nmpa -A el puerto 80 indica como abierto pero los servicios no

se extraen porque la solicitud URL no fue encontrada por el servidor y por ende tiene como resultado en el navegador: servicio no encontrado, pero en el escaneo del puerto 8080 se observa el título de la página web: TOWER SITE con lo que indica posiblemente acceso al servicio 8080 desde un navegar para saber qué información tiene este servicio.

A continuación, se ingresa la ip con el puerto 8080 para verificar que información se extrae:


***FIGURA 4.1: NAVEGADOR LA CÁMARA***

***FUENTE: AUTOR***

Pueden darse cuenta de que abre el puerto 8080 una página web con usuario y contraseña para que los guardias de la empresa se conecten al aplicativo desde la garita. Este escaneo muestra que este servicio web es local y que tiene acceso de usuario para administrar posiblemente la conexión de la base de datos que está alojado en matriz.

Para revisar que vulnerabilidades se pueden encontrar en este servidor web local, ejecutaremos desde una maquina Kali la herramienta gratuita denominada OWASP ZAP que es una herramienta de seguridad de código abierto desarrollada para encontrar vulnerabilidades en servicios web. OWASP (Open Web Application Security Project), que se centra en mejorar la seguridad de las aplicaciones web. ZAP proporciona funcionalidades de escaneo de seguridad automatizado, pruebas manuales y diversas características para identificar y corregir problemas de seguridad en aplicaciones web.

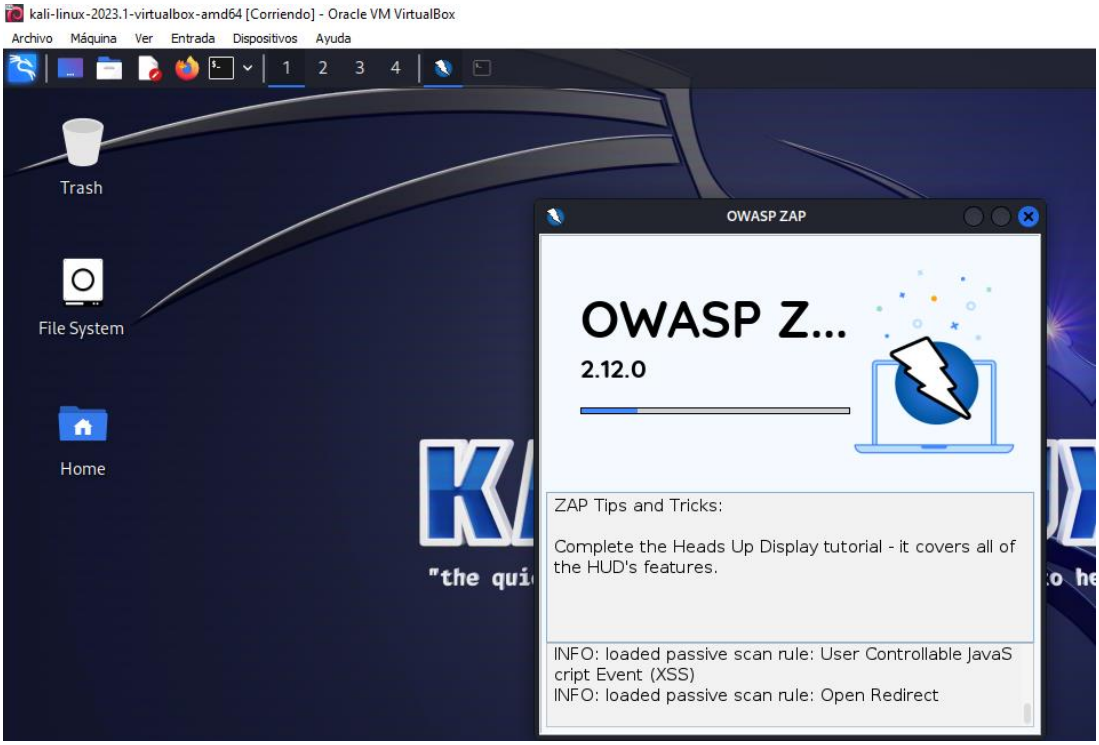



***FIGURA 4.2: ABRIR OWASP ZAP***

***FUENTE: AUTOR***

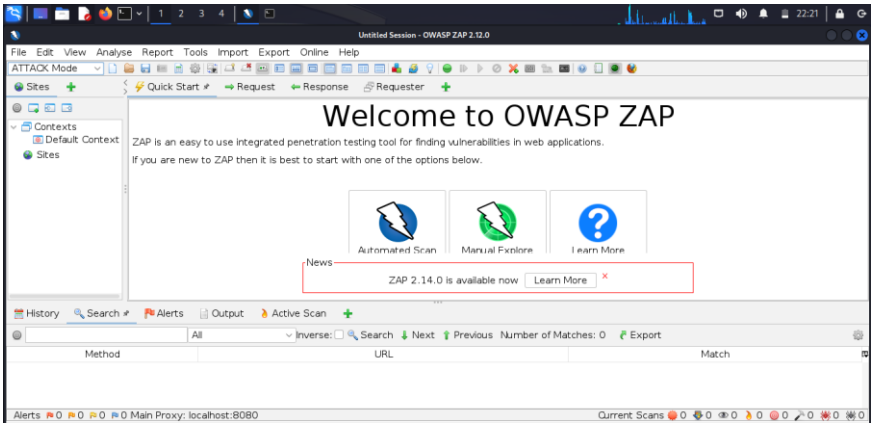



***FIGURA 4.3: MENÚ OWASP ZAP***

***FUENTE: AUTOR***

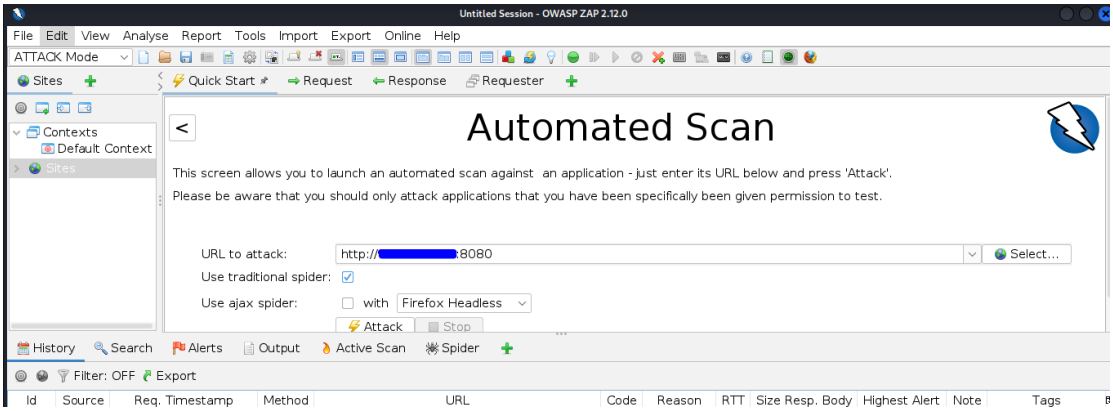



***FIGURA 4.4: EJECUCIÓN DEL SACAN Y DEL SPIDER***

***FUENTE: AUTOR***

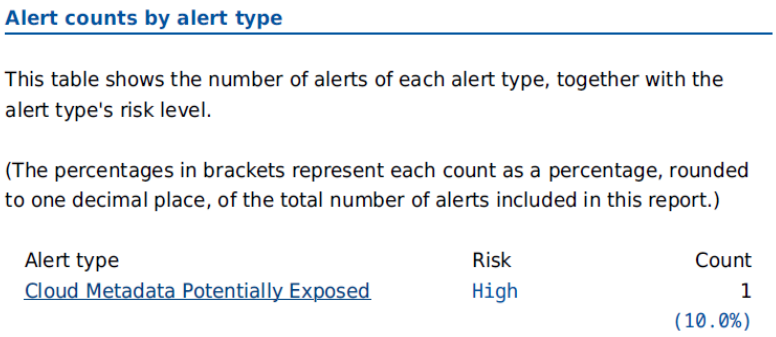
Se activo la opción spider dentro del ZAP para descubrir automáticamente nuevos recursos del Sitio Web que se desea escanear identificando todos los hipervínculos en la página agregándolos a una lista de URL para visitar y de esta manea sucesivamente el proceso continúa de forma recursiva siempre que se encuentren nuevos recursos.

Después de la ejecución, se procedió a generar un reporte en la herramienta ZAP donde se detalla las vulnerabilidad y amenazas que serán explicados en los siguientes apartados (consulte el anexo 2 que es el reporte o informe del ZAP).

## 4.2 Identificación de amenazas

Las amenazas en seguridad informática es un evento que tiene el potencial de causar daño mediante la explotación de vulnerabilidades por un atacante con intenciones maliciosas que buscan acceder a información confidencial.

En base al escaneo realizado en ZAP y mediante el informe, se tiene como única vulnerabilidad de riesgo alto el evento o alerta denominada: Cloud Metadata Potentially Exposed como se observa a continuación:



**Alert counts by alert type**

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

| Alert type | Risk | Count |
|---|---|---|
| Cloud Metadata Potentially Exposed | High | 1 (10.0%) |

***FIGURA 4.5: ALERTA DE RIESGO ALTO CLOUD METADATA POTENTIALLY EXPOSED***

***FUENTE: ANEXO 2 (REPORTE ZAP)***

Este tipo de alerta de nivel alto fue generado mediante un ataque de metadatos al destino web con la finalidad de obtener referencias que conllevan los metadatos que son información adicional o descriptiva como creación, modificación, formato, ubicación u otras características que se encuentra asociadas con un archivo, documento, imagen u otro tipo de datos.

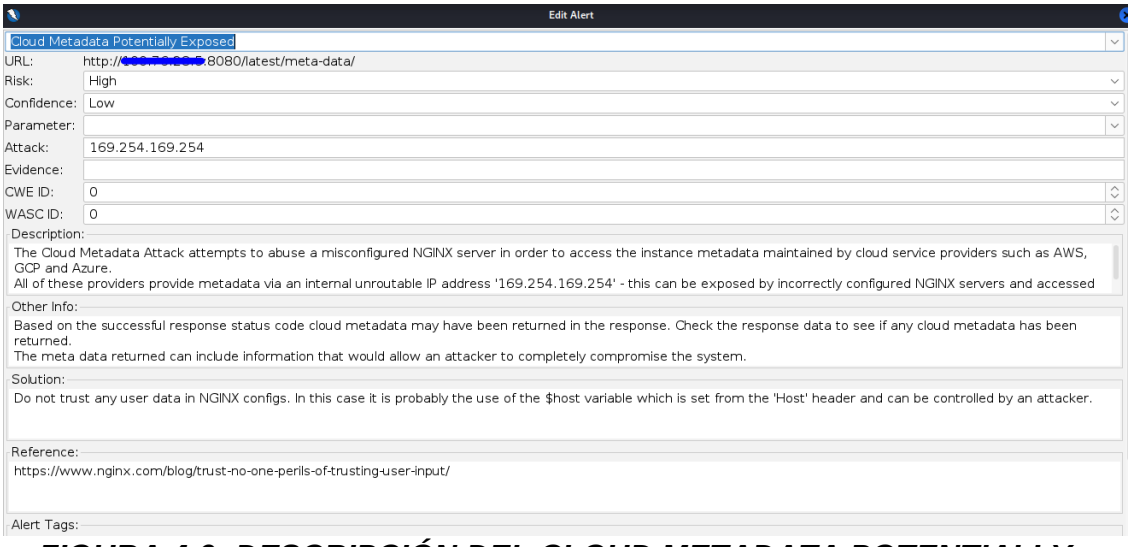



***FIGURA 4.6: DESCRIPCIÓN DEL CLOUD METADATA POTENTIALLY EXPOSED***

***FUENTE: AUTOR***

Después de la explotación, se obtiene que el servidor web utilizado es NGINX y que se encuentra mal configurado porque en el encabezado HTTP existe configuración de proxy de manera incorrecta donde se tiene la ip: 169.254.169.254 en el atributo proxy_pass y por la cual indica que existe

posiblemente conexiones con aplicativos externos como por ejemplo Amazon, Azure, etc.

Al tener una ip en el proxy, el atacante puede fácilmente configurar dicha ip en un servidor arbitrario utilizando el proxy actual como un proxy de reenvió donde se capturarán los archivos que contengan metadatos por ende es recomendable poner en la opción proxy_pass un dominio asegurándose de que el atacante no pueda resolver el proceso de resolución de DNS o utilizar un Firewall de por medio para solo aceptar solicitudes de IPS confiables.

## 4.3 Evaluación de Vulnerabilidades

Las vulnerabilidades se asocian a una debilidad o fallo en un sistema, aplicación, red o proceso que podría comprometer la seguridad mediante una amenaza explotada.

La vulnerabilidad es una debilidad intrínseca o inherente en un sistema a diferencia de la amenaza que es un evento que podría aprovechar esa vulnerabilidad o debilidad por tal motivo a continuación se abordan las alertas de nivel medio que fueron proporcionadas por la herramienta ZAP

### 4.3.1. Content Security Policy (CSP) Header Not Set


***FIGURA 4.7: DESCRIPCIÓN DEL CONTENT SECURITY POLICY***

***FUENTE: AUTOR***

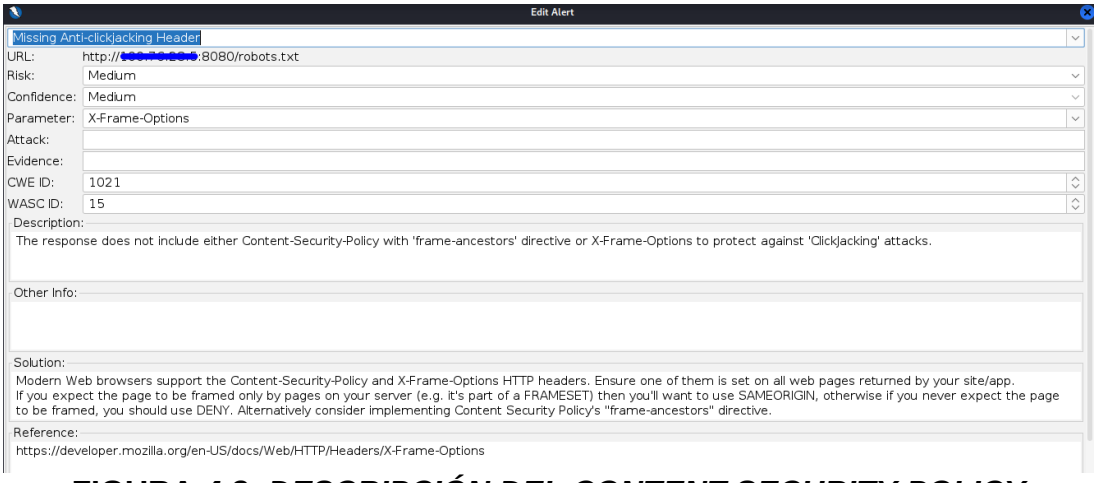



**FIGURA *4.8: DESCRIPCIÓN DEL CONTENT SECURITY POLICY***

***EXTENSIÓN ROBOOTS.TXT***

***FUENTE: AUTOR***

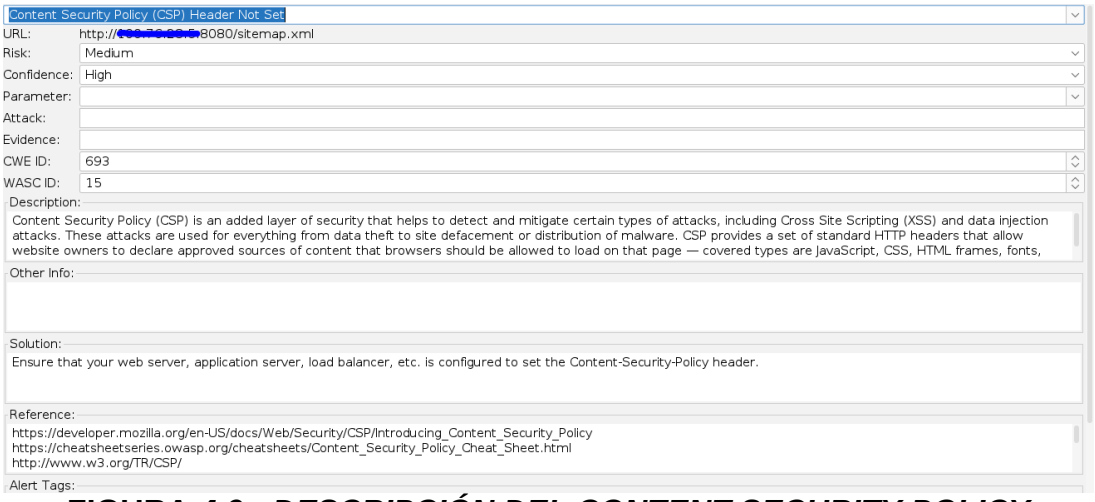



**FIGURA *4.9: DESCRIPCIÓN DEL CONTENT SECURITY POLICY EXTENSIÓN SITEMAP.XML***

***FUENTE: AUTOR***

En base a la revisión del código de la página web, el programa Zap identifica mal configurado el atributo content security policy que es una medida de seguridad implementada en navegadores web para ayudar a mitigar ataques de inyección de código malicioso (Cross-Site Scripting o XSS). Estos ataques se utilizan para todo, desde el robo de información al usuario hasta la desfiguración del sitio o la distribución de malware.

Para prevenir estos riesgos, es crucial implementar y mantener una CSP sólida y actualizada. Esto implica configurar adecuadamente las directivas de CSP dentro de encabezado HTTP donde se permita a los propietarios de sitios web declarar fuentes de contenido confiable como se explica en el siguiente ejemplo.

Un desarrollador de sitio web requiere permitir que los usuarios a través de una web incluyan imágenes de cualquier origen en su propio contenido y se restrinja los medios de audio o vídeo a proveedores de confianza

La script seria de la siguiente manera: Content-Security-Policy: default-src 'self'; img-src *; media-src ejemplo.org ejemplo.net

En este código se puede verificar el parámetro img-src con el “*”, el cual permite que las imágenes pueden cargarse desde cualquier sitio y también se puede observar que los medios solo estén permitidos desde ejemplo.org y ejemplo.net mediante el atributo media-src.

### 4.3.2. Missing Anti-clickjacking Header

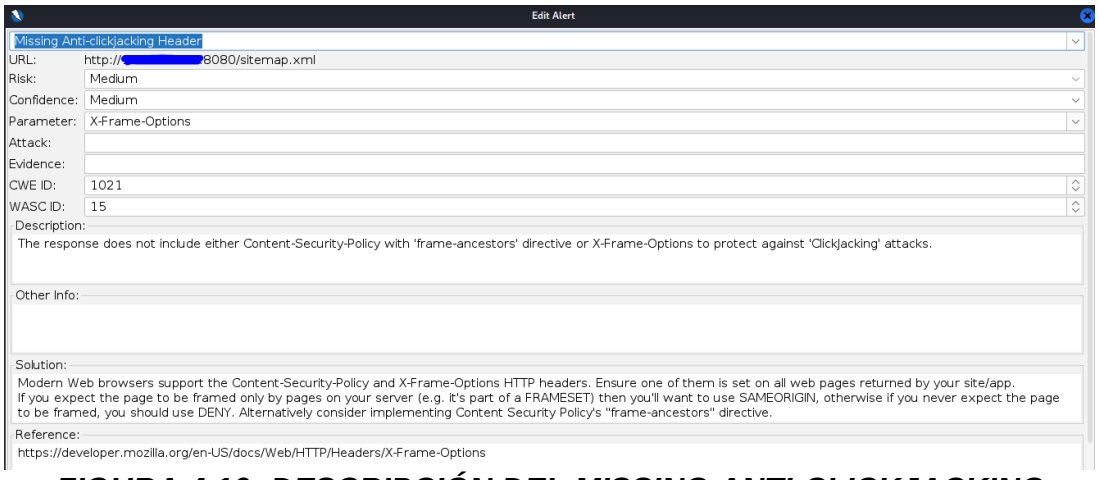



***FIGURA 4.10: DESCRIPCIÓN DEL MISSING ANTI-CLICKJACKING HEADER***

***FUENTE: AUTOR***

El Missing Anti-clickjacking Header es una técnica maliciosa en la que un atacante superpone elementos invisibles o engañosos sobre el contenido de una página web, de modo que cuando un usuario hace click en lo que parece ser una parte confiable o legítima de la página, está interactuando con un elemento oculto y no deseado causando problemas de seguridad como suplantación de Interacciones y robo de Información o redirección a sitios maliciosos.

Este problema es debido a la falta de configuración del atributo Content-Security-Policy y X-Frame-Options en el encabezado de un sitio web que previene el framing no autorizado.

Existen dos directivas posibles para X-Frame-Options que se explican a continuación:

La directiva DENY donde la página no se puede mostrar en un marco, independientemente del sitio que intente hacerlo y la directiva SAMEORIGIN donde La página solo se puede mostrar si todos los marcos antecesores son del mismo origen que la propia página.

Por ejemplo, si se requiere configurar Apache para que se envíe el encabezado de todas las páginas, se debe ingresar lo siguiente: Header always set X-Frame-Options "SAMEORIGIN"

### 4.3.3. Vulnerable JS Library

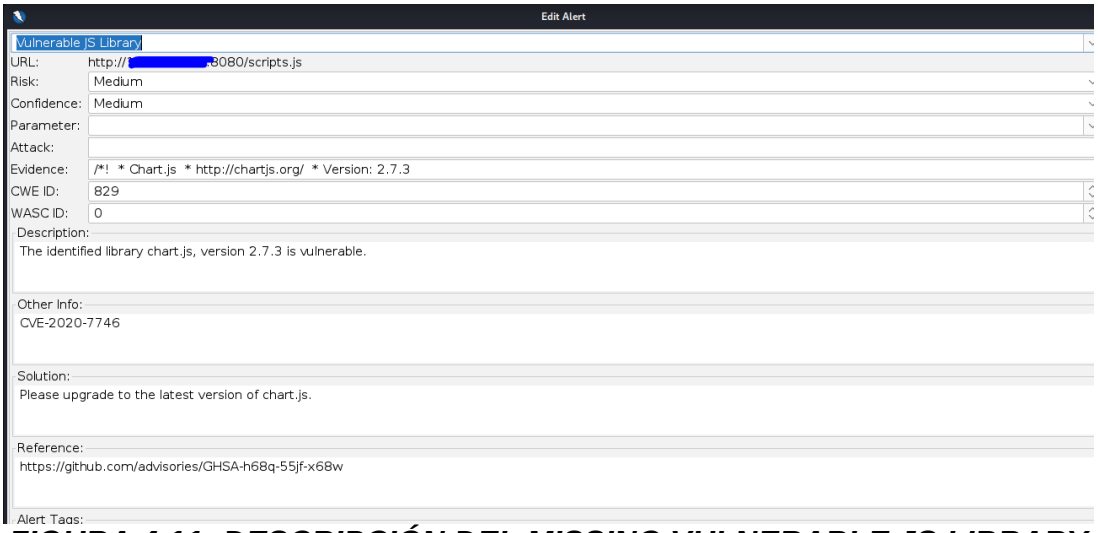



***FIGURA 4.11: DESCRIPCIÓN DEL MISSING VULNERABLE JS LIBRARY***

***FUENTE: AUTOR***

La utilización de bibliotecas de JavaScript vulnerables en aplicaciones web puede tener diversas consecuencias en términos de seguridad como Inyección de código malicioso, robo de información, ataques de fuerza bruta y riesgo de ataques de desbordamiento de búfer. El programa ZAP recomienda que se actualice la última versión del JavaScript que contiene los nuevos parches de seguridad para mitigar esta vulnerabilidad.

### 4.3.4. Private IP Disclosure


***FIGURA 4.12: DESCRIPCIÓN DEL PRIVATE IP DISCLOSURE***

***FUENTE: AUTOR***

La vulnerabilidad "Private IP Disclosure" (Divulgación de IP privada) se refiere a la exposición no autorizada de direcciones IP privadas en un contexto donde deberían mantenerse confidenciales. Las direcciones IP privadas, como las definidas en el rango de direcciones IP reservadas por la especificación IPv4 (por ejemplo, 10.0.0.0 a 10.255.255.255, 172.16.0.0 a 172.31.255.255, 192.168.0.0 a 192.168.255.255), están destinadas a ser utilizadas en redes privadas y no deben ser visibles públicamente a través de Internet.

Las consecuencias de la divulgación de IP privada pueden incluir los siguientes problemas de seguridad:

Ataques dirigidos: Los atacantes pueden aprovechar la información sobre direcciones IP privadas para lanzar ataques dirigidos contra redes o sistemas específicos. Esto podría incluir intentos de intrusión, escaneo de puertos y otros tipos de ataques.

.

Exposición de servicios internos: Si se revelan direcciones IP privadas asociadas a servicios internos, como bases de datos o servidores de aplicaciones, podría facilitar a los atacantes la identificación de servicios específicos que podrían ser objetivos de ataques.

Violación de privacidad: La divulgación de información interna, incluidas las direcciones IP privadas, puede considerarse una violación de la privacidad de la infraestructura de una organización.

Para mitigar los riesgos asociados con la divulgación de IP privada, es esencial implementar prácticas de seguridad sólidas como el control de acceso para restringir el acceso no autorizado a información confidencial, utilizar firewalls para filtrar el tráfico no deseado y capacitar a los empleados y usuarios sobre la importancia de mantener la confidencialidad de la información de red.

## 4.4 Análisis de impacto y probabilidad

Una matriz de riesgo es una herramienta visual que se utiliza en la gestión de riesgos para evaluar y presentar de manera sistemática la probabilidad y el impacto de los riesgos en un proyecto, proceso o sistema. Esta herramienta ayuda a las organizaciones a identificar, clasificar y priorizar los riesgos con el objetivo de tomar decisiones informadas sobre cómo abordarlos.

Para realizar un estudió de análisis de impacto y probabilidad referente a las alertas encontradas en los 3 capítulos anteriores, se desarrollará en este capítulo un matriz de riesgo que ayuda a las organizaciones a identificar, clasificar y priorizar los riesgos.

Para crear una matriz de riesgo, se establecieron 20 eventos comunes que podrían ocurrir ante un ataque de ciberseguridad detallados en la tabla 3 y que serán de ayuda para referenciar las descripciones de los eventos con las 7 vulnerabilidades encontradas en el apartado 4.2 y 4.3.

Para esta matriz de riesgo (tabla 1) se crearon 3 niveles de probabilidad (alto, medio, bajo) y 3 niveles de consecuencias (menor, moderado, máximo) que al combinarse muestran 3 niveles de riegos: Aceptable, tolerable y alto como se indica en la tabla 2.

| MATRIZ DE RIESGOS | | | | |
|---|---|---|---|---|
| CONSECUENCIAS | | | | |
| | | MENOR | MODERADO | MAXIMO |
| PROBABILIDAD | | 1 | 2 | 4 |
| ALTA | 3 | 3 | 6 | 12 |
| MEDIA | 2 | 2 | 4 | 8 |
| BAJA | 1 | 1 | 2 | 4 |

***Tabla 1: Matriz de Riesgos***

***Fuente: Autor***

| NIVEL DE RIESGO | COLOR |
|---|---|
| RIESGO ACEPTABLE | |
| RIESGO TOLERABLE | |
| RIESGO ALTO | |

***Tabla 2: Niveles de Riesgo***

***Fuente: Autor***

| EVENTOS | DESCRIPCION |
|---|---|
| EVENTO 1 | Sobrecarga de tráfico en la red IoT |
| EVENTO 2 | Interrupción del servicio de acceso |
| EVENTO 3 | Intentos de intrusión |
| EVENTO 4 | Robo de credenciales de acceso |
| EVENTO 5 | Explotación de vulnerabilidades |
| EVENTO 6 | Fallos en la actualización del firmware |
| EVENTO 7 | Sniffing de tráfico en la red |
| EVENTO 8 | Uso de claves débiles en la encriptación |
| EVENTO 9 | Ataques de fuerza bruta |
| EVENTO 10 | Acceso no autorizado a áreas restringidas |
| EVENTO 11 | Desconfiguración de permisos |
| EVENTO 12 | Manipulación de registros de acceso |
| EVENTO 13 | Eliminación no autorizada de registros |
| EVENTO 14 | Modificación no autorizada de datos |
| EVENTO 15 | Inyección de datos maliciosos |
| EVENTO 16 | Ataques durante el proceso de actualización |
| EVENTO 17 | Descarga de firmware malicioso |
| EVENTO 18 | Daños físicos a los dispositivos IoT |
| EVENTO 19 | Condiciones climáticas adversas |
| EVENTO 20 | Escaneo de Red Rutinario |

***Tabla 3: Eventos y descripción para la matriz de riesgos***

***Fuente: Autor***

## 4.5 Clasificación de riesgos

Los riesgos en ciberseguridad se refieren a la posibilidad que suceda un evento no deseado con impacto negativo en la seguridad de información, sistemas informáticos o en las operaciones de una organización. La gestión de riesgos en ciberseguridad implica identificar, evaluar y mitigar estos riesgos de manera proactiva para proteger la infraestructura de TI y los activos digitales de una organización.

Para obtener el resultado de los riesgos si es tolerable, aceptable o alto, se realizará una tabla donde se coloquen los eventos de la tabla 3 referenciada con las 7 vulnerabilidades encontradas añadiendo el grado de impacto y el de probabilidad según el detalle de lo que contiene cada nivel como se indica a continuación:

El nivel alto es el de mayor impacto para la seguridad del sistema y la continuidad del servicio ante amenazas críticas que causan daños graves al explotar o aprovechar las vulnerabilidades intrínsecas en una red.

El nivel medio es un riesgo moderado y podría afectar la seguridad o la funcionalidad del sistema como amenazas menos sofisticadas pero que aún pueden ser efectivas y que a su vez pueden causar daños limitados y temporales.

El nivel bajo es un riesgo que generalmente tienen un impacto limitado o son de baja probabilidad como amenazas comunes y conocidas que pueden causar daños mínimos y temporales como por ejemplo intentos de escaneo o exploración. A continuación, mediante un cuadro se detalla cuáles son estas vulnerabilidades con su respectivo riesgo.

| VULNERABILIDADES | Descripción | PROBABILIDAD | CONSECUENCIA | NIVEL DE RIESGO | CALIFICACION |
|---|---|---|---|---|---|
| Cloud Metadata Potentially Exposed | Sobrecarga de tráfico en la red IoT | ALTA | MAXIMO | Riesgo extremo | 12 |
| Cloud Metadata Potentially Exposed | Interrupción del servicio de acceso | ALTA | MAXIMO | Riesgo extremo | 12 |
| Cloud Metadata Potentially Exposed | Intentos de intrusión | ALTA | MAXIMO | Riesgo extremo | 12 |
| Missing Anti-clickjacking Header | Robo de credenciales de acceso | ALTA | MAXIMO | Riesgo extremo | 12 |
| Cloud Metadata Potentially Exposed | Explotación de vulnerabilidades | ALTA | MAXIMO | Riesgo extremo | 12 |
| Private IP Disclosure | Fallos en la actualización del firmware | MEDIA | MODERADO | Riesgo tolerable | 4 |
| Cloud Metadata Potentially Exposed | Sniffing de tráfico en la red | ALTA | MAXIMO | Riesgo extremo | 12 |
| Missing Anti-clickjacking Header | Uso de claves débiles en la encriptación | MEDIA | MODERADO | Riesgo tolerable | 4 |
| Vulnerable JS Library | Ataques de fuerza bruta | ALTA | MAXIMO | Riesgo extremo | 12 |
| Missing Anti-clickjacking Header | Acceso no autorizado a áreas restringidas | ALTA | MODERADO | Riesgo extremo | 6 |
| Missing Anti-clickjacking Header | Desconfiguración de permisos | MEDIA | MODERADO | Riesgo tolerable | 4 |
| Missing Anti-clickjacking Header | Manipulación de registros de acceso | MEDIA | MODERADO | Riesgo tolerable | 4 |
| Missing Anti-clickjacking Header | Eliminación no autorizada de registros | ALTA | MAXIMO | Riesgo extremo | 12 |
| Missing Anti-clickjacking Header | Modificación no autorizada de datos | MEDIA | MODERADO | Riesgo tolerable | 4 |
| Content Security Policy (CSP) | Inyección de datos maliciosos | ALTA | MAXIMO | Riesgo extremo | 12 |
| Private IP Disclosure | Ataques durante el proceso de actualización | MEDIA | MAXIMO | Riesgo extremo | 8 |
| Private IP Disclosure | Descarga de firmware malicioso | ALTA | MAXIMO | Riesgo extremo | 12 |
| No existe vulnerabilidad | Daños físicos a los dispositivos IoT | ALTA | MAXIMO | Riesgo extremo | 12 |
| No existe vulnerabilidad | Condiciones climáticas adversas | ALTA | MAXIMO | Riesgo extremo | 12 |
| Private IP Disclosure | Escaneo de Red Rutinario | BAJA | MENOR | Riesgo aceptable | 1 |

***Tabla 4: Evaluación del impacto y la probabilidad según las vulnerabilidades encontradas***

***Fuente: Autor***

| Vulnerabilidades | Riesgo |
|---|---|
| Cloud Metadata Potentially Exposed | Extremo |
| Content Security Policy (CSP) | Tolerable |
| Missing Anti-clickjacking Header | Tolerable |
| Vulnerable JS Library | Tolerable |
| Private IP Disclosure | Aceptable |
| Server Leaks Version Information Via "Server" HTTP response Header Field | Aceptable |
| X-Content-Type-Options Header Missing | Aceptable |
| Information Disclosure - Suspicious Comments | Información |
| Modern Web Application | Información |
| User Agent Fuzzer | Información |

***Tabla 5: Vulnerabilidades y riesgos***

***Fuente: Autor***

# CAPITULO V.

# DISEÑO LÓGICO DE SEGURIDAD PARA PROTEGER DISPOSITIVOS IOT

## 5.1 Selección de herramientas de seguridad

Es fundamental adaptar las herramientas de seguridad mencionadas en el capítulo anterior en el diseño de solución que se dará a conocer en este capítulo considerando aspectos de seguridad y privacidad que garantizan un control de acceso eficiente y seguro.

El funcionamiento en conjunto de estas herramientas no solo comprende aspectos técnicos, sino que también incluyen protocolos de seguridad garantizando la protección de la comunicación y la autorización adecuada para acceder a recursos críticos.

El diseño de soluciones para la infraestructura de control de acceso vehicular en los equipos IOT debe tener una combinación equilibrada de estas herramientas con el objetivo de crear entornos seguros y eficientes para los residentes de la urbanización. Los dispositivos utilizados en el diseño de solución para el acceso de control vehicular son fortigate, fortiswitch, fortiNac.

**Fortigate**

Posee un alto rendimiento de red y seguridad de hasta unos 4 Gbps para brindar protección contra amenazas, filtrado de contenidos, inspección SSL/TLS y prevención de pérdida de datos, este equipo protege contra malwares, exploits y sitios web peligrosos que se pueden detectar tanto en el tráfico cifrado como en el no cifrado.


***FIGURA 5.1: FORTIGATE 40F***

***FUENTE:***

***HTTPS://WWW.FORTINET.COM/CONTENT/DAM/FORTINET/ASSETS/DATA-SHEETS/FORTIGATE-FORTIWIFI-40F-SERIES.PDF***

**Fortiswitch**

Este dispositivo un conmutador que ofrece escalabilidad inteligente que puede ser administrado directamente desde un fortigate como un controlador de switch para administrar y configurar desde una sola plataforma y no realizar configuraciones independientes, aunque si lo soporte.

***FIGURA 5.2: FORTISWITCH***

***FUENTE:***

***HTTPS://WWW.FORTINET.COM/CONTENT/DAM/FORTINET/ASSETS/DATA-SHEETS/FORTIGATE-FORTIWIFI-40F-SERIES.PDF***

**FortiNAC**

Proporciona tres pilares de seguridad integral: visibilidad, control y respuesta automatizada. La visibilidad identifica y clasifica todos los puntos de la red, el control garantiza que solo los dispositivos confiables obtengan acceso a la red y las capacidades de respuestas automatizadas hace referencia a la inteligencia que posee Fortinet para identificar una amenaza en tiempo real. Además, cuenta con la flexibilidad para integrar soluciones de seguridad que se puede aplicar en prácticamente todas las industrias por ende los clientes

empresariales aprovechan estas capacidades para monitorear activos, proteger sus redes, puntos finales, datos y usuarios.

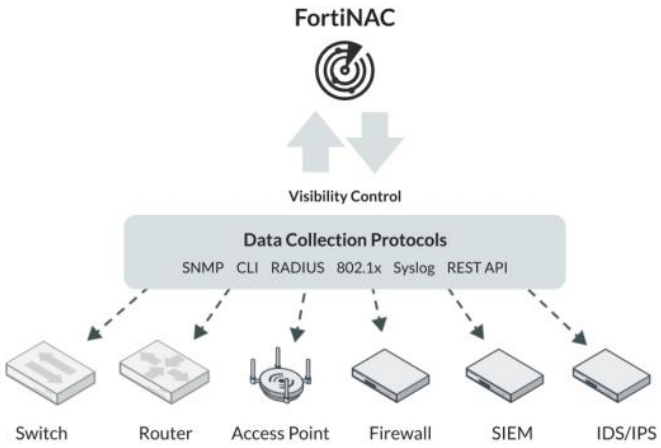



***FIGURA 5.3: FORTINAC***

***FUENTE:***

***HTTPS://WWW.FORTINET.COM/CONTENT/DAM/FORTINET/ASSETS/DATA-SHEETS/FORTINAC.PDF***

FortiNAC utiliza los siguientes métodos para comunicarse y recopilar información de la infraestructura:

- SSH o Telnet a través de CLI se usa comúnmente para completar tareas relacionadas con la infraestructura. Por ejemplo, FortiNAC puede usar SSH para conectarse a un dispositivo y emitir comandos para recopilar información de visibilidad o ejecutar funciones de control.

- FortiNAC utiliza SNMP para descubrir la infraestructura, completar la recopilación de datos y realizar tareas continuas.
- FortiNAC también puede usar RADIUS a través de una conexión por cable o inalámbrica, para recopilar información de visibilidad y controlar el acceso.
- FortiNAC utiliza syslog para mantenerse actualizado sobre los detalles de visibilidad, como la desconexión de hosts mediante alertas de seguridad.
- Dependiendo del proveedor del dispositivo de infraestructura, FortiNAC puede aprovechar las capacidades API disponibles para mejorar la visibilidad y hacer cumplir el control.
- FortiNAC puede usar DHCP, generalmente a través de huellas digitales, para identificar dispositivos conectados y obtener mejoras de visibilidad.

Los métodos de comunicación que utiliza FortiNAC dependen del proveedor y modelo del dispositivo de infraestructura con el que FortiNAC intenta integrarse. Una vez que FortiNAC sabe el tipo de dispositivo con el que se está comunicando, determina y utiliza los métodos y comandos apropiados para recopilar información y mantener el control.

## 5.2 Diseño lógico para proteger dispositivos IOT

En base a la explotación realizada en el capítulo 3 donde se realizó el test de puertos y en el capítulo 4 donde se encuentran vulnerabilidades con sus riesgos, se identifica que la placa raspberry es el elemento más sensible ya que se encuentran muchos eventos que pueden ser vulnerados por motivo de puertos abiertos no seguro a toda la red y en termino de software por la falta de configuración de ciertos parámetros de seguridad en el código.

Estas alertas o factores de inseguridad muestran que la placa raspberry no está siendo protegido de ataques informáticos por elementos de seguridad o dispositivos que ayuden a mitigar vulnerabilidades y amenazas, lo que conlleva a proponer en este capítulo una solución de diseño con dispositivos de seguridad informática para los elementos IOT como se observa a continuación:

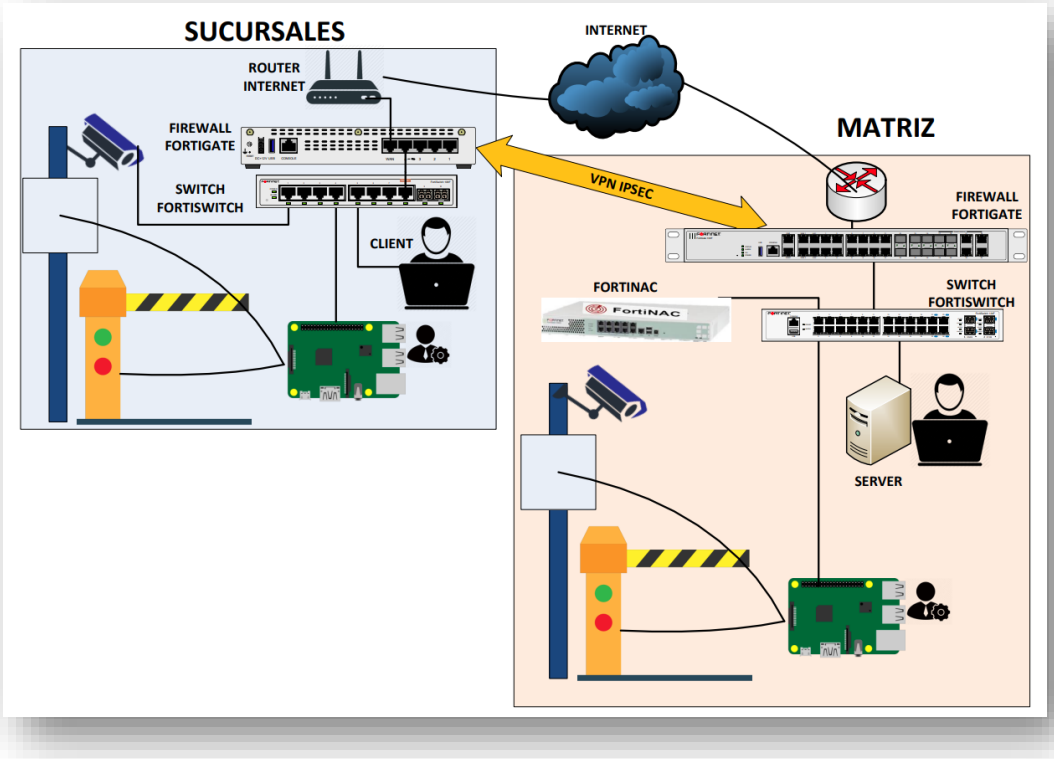



***FIGURA 5.4: ESQUEMA DE SOLUCIÓN PROPUESTA PARA URBANIZACIONES***

***FUENTE: AUTOR***

En este gráfico se observa que el diseño de solución contiene las tres herramientas de seguridad de la marca Fortinet (fortigate, fortiswitch y fortinac) descritos en el punto anterior 5.1 en donde cada elemento cumple un rol importante que se muestran a continuación con más detalle para saber cómo se integran y ayudan con sus características al esquema propuesto:

**Fortigate**

En matriz como en los extremos o sucursales estará conectado a los router de última milla o de los proveedores que brindan servicio de internet y a los cuales se les debe solicitar una ip pública adicional para todos los enlaces, ya que se necesita que cada sucursal llegue a matriz como un enlace de datos. Por ejemplo, la ip que asigne el proveedor de internet, se debe configurar en la interfaz wan del equipo fortigate que está conectada de manera directa al equipo del proveedor.

Las ip pública ingresada a cada sucursal ayudaran a comunicarse entre sí permitiendo armar interconexión entre las sucursales y matriz, ya que el esquema mostrado de solución indica que cualquier paquete de origen enviado desde un dispositivo sea enviado a matriz para que este pueda capturar la trama o el paquete de origen y lo pueda analizar en base a las configuraciones realizadas.

Las configuraciones que se requieren para proteger los dispositivos IOT y establecer conexiones seguras entre matriz y sus sucursales o viceversa se explicaran a continuación:

- ✓ Políticas

En fortigate las políticas son utilizadas para permitir o denegar segmentos de red, host, puertos puedan comunicarse hacia otros segmentos de red, host y puertos mediante parámetros específicos de configuración, por ejemplo, en este caso en particular el raspberry que se encuentra de lado de la sucursal o punto extremo necesita comunicarse con el servidor que está en matriz, pero antes de comunicarse, primero debe pasar el filtro de la política configurada en el fortigate. Esta política debe contener parámetros específicos de configuración y para el ejemplo indicado, los parámetros serían los siguientes:

- Ip origen de la placa raspberry
- Interfaz origen
- Puerto origen de la placa raspberry
- Ip destino del servidor
- Interfaz destino
- Puerto destino del servidor
- Acción que va a tomar la política puede ser “permitir o denegar”, para este caso sería la opción permitir.

A continuación, se observa dos tablas que se debe configurar como filtro de política para permitir la conexión desde la lan de las sucursales hacia los

destinos lan de matriz y viceversa porque de lado del fortigate configurado en matriz también se deben realizas configuraciones de políticas para aceptar peticiones desde la ip o red lan que se encuentra en las sucursales.

| Reglas de Firewall. | IP Origen (Sucursal) | IP de Destino (Matriz) | Puertos a permitir. | Acción (Permitir/Denegar) |
|---|---|---|---|---|
| **Rule 1** | Ips de la Lan de la sucursal | Ips de la Lan de la matriz | 443 , 8080 más los puertos de cámaras | **Permitir** |

***Tabla 6 : Política de salida en el fortigate de la sucursal***

***Fuente: Autor***

| Reglas de Firewall. | IP Origen (Matriz) | IP de Destino (Sucursal) | Puertos a permitir. | Acción (Permitir/Denegar) |
|---|---|---|---|---|
| **Rule 1** | Ips de la Lan de matriz | Ips de la Lan de la sucursal | 443 , 8080 más los puertos de cámaras | **Permitir** |

***Tabla 7 : Política de entrada en el fortigate de la sucursal***

***Fuente: Autor***

- ✓ **Tunel Ipsec**

La VPN IPsec o túnel Ipsec utiliza el protocolo de seguridad de internet (IPsec) que opera en la capa de red del modelo OSI. Este protocolo permite crear

túneles cifrados en Internet que para proteger los datos transmitidos entre redes privadas.

Para armar la conexión entre túneles y que la información viaje cifrada, se debe configurar dos fases las cuales conllevan ciertos parámetros que se deben realizar para que la negociación entre ambos puntos: sucursal y matriz o viceversa puedan trasladas la información encriptada.

En el esquema propuesto se visualiza una flecha de color naranja denominada IPSEC para indicar que se requiere armar la conexión de manera encriptada entre matriz y sucursal, es decir la información que viajará entre estos dos puntos será cifrada mediante parámetros o fases configurables a aplicar de la siguiente forma:

| Propiedades del Tunnel. | | SUCURSAL | MATRIZ |
|---|---|---|---|
| Phase 1 | **Authentication Method (PSK)** | Definir contraseña | Definir contraseña |
| | **IKE Version.** | 1 | 1 |
| | **Diffie-Hellman Group** | Group2 | Group2 |
| | **Encryption Algorithm** | AES256 | AES256 |
| | **Hashing Algorithm** | SHA-1 | SHA-1 |
| | **Keylife (for renegotiation)** | 86400 segundos. | 86400 segundos |

| | | | |
|---|---|---|---|
| Phase 2 | **Nat Trasnversal** | Activo, por defecto.<br><br>*Nota: Considerar la activación de Puerto ÚDP4500 para la comunicación entre los firewalls.* | Activo, por defecto. |
| | **Dead Peer Detection.** | Activo. | Activo |
| | **Encryption Algorithm** | AES256 | AES256 |
| | **Authentication Algorithm** | SHA-1 | SHA-1 |
| | **Perfect Forward Secrecy** | NO PFS | NO PFS |
| | **Lifetime (for renegotiation)** | 86400 sec. | 86400 sec. |

***Tabla 8 : Fases de configuración VPN IPSEC***

***Fuente: Autor***

- ✓ **Filtrado de tráfico**

Se debe agregar a las políticas el filtro de Sistema de Prevención de Intrusiones o también conocido en su abreviatura IPS que tiene como objetivo analizar el tráfico de red en busca de patrones y firmas asociadas con exploits y ataques conocidos para después tomar medidas de bloqueo o prevención de explotación de vulnerabilidades.

**Fortiswitch**

Este equipo reemplaza los switches de capa 2 utilizados en la red actual del cliente para interconectar al fortigate y FortiNAC con los dispositivos finales como son las cámaras, barra vehicular y la placa controladora.

Para poder administrar y configurar los switches, se utiliza el protocolo fortilink uniéndolo al fortigate para que este lo controle, es decir los switches ya no funcionan de manera autónoma porque dependerán del fortigate.

Cuando el switch pasa a ser controlado por el fortigate, el fortigate administra el switch y podrá configurar los puntos comunes que se tiene en cualquier marca de switch administrable como indica en la tabla 8.

Adicional a las configuraciones comunes que permite el controlador de fortiswitch también se agregan nuevas características en términos de seguridad mostrados en la tabla 9 y que serán muy útil para prevenir riesgos de seguridad referente a equipos IOT.

| Definición de Hostname |
| --- |
| **Definición de niveles de permiso de Usuarios** |
| **Configuración de acceso por SSH (único permitido)** |
| **Configuración de Port Security** |

| Configuración de IP de administración |
| --- |
| Configuración de puertos en Trunk |
| Configuración de puertos en Access |
| Asignación de VLAN a puertos de cliente |
| Configuración de segmentos de red (VLANS) |

***Tabla 9 : Configuraciones de switch de capa 2***

***Fuente: Autor***

| Habilitación de la detección de dispositivos asistida por red |
| --- |
| Detección de dispositivos de voz |
| Control de acceso a la red FortiSwitch |
| Cuarentenas |
| Bloquear el tráfico intra-VLAN |

***Tabla 10 : Configuraciones adicionales de fortiswitch***

***Fuente: Autor***

**FortiNAC**

El fortinac como indica el diseño, solo está en el punto concentrador conectado al fortigate que es el encargado de conectar con las sucursales o extremos y en la cual será de gran ayuda para recopilar información de la red.

Para obtener la visibilidad de todos los dispositivos de la red, se crean contenedores dentro de la opción Network para descubrir dispositivos usando protocolos de comunicación como SNMP y SSH.

Además, se debe crear grupos para rangos de puertos físicos que nos ayudará a posterior gestionar de manera fácil un evento de seguridad, por ejemplo, para el caso de las cámaras, se crea un grupo catalogado cámaras donde se incluya todos los puertos que contengan dicha descripción puesta por el FortiNAC cuando realizo el descubrimiento indicado en el párrafo anterior.

Mediante esta herramienta se indica que ciertas macs puedan recibir actualizaciones y otras no mediante el campo vendor OUIS que se encuentra en la opción Network, para este caso se permite que solo las cámaras se actualicen cuando lo requiera, por lo contrario, no se permie paquetes de actualización a la placa base encargada de administrar los equipos OT.

## 5.3 Gestión de incidentes de seguridad y registro de eventos

La gestión de incidentes de seguridad y el registro de eventos son aspectos críticos en un proyecto de ciberseguridad para proteger equipos IoT (Internet de las cosas). Existen algunas buenas prácticas que permiten que estos procesos se den de la mejor manera.

**Monitorización Continua:**

Se debe implementar sistemas de monitorización continua para supervisar el tráfico y la actividad en los dispositivos IOT. Utilizar herramientas de detección de anomalías para identificar patrones inusuales o comportamientos sospechosos.

**Registros de Eventos Seguros:**

Establecer un sistema robusto de registro de eventos que capture y almacene información detallada sobre las actividades en los dispositivos IOT que incluyan registros de autenticación, cambios de configuración y cualquier otro evento relevante para la seguridad.

**Detección de Intrusiones:**

Implementar sistemas de detección de intrusiones (IDS) específicos para IOT ya que estos sistemas pueden identificar patrones de tráfico malicioso o intentos de acceso no autorizado a los dispositivos.

**Respuesta Rápida a Incidentes:**

Desarrollar un plan de respuesta a incidentes que especifique los pasos a seguir en caso de detectar una amenaza. Definir roles y responsabilidades, y asegurarse de que el equipo esté preparado para responder de manera rápida y eficiente.

**Análisis Forense:**

Implementar capacidades de análisis forense para investigar incidentes de seguridad. Esto incluye la capacidad de revisar registros históricos, identificar la causa raíz de un incidente y recopilar evidencia para acciones legales, si es necesario.

**Seguridad en la Configuración:**

Se debe asegurar de que los dispositivos IOT estén configurados de manera segura desde el principio. Deshabilitar servicios no necesarios, utilizar contraseñas fuertes y aplicar actualizaciones de seguridad de forma regular.

**Actualizaciones y Parches:**

Establecer un proceso para gestionar y aplicar actualizaciones y parches de seguridad de manera regular. Los dispositivos IOT deben contar con las últimas correcciones de seguridad para mitigar posibles vulnerabilidades.

**Colaboración con Proveedores:**

Trabajar estrechamente con los proveedores de los dispositivos IOT para obtener información sobre posibles vulnerabilidades y parches. Mantener una comunicación activa para garantizar la seguridad de los dispositivos en todo momento.

**Capacitación del Personal:**

Proporcionar formación continua al personal involucrado en la gestión de la seguridad para asegurar de que estén al tanto de las últimas amenazas y mejores prácticas de seguridad.

**Cumplimiento Normativo:**

Se debe asegurar de cumplir con las normativas y estándares de seguridad pertinentes en el ámbito de los dispositivos IOT. Esto puede incluir regulaciones específicas de la industria y estándares de seguridad reconocidos internacionalmente.

Para implementar estas buenas prácticas se debe fortalecer la seguridad de los equipos IOT y facilitar una respuesta efectiva en caso de que ocurran los incidentes de seguridad.

# CONCLUSIONES Y RECOMENDACIONES

**Conclusiones:**

1. La evaluación de riesgos y vulnerabilidades permite identificar accesos no autorizados, y ataques de denegación de servicio. La evaluación detallada de estos riesgos es crucial para desarrollar estrategias efectivas de mitigación.

2. La importancia del diseño de los sistemas de control de acceso vehicular debe incorporar medidas de seguridad desde el principio. La implementación de prácticas de diseño seguro, como la encriptación de datos y la autenticación robusta, es fundamental para proteger los equipos IOT de posibles amenazas.

3. La implementación de un sistema de monitoreo continuo es esencial para detectar actividades sospechosas y responder a incidentes de manera oportuna. Los mecanismos de respuesta rápida pueden minimizar el impacto de un posible ataque o brecha de seguridad.

4. La capacitación de los residentes y administradores de las urbanizaciones en prácticas de seguridad cibernética es crucial. La conciencia sobre las amenazas y las mejores prácticas para mantener la seguridad ayuda a prevenir errores humanos que podrían comprometer la seguridad del sistema.

5. Los sistemas de ciberseguridad deben mantenerse actualizados para protegerse contra nuevas amenazas. Las actualizaciones regulares de firmware y software, así como la revisión periódica de las políticas de seguridad, son esenciales para mantener la integridad del sistema.

6. La seguridad es un proceso continuo y es fundamental realizar evaluaciones periódicas del sistema y ajustar las medidas de seguridad en función de las nuevas amenazas y desafíos emergentes. La mejora continua garantiza que el sistema se mantenga eficaz y resiliente.

**Recomendaciones:**

1. Identificar posibles amenazas y vulnerabilidades específicas para el control de acceso vehicular en urbanizaciones. Considera ataques como interceptación de comunicaciones, manipulación de datos y acceso no autorizado.

2. Evaluar el impacto potencial de cada amenaza en la seguridad del sistema y la privacidad de los residentes e implementar una red segmentada para separar los dispositivos IOT del resto de la red corporativa o doméstica.

3. Utilizar métodos de autenticación robustos para el acceso al sistema de control de acceso vehicular y asegurarse de que todos los datos que se transmiten entre los dispositivos IOT y los sistemas centrales estén cifrados usando protocolos seguros.

4. Proteger los datos almacenados en los dispositivos y servidores mediante cifrado para prevenir el acceso no autorizado, establecer un plan para aplicar actualizaciones y parches de seguridad regularmente a los dispositivos y software del sistema.

5. Proporcionar formación y recursos educativos para los usuarios sobre prácticas seguras y cómo identificar posibles amenazas y a su vez realizar campañas de concientización para resaltar la importancia de la seguridad en los dispositivos y efectuar un plan de ciberseguridad para el control de acceso vehicular en urbanizaciones garantizará que el sistema sea seguro, confiable y capaz de proteger a los residentes de posibles amenazas.

# BIBLIOGRAFÍA

[1] W. López Garzón y J. Cárdenas López, «Tecnología internet of things (IoT) y el big data», *Mare Ingenii*, vol. 1, n.º 1, pp. 73-79, abr. 2019, doi: 10.52948/mare.v1i1.183.

[2] J. García Gallego, «Implementación de mecanismos de control y seguridad en una red corporativa basados en el software Fortinac», PhD Thesis, Universitat Politécnica de València, 2023.

[3] J. M. Montes Larios y M. A. Iturrizaga Hernández, «Diseño de arquitectura de seguridad perimetral para una empresa dedicada a la actividad inmobiliaria», 2015.

[4] B. A. Hernández y D. P. Ortiz Galeano, «Análisis general del enfoque IOT en redes», PhD Thesis, Editorial Universitaria San Mateo, 2019.

[5] R. C. Motta, K. M. de Oliveira, y G. H. Travassos, «On Challenges in Engineering IoT Software Systems», en *Proceedings of the XXXII Brazilian Symposium on Software Engineering*, en SBES '18. New York, NY, USA: Association for Computing Machinery, 2018, pp. 42-51. doi: 10.1145/3266237.3266263.

[6] M. Alhawamdeh y R. Tahboub, «Enabling Security as a Service for IoT Emerging Technologies: A Survey», en *The 7th Annual International Conference on Arab Women in Computing in Conjunction with the 2nd Forum of Women in Research*, en ArabWIC 2021. New York, NY, USA:

Association for Computing Machinery, 2021. doi: 10.1145/3485557.3485582.

[7] A. Jabbari y C. Fung, «A Secure Cloud-Based Video Recording and Sharing Scheme for Home Security Applications», en *2023 Zooming Innovation in Consumer Technologies Conference (ZINC)*, 2023, pp. 154-159. doi: 10.1109/ZINC58345.2023.10174147.

[8] O. Almazrouei, P. Magalingam, M. Kamrul Hasan, M. Almehrzi, y A. Alshamsi, «Penetration Testing for IoT Security: The Case Study of a Wireless IP Security CAM», en *2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC)*, 2023, pp. 1-5. doi: 10.1109/ICAIC57335.2023.10044176.

# ANEXOS

| Características |
|---|
| 1/3 "CMOS |
| 5MP a 15 fps |
| Lente motorizada de 2.8 ~ 12 mm |
| Soporte H.265 + / H.265 |
| WDR verdadero |
| Rango IR de hasta 98 pies (30m) |
| Hik-Connect |
| DC12V / PoE |

***Tabla 11: Características de Cámara Hikvision***

***Fuente: Autor***

| **Especificaciones de Red** | |
|---|---|
| **Protocolos** | IPv4/IPv6, HTTP, HTTPS, 802.1x, Qos, FTP, SMTP, UPnP, SNMP, DNS, DDNS, NTP, RTSP, RTCP, RTP, TCP, UDP, IGMP, ICMP, DHCP, PPPoE |
| **Almacenamiento en Red** | MicroSD/SDHC/SDXC card (256 G) local storage, and NAS (NFS, SMB/CIFS), auto network |

| | |
|---|---|
| | replenishment (ANR) |
| **API** | ISAPI, HIKVISION SDK, third-party management platform, ONVIF profile S,T,G) |
| **Vista en vivo simultaneal** | Up to 20 channels |
| **Nivel de usuario** | Up to 32 users, 3 levels: Administrator, Operator, User |
| **Seguridad** | User authentication (ID and password), MAC address binding, HTTPS encryption, IEEE 802.1x access control, IP address filtering |
| **Cliente** | iVMS-4200, Hik-Connect |
| **Navegador web** | Live view (plug-in allowed) : Internet Explorer 11 Live view (plug-in free) : Chrome 57.0 +, Firefox 52.0 + Local service : Chrome 57.0+, Firefox 52.0 + |

***Tabla 12: Especificaciones de Red de cámara Hikivision***

***Fuente: Autor***

| **Especificaciones Técnicas** | |
|---|---|
| **Procesador** | ARM Cortex-A72 |
| **Frecuencia de reloj** | 1,5 GHz |

| | |
|---|---|
| **Cpu** | VideoCore VI (con soporte para OpenGL ES 3.x) |
| **Memoria** | 1 GB / 2 GB / 4 GB LPDDR4 SDRAM |
| **Conectividad** | Bluetooth 5.0, Wi-Fi 802.11ac, Gigabit Ethernet |
| **Puertos** | GPIO 40 pines 2 x micro HDMI 2 x USB 2.0 2 x USB 3.0 CSI (cámara Raspberry Pi) DSI (pantalla táctil) Micro SD Conector de audio jack USB-C (alimentación) |

***Tabla 13: Especificaciones Técnicas de Raspberry***

***Fuente: Autor***

| **Parámetros de la Interfaz** | |
|---|---|
| **Puerto Gpon** | Clase B+ |
| | Sensibilidad del receptor: -27 dBm |
| | Potencia óptica de sobrecarga: -8 dBm |
| | Longitudes de onda: US 1310 nm, DS 1490 nm |
| | Filtro de bloqueo de longitud de onda (WBF) de G.984.5 |
| | Mapeo flexible entre el puerto GEM y TCONT |
| | GPON: consistente con la Autentificación de SN o de contraseña definida en G.984.3 |
| | FEC bidireccional |

| | |
|---|---|
| | SR-DBA y NSR-DBA |
| | Tipo B (homing-single y dual-homing) |
| **Puerto Ethernet** | Etiquetas VLAN basadas en puertos Ethernet y y eliminación de etiquetas |
| | 1: 1 VLAN, N: 1 VLAN o Transmisión transparente VLAN |
| | QinQ VLAN |
| | Límite en el número de direcciones MAC aprendidas |
| | Aprendizaje de la dirección MAC |
| | Autoadaptativa 10 Mbit / s, 100 Mbit / s o 1000 Mbit / s |
| **Puerto Post** | REN máximo: 4 |
| | Codificación / decodificación G.711A / μ, G.729a / b y G.722 |
| | Modo de fax T.30 / T.38 / G.711 |
| | DTMF |
| | Llamadas de emergencia (con el protocolo SIP) |
| **Puerto USB** | USB2.0 |
| | Almacenamiento de red basado en FTP |
| | Compartir archivos / impresoras basado en |

| | |
|---|---|
| | SAMBA |
| | Función DLNA |
| **WLAN** | IEEE 802.11 b / g / n (2.4G) |
| | IEEE 802.11 a / n / ac (5G) |
| | 2 × 2 MIMO (2.4G y 5G) |
| | Ganancia de antena: 5 dBi |
| | WMM / SSID múltiples / WPS |
| | 2.4G y 5G concurrentes |
| | Velocidad de interfaz WLAN: 300 Mbit / s (2.4G); 867 Mbit / s (5G) |

***Tabla 14: Especificaciones de Huawei***

***Fuente: Autor***

| **Especificaciones** | |
|---|---|
| Interfaz del dispositivo | 8 puertos Gigabit PoE |
| | Indicadores LED |
| Tasa de transferencia de datos | Ethernet 10 Mbps half duplex, 20 Mbps full duplex |
| | Fast Ethernet 100 Mbps half duplex, 200 Mbps full duplex |

| | |
|---|---|
| | Gigabit 2000 Mbps full duplex |
| Rendimiento | Estructura de conmutación |
| | Búfer RAM: 192 KB |
| | Tabla de direcciones MAC 4k de entradas |
| | Jumbo frames 9KB |
| | Tasa de reenvió 7.44 Mpps (tamaño de paquetes de 64 bytes) |
| Características especiales | Clases de servicio (CoS) 802.1p |
| | Pared aumentable |
| POE | Potencia PoE disponible 65W |
| | Modo PoE A: Pins 1, 2 para alimentación y pins 3, 6 para alimentación |
| Certificaciones | CE |
| | FCC |
| | LVD |
| Temperatura | 00 -40 0C (320 - 104 0F) |

***Tabla 15: Especificaciones Switch Trendnet***

***Fuente: Autor***