# Sistema de seguridad para dispositivos IoT mediante raspberry Pi

Ricardo Castro Valdivia*
Universidad Tecnológica del Centro de Veracruz
Veracruz, Mexico.
*ricardo.castro@utcv.edu.mx*
ORCID 0000-0002-9329-3003

Felipe de Jesús López Álvarez
Universidad Tecnológica del Centro de Veracruz
Veracruz, Mexico.
*20213L001113@utcv.edu.mx*
ORCID: 0009-0001-7085-7566

Maria Reina Zarate Nava
Universidad Tecnológica del Centro de Veracruz
Veracruz, Mexico.
*maria.zarate@utcv.edu.mx*
ORCID: 0000-0003-1469-5504

Ricardo Castillo Tapia
Universidad Tecnológica del Centro de Veracruz
Veracruz, Mexico
*20213L001048@utcv.edu.mx*
ORCID: 0009-0008-9548-6731

Cesar Augusto Pacheco Sánchez
Universidad Tecnológica del Centro de Veracruz
Veracruz, Mexico.
*20213L001017@utcv.edu.mx*
ORCID: 0009-0003-2530-7017

Eva María Landa Huerta
Universidad Tecnologica del Centro de Veracruz
Veracruz Mexico
*eva.landa@utcv.edu.mx*
ORCID: 0002-4665-3985

***Resumen*— En el mundo interconectado de hoy, la creciente amenaza de ciberataques dirigidos a dispositivos IoT en nuestros hogares representa un riesgo significativo para la seguridad y privacidad de las familias. En México, se ha reportado que aproximadamente 25% de los dispositivos IoT han sido expuestos a ciberataques, lo que resalta la urgencia de este tema. Estos ataques pueden resultar en el robo de información confidencial, acceso no autorizado y manipulación de dispositivos. Para abordar este problema, se propone un sistema de seguridad integral para Raspberry Pi diseñado para proteger entornos domésticos.**

***Palabras Clave— IoT, Ciberataques, Seguridad, Privacidad.***

## I. INTRODUCCIÓN

En la actualidad, en un mundo donde la conectividad de dispositivos en nuestros hogares es común, el riesgo en constante crecimiento de ataques cibernéticos dirigidos a dispositivos IoT representa una amenaza latente para la seguridad y la privacidad de nuestras familias. Estos ataques pueden manifestarse de diversas maneras, incluyendo el robo de información confidencial, intrusiones no autorizadas en nuestros dispositivos e incluso la manipulación de los mismos. Con plena conciencia de esta problemática, este proyecto se presenta como un sólido sistema de seguridad diseñado específicamente para la Raspberry Pi, con el propósito de proteger el entorno doméstico.

El prototipo del proyecto se considera un modelo de arquitectura para resguardar dispositivos IoT, desde un enfoque de mecanismos para proteger el acceso a ellos, pero va más allá, al permitir un monitoreo constante de los dispositivos conectados a la red donde se encuentran estos dispositivos IoT. La información que registre tanto el programa de control de acceso FreeRadius, así como Zabbix permitirá aprender patrones y comportamientos en los ataques, mejorando así su capacidad de detección y prevención, lo que a su vez impulsará actualizaciones periódicas para mantenerse a la vanguardia y defenderse de los ciberdelincuentes.

Adicionalmente, la administración de las herramientas que proveen mecanismos de seguridad podrá llevarse a cabo de forma remota, manteniendo una conexión segura, ya que el enlace de comunicación cifrado garantiza la comunicación protegida, minimizando las vulnerabilidades entre el sistema de seguridad y los dispositivos IoT, estableciendo niveles de seguridad fortalecidos contra posibles amenazas.

## II. TRABAJOS RELACIONADOS

A continuación, se describe una recopilación de aspectos importantes de proyectos con características similares al desarrollado por nuestro equipo de trabajo, es de vital importancia mencionar, que estos han sido considerados por la cercanía ya en sea tecnologías utilizadas, proceso de desarrollo, en inclusive por los objetivos iniciales planteados.

Diseño de un sistema de seguridad en el hogar basado en IoT y creación de prototipo [1]. Este Proyecto enfocó los trabajos en el diseño y desarrollo de un sistema para la seguridad del hogar, esencialmente resuelve las necesidades de vigilancia y validación para el control de acceso mediante el uso de dispositivos IoT.

Desarrollo de un firewall con una arquitectura de bajo costo para sistemas de monitoreo y control en redes industriales. [2]. Es un proyecto que considera que los riesgos que actualmente corre la información al ser enviada a sitios de almacenamiento, o procesamiento para la toma de decisiones mediante redes industriales, corre el riesgo de ser robada, alterada e incluso borrada. Identificando esa problemática, el proyecto desarrolla un firewall de monitoreo y control de flujo en tiempo real, donde prevalece el filtrado de paquetes para determinar contenidos propios y separar aquellos que no lo sean.

Diseño e implementación de infraestructura NIDS (Network Intrussion Detection System) para PIMES. [3]. El trabajo consiste en seleccionar, configurar e integrar todos los elementos hardware, software y organizativos para conseguir una solución operativa NIDS contra ataques informaticos.

Home security monitoring system with IoT-based Raspberry Pi. [4]. El sistema de monitoreo de seguridad para el hogar, es un proyecto que dirige sus esfuerzos, para ofrecer una infraestructura de dispositivos IoT que recaban información de factores que ponen en riesgo la seguridad por intrusiones físicas, así como de indicadores de presencia de gas, temperatura, que puedan ocasionar tragedias que desencadenen pérdidas materiales.

A continuación, se muestra la tabla 1, que nos proporciona un concentrado de contenidos que han sido seleccionados al ser una base que ha permitido enriquecer conocimientos, e incluso validar el rumbo propuesto en los objetivos planteados antes de desarrollar el presente proyecto.

Tabla 1. Trabajos consultados.

| Trabajo de investigación | Problemática | Contribución |
|---|---|---|
| [1] | Implementar de manera efectiva las tecnologías del Internet de las Cosas (IoT) en un sistema de seguridad. | Implementación de tecnologías IoT en seguridad, para contribuir a explorar y demostrar cómo estas tecnologías tienen aplicaciones significativas en la vida cotidiana. |
| [2] | Vulnerabilidades de las redes industriales actuales, que suelen conectarse directamente a los sistemas administrativos empresariales utilizando sistemas de seguridad convencionales no especializados. | Implementación de políticas empresariales, registro de actividades, biometría para el acceso, sistemas de detección de intrusos, criptografía e implementación de firewalls, reduciendo así la posibilidad de manipulación de información crítica del proceso. |
| [3] | Las PYMES a menudo descuidan la protección de su infraestructura debido a la percepción de que son menos susceptibles a ataques cibernéticos o por el costo asociado con la implementación de medidas de seguridad | Desarrollo de un Sistema de Detección de Intrusos en Red (NIDS), diseñado específicamente para las necesidades y recursos de las PYMES. |
| [4] | De acuerdo a la agencia nacional de estadísticas de indonesia, en 2015, el número de robos y hurtos con violencia contra los hogares registrados fue de 1.628.634. De cada 100.000 personas. Esto debido en parte a que no se cuenta con infraestructura dedicada a la vigilancia y monitoreo. | Creación de una herramienta de sistema de seguridad para el hogar con un Raspberry Pi basado en una red social de mensajería instantánea y comunicación. |

Después de haber realizado el análisis de contenidos relacionados, podemos determinar que la tecnología de una raspberry Pi 5, tiene las características de procesador y memoria RAM, así como los módulos ya integrados para el control de dispositivos IoT ideales y suficientes para el procesamiento y conectividad que se han requerido.

También podemos validar que los diversos proyectos analizados se enfocan hacia la seguridad de las instalaciones y de personas, pero en una gran minoría se observa el enfoque hacia la protección al acceso de los equipos (excepto aquellos proyectos que se enfocan en protección de servidores principalmente), siendo una área de oportunidad que consideramos de suma importancia, la protección de dispositivos IoT, puesto que estos equipos han sido creados para cumplir con una funcionalidad específica, sin embargo podemos mencionar que presentan aun debilidades, en el rubro para el control de acceso a su administración.

Implementar un sistema de seguridad basado en una Raspberry Pi en entornos domésticos, no solo mejora la protección de los dispositivos IoT, sino que también brinda entornos gráficos para su facilidad de uso. La Raspberry Pi es conocida por su accesibilidad y simplicidad, permitiendo que incluso usuarios con poca experiencia técnica, e incluso capacitación básica, puedan configurar y gestionar el sistema de seguridad, además que su interfaz intuitiva y la abundancia de recursos de consulta en línea hacen que la instalación y el mantenimiento sean tareas de fácil aprendizaje.

Los hogares y los entornos empresariales se enfrentan a un creciente número de ciberataques dirigidos a dispositivos IoT, que incluyen desde cámaras de seguridad hasta electrodomésticos inteligentes. Estas vulnerabilidades pueden resultar en la invasión de la privacidad, el robo de datos personales y, en algunos casos, el control no autorizado de los dispositivos. Un sistema de seguridad basado en Raspberry Pi puede mitigar estos problemas al proporcionar una capa adicional de defensa, detectando y previniendo eficazmente intentos de acceso no autorizado y comportamientos sospechosos en la red.

Una de las características más atractivas del sistema basado en Raspberry Pi, que se describe en este proyecto, es la flexibilidad, ya que permite adaptarlo a las necesidades específicas de cada hogar. Los usuarios pueden personalizar las configuraciones de seguridad para proteger una variedad de dispositivos IoT, asegurando así una protección integral y ajustada a sus requerimientos individuales. Esta capacidad de adaptación facilita la integración del sistema de seguridad en la rutina diaria, proporcionando tranquilidad y permitiendo a las familias disfrutar de la tecnología sin preocuparse por posibles amenazas cibernéticas.

## III. DISEÑO DE ARQUITECTURA

La arquitectura del sistema mostrado en la fig. 1, se determinó después de definir los requisitos funcionales y no funcionales, asegurando la compatibilidad con el hardware seleccionado. La planificación del sistema incluye la especificación detallada de los componentes y los entornos de configuración necesarios, esto abarca tanto los diseños lógicos como los físicos, que son esenciales para la implementación efectiva del sistema de seguridad.

Se resalta la importancia de trabajar con un enfoque iterativo para el diseño de la arquitectura, lo que permitió una visión clara y coherente del proyecto global. Esta fase incluyó la creación de diagramas de bajo nivel que identifican los diferentes módulos y componentes del sistema de seguridad. Estos diagramas detallan las interacciones entre los elementos, los flujos de datos y las interfaces de configuración facilitando la comunicación, la planificación y el diseño.

La instalación y configuración del sistema operativo Raspbian, en la Raspberry Pi 5 permitió la disposición de un elemento clave en el desarrollo del proyecto, considerando este, el principal componente de la infraestructura determinada. Lo anterior incluyó la descarga de la imagen del instalador y la validación de la compatibilidad dispositivo-sistema operativo, asegurando la configuración de parámetros

de red, así como la configuración del protocolo SSH para comunicación remota eficiente.

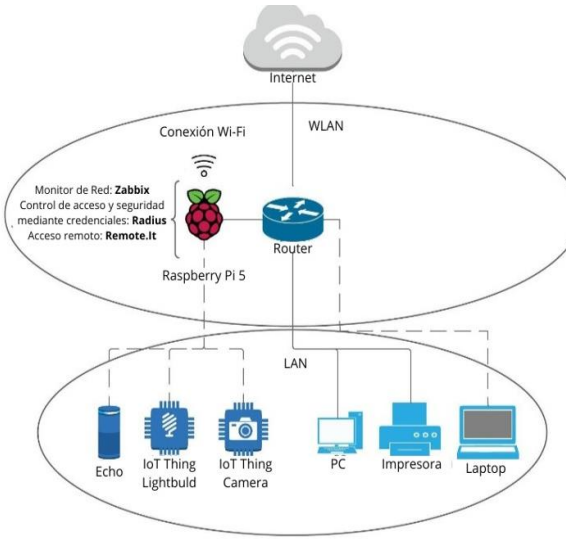



Fig. 1 Diseño de la Arquitectura Fase 1

Descripción de la Arquitectura:

- En el primer nivel, tenemos la conexión a Internet con el router de nuestro proveedor de Internet.
- Segundo nivel, tenemos la Raspberry Pi conectada directamente al router para asegurarnos que tenemos una conexión al exterior y al resto de la red LAN. La ubicación de la raspberry Pi permite implementar mecanismos de seguridad y monitoreo que la protegen y a los dispositivos IoT que le conectemos.
- En el tercer nivel, se observan todos los dispositivos relacionados con las conexiones, tanto IoT conectados a la Raspberry Pi, así como los dispositivos finales (PC, móviles, portátiles e impresoras) conectados al Router.

## IV. CASO DE ESTUDIO.

La implementación del prototipo para efectos de prueba se realizó en 2 entornos:

- La Fig. 2. Muestra un primer caso en las Instalaciones de la Universidad Tecnológica del centro de Veracruz.
- La Fig. 3. Muestra un segundo caso, donde se muestra la implementación en una ubicación doméstica.

En ambos casos se interconectó la raspberry Pi mediante cableado de red a dispositivo router, una computadora laptop conectada de forma inalámbrica a la raspberry Pi para ejecutar el entorno de administración del S.O., Una 2da computadora laptop conectada de forma inalámbrica al router para ejecutar el entorno de administración de la herramienta de monitoreo y seguridad. La raspberry Pi mantiene comunicación inalámbrica a una cámara IP, un foco LED Wi-Fi y una bocina inteligente controlada mediante voz. La finalidad de hacerlo en diferentes entornos fue evaluar variaciones en características de los dispositivos proveídos por el ISP que brinda el servicio de conexión a internet, considerando diferentes marcas de fabricantes de estos dispositivos.

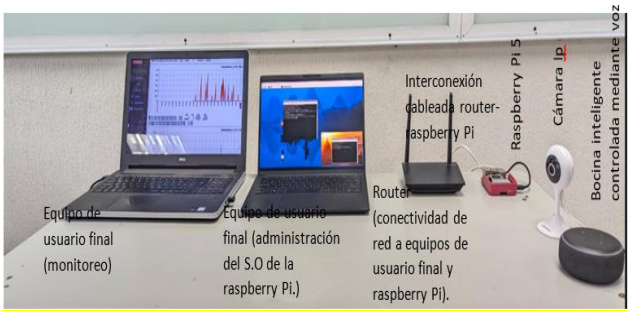



Fig. 2. Interconexión de prototipo de proyecto en instalaciones de la Universidad Tecnológica del Centro de Veracruz.

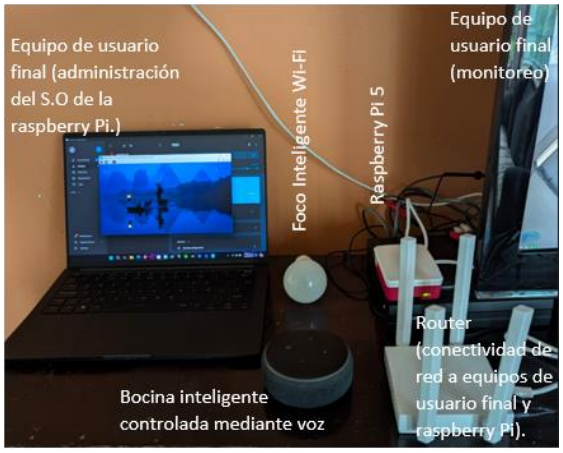



Fig. 3. Interconexión de prototipo de proyecto en ubicación doméstica.

Durante el desarrollo del proyecto se tomó de referencia la metodología PPDIOO, que nos proporcionó un enfoque estructurado y sistemático, asegurando una implementación exitosa y una gestión efectiva a lo largo del ciclo de vida del proyecto.

Se compone de las siguientes fases:

Prepare, Plan, Design, Implement, Operate y Optimize. [6]

Este modelo es apropiado para el trabajo operativo en redes debido a sus características secuenciales, ya que divide claramente las diferentes etapas del ciclo de vida, y su naturaleza iterativa, que permite una retroalimentación constante. A continuación, se muestra el proceso de trabajo y evidencias correspondientes. [7]

1.- Una de las actividades esenciales fue realizar un análisis detallado de los requisitos de hardware y software necesarios para la implementación del proyecto, ello derivó que se seleccionaran: Raspberry Pi5 con el sistema operativo Raspbian OS de 64 bits, una tarjeta micro SD de 128Gb, una cámara IP, una bocina inteligente controlada mediante voz, un foco LED Wi-Fi, un dispositivo router con conexión a internet y disponibilidad de puerto cableado.

2.- En la elección del gestor de la base de datos para almacenar la información de autenticación de los dispositivos IoT en el hogar, se tomó en cuenta, la compatibilidad, consumo de

recursos y robustez. El script de base de datos se desarrolló como un componente para proporcionar una estructura organizada y eficiente para almacenar y gestionar la información de los dispositivos mediante MariaDB, lo que permitirá su adaptación a futuras expansiones y actualizaciones del sistema de seguridad. La Fig. 4 muestra el script que define la estructura de la base de datos "sistema_de_seguridad_iot", que se utiliza en el proyecto de seguridad para dispositivos IoT, consta de dos tablas principales “Dispositivos de IoT” y “Usuarios”.

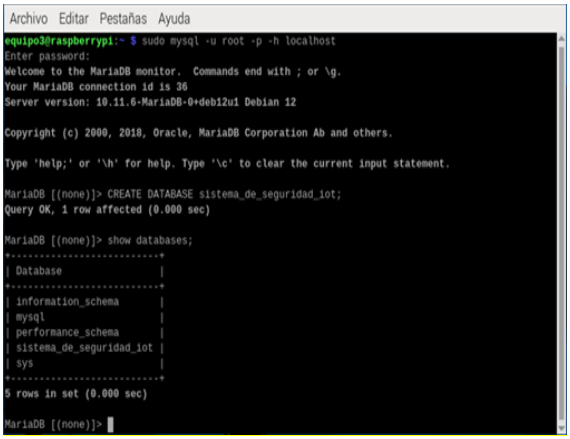



Fig. 4 script que define la estructura de la base de datos "sistema_de_seguridad_IoT",

En la Fig. 5, se muestra los campos y atributos correspondientes a una de las tablas mencionadas. La información registrada en esta base de datos nos sirve para tener identificados los dispositivos que son parte de la red, desde el punto de vista que son aquellos mismos que estarán autenticados por la herramienta FreeRadius habiéndose conectado a la red, pero además coincidiendo con aquellos que se ven reflejados por la herramienta de monitoreo Zabbix

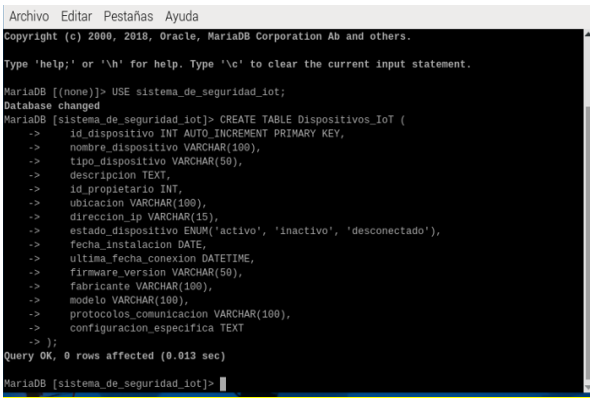



Fig. 5 Campos y atributos de la tabla “Dispositivos_IoT de la B.D.”

3.- Una parte fundamental del prototipo fue la configuración en la raspberry PI como punto de acceso Wi-Fi Hotspot. Primero se estableció conexión mediante cable del router a la raspberry PI y posteriormente se utilizó el módulo de Wi-Fi de la raspberry Pi como trasmisor para la conexión de los dispositivos IoT. En la Fig. 6, se observa la configuración de la red inalámbrica, indicando el nombre de la red del punto de acceso creado, en este caso rasp_ap junto con la seguridad y una contraseña para evitar accesos no autorizados.


Fig. 6. Creación de Wi-Fi Hotspot para interconexión de dispositivos IoT

4.- La configurar el servicio de FreeRadius en la Raspberry Pi 5, proporciona un mecanismo robusto y seguro para la autenticación de usuarios que intentan acceder a la red doméstica, lo que contribuye a prevenir accesos no autorizados y proteger la privacidad de los datos. Además, Free Radius permitió la centralización de la gestión de usuarios y contraseñas, lo que simplificó la administración de credenciales y facilitó la aplicación de políticas de seguridad coherentes en los 3 dispositivos IoT conectados. En la Fig. 7 se muestra el estado activo de Free Radius.

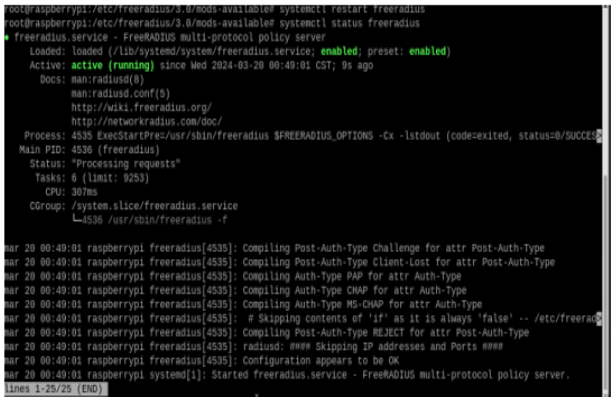



Fig. 7 Comprobación de status de FreeRadius

En la información del reporte mostrado por FreeRadius se observa equipos que trataron de conectarse a la red doméstica, cuantas veces lo intentaron, y si cada intento fue exitoso. En la Fig. 8 se puede visualizar el intento de conexión a la red LAN de los equipos: 20213L001113@utcv.edu.mx, pipe y equipo3, observándose que la única conexión permitida exitosa es para equipo3, que es una conexión autorizada. Esta prueba en esta herramienta, se realiza como una demostración

del control de acceso para equipos que intentan conectarse a la red donde se encuentra la raspberry Pi.

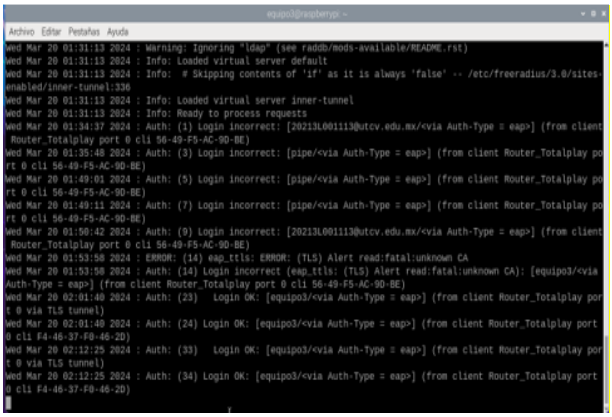
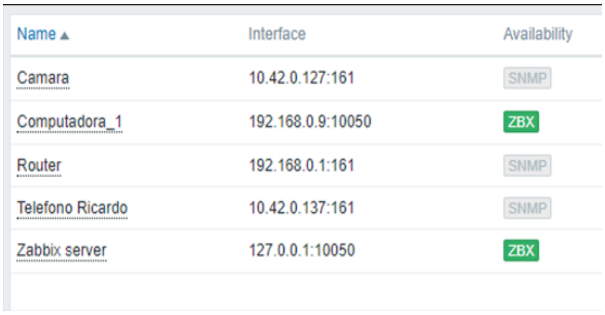


Fig. 8 Verificación de que dispositivos y cantidad de veces se han conectado a la red inalámbrica.

5.- Monitoreo de dispositivos conectados a la red con la herramienta Zabbix, para ello se instaló la aplicación agente cliente que mostró listado de equipamiento en monitoreo,



| Name ▲ | Interface | Availability |
|---|---|---|
| Camara | 10.42.0.127:161 | SNMP |
| Computadora_1 | 192.168.0.9:10050 | ZBX |
| Router | 192.168.0.1:161 | SNMP |
| Telefono Ricardo | 10.42.0.137:161 | SNMP |
| Zabbix server | 127.0.0.1:10050 | ZBX |

Fig. 9 Dispositivos conectados a la red

La implementación de monitoreo nos permitió observar una gráfica, para evaluar de cada dispositivo el estado de sus características técnicas funcionales. En la Fig. 10 se puede observar una gráfica que indica las características funcionales de la laptop conectada a la red LAN.

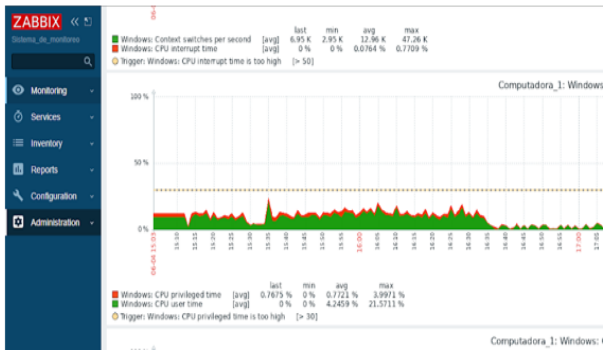



Fig. 10 Grafica del estado de las características técnicas funcionales de uno de los dispositivos conectados a la red.

La implementación de conexión remota a la raspberry Pi, provee de la oportunidad de realizar revisión y administración de configuraciones en tiempo real desde cualquier ubicación, esto da una importante ventaja ya que abre la posibilidad de salir fuera de la cobertura de la red LAN y aun así mantener comunicación con el sistema de seguridad que protege los dispositivos IoT. En la Fig. 11 podemos observar una conexión remota haciendo uso de la herramienta.

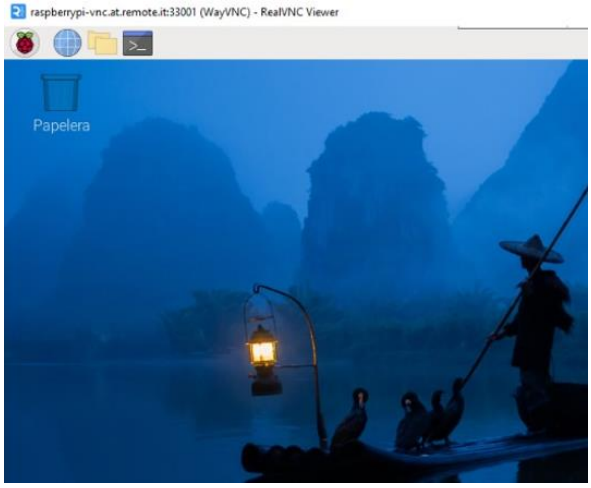



Fig. 11. conexión remota hacia la Raspberry PI. Haciendo uso de la herramienta VNC.

Es muy importante subrayar la importancia de trabajar en un proyecto como el presente con un enfoque estructurado y sistemático para garantizar un diseño, desarrollo, implementación y funcionamiento del prototipo, desde la instalación inicial hasta las pruebas de integración.

Es esencial mencionar que la implementación de este prototipo para el proceso de pruebas ha sido bajo el consentimiento de las personas donde se ha llevado a cabo, teniendo presente con ello el respeto a la privacidad de la información que es parte de una red interna, teniendo como principal motivación la mejora en la seguridad de la administración de sus propios dispositivos IoT. También se consideró una capacitación básica a los responsables para el ingreso de nuevos IoT a la red que ofrece el sistema, así como también el ingreso de aquellos equipos que no lo sean y que solo requieren conectividad para navegación a internet.

## V. CONCLUSIONES Y TRABAJOS FUTUROS

Se propone que uno de los trabajos a futuro sea la generación de reportes de estadísticos apoyándose de las herramientas de monitoreo que permitan determinar el bloqueo inmediato de intrusos habiendo sido identificados como no validos dentro de la red. Una funcionalidad más, que es viable, agregar a este proyecto es el envío de alarmas a un teléfono celular cuando se haya identificado actividad sospechosa, y al tener acceso remoto a la raspberry Pi, se podrá revisar el estado que guarda la red y tomar acciones inmediatas para salvaguardar el acceso y seguridad de los dispositivos IoT.

## RECONOCIMIENTOS

Agradecimiento especial para los profesores de la Carrera de Ingeniería en redes inteligentes y Ciberseguridad de Universidad tecnológica del centro de Veracruz, que de manera continua son parte de la formación académica de generaciones de egresados. También un reconocimiento especial para nuestros padres, que en todo momento nos apoyan en lo económico, así como también en lo motivacional.

## REFERENCIAS

[1] F. Eduardo. Diseño de un sistema de seguridad en el hogar basado en IoT y creación de prototipo, Consultado 22 agosto 2024 en: https://crea.ujaen.es/handle/10953.1/16437. Marzo-2022

[2] O. Naime, J. Henry. Desarrollo de un firewall con una arquitectura de bajo costo para sistemas de monitoreo y control en redes industriales. https://repository.unad.edu.co/jspui/bitstream/10596/20250/9/94453153.pdf . 2018

[3].- Diseño e implementación de infraestructura NIDS (Network Intrussion Detection System) para PIMES. Agra Monte, A. Diseño e implementación de infraestructura NIDS (Network Intrussion Detection System) para PIMES (upv.es) Pag. 24-25. 2017.

[4] I G. Made Ngurah Desnanjaya, I N. Alit Arsana. Home security monitoring system with IoT-based Raspberry Pi. DOI:10.11591/ijeecs.v22.i3.pp1295-1302. Junio 2021

[5] A. Julieth., & A. Stephanny. Metodologías para el desarrollo de proyectos. http://repository.unicatolica.edu.co/handle/20.500.12237/2037. 2020.

[6] A. Rey, W. Eusebio. Rediseño de la arquitectura de red basado en la metodología PPDIOO para la gestión de red de la I.E.P.E. “Mariscal Castilla” El Tambo – Huancayo. http://repositorio.uncp.edu.pe/handle/20.500.12894/7348. 2021

[7] G. Sagñay, M. Antonio. Análisis de vulnerabilidades en redes Ethernet utilizadas para la computación en malla con un Middleware Free Source utilizando la metodología PPDIOO. [masterThesis, Escuela Superior Politécnica de Chimborazo]. http://dspace.espoch.edu.ec/handle/123456789/9441. 2019.

[8] M. Francisco. Desarrollo de una aplicación IoT para el envío de imágenes mediante el protocolo MQTT [Proyecto/Trabajo fin de carrera/grado, Universitat Politècnica de València]. https://riunet.upv.es/handle/10251/152408. 2020

[9] M. del P. Virginia. Ciberataque en dispositivo IOT de reducidas prestaciones [Info:eu-repo/semantics/bachelorThesis]. E.T.S.I. Industriales (UPM). https://oa.upm.es/67591/ . Junio 2021