UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE ELECTRÓNICA Y TELECOMUNICACIONES

TRABAJO DE TITULACIÓN

PROPUESTA TECNOLÓGICA PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

IMPLEMENTACIÓN DE UN LABORATORIO REMOTO ORIENTADO AL DESARROLLO DE PRÁCTICAS DE AUTOMATIZACIÓN INDUSTRIAL PARA LA CARRERA ELECTRÓNICA Y AUTOMATIZACIÓN DE LA UPSE.

AUTORES

JAIME ENRIQUE MENOSCAL SALTOS

LUIS MIGUEL ARAUZ PINELA

CARRERA

ELECTRÓNICA Y TELECOMUNICACIONES

PROFESOR TUTOR

ING. LUIS ENRIQUE CHUQUIMARCA JIMÉNEZ, Mgt.

LA LIBERTAD – ECUADOR

ENERO DE 2023

DEDICATORIA

Dedico el resultado de este trabajo a toda mi familia y amigos. Principalmente a mis padres, quienes me brindaron de su apoyo tanto moral como económico. Gracias por entrenarme desde casa para afrontar desafíos como este y los demás que estén por venir.

También quiero agradecer a mis docentes, quienes compartieron sus conocimientos y experiencias conmigo para formar al profesional al que aspiro llegar a ser, espero que sigan instruyendo a las futuras generaciones de ingenieros e ingenieras que llevaran al país hacia la siguiente etapa con sus buenos valores y ética profesional.

Finalmente, también agradezco a mi novia, María Villon de la Cruz, quien me apoyó y motivó desde el principio para aceptar el desafío de iniciar una carrera de tercer nivel.

Luis Arauz Pinela

El presente trabajo de titulación se lo dedico a mis padres, por su amor, trabajo y ayuda incondicional, y a mis hermanos.

Jaime Menoscal Saltos

AGRADECIMIENTO

Quiero agradecer a mis compañeros y amigos de la carrera, con quienes batallamos juntos para lograr terminarla, estudiando hasta altas horas de la noche, terminado proyectos en grupo hasta la madrugada, gracias a nuestro esfuerzo en conjunto todos nosotros hemos llegado hasta este punto, a un paso de ser ingenieros.

Agradezco a mi compañero de titulación, con quien he trabajado durante varios meses para lograr el presente documento con mucho esfuerzo, espero que ambos logremos el éxito en nuestra vida profesional.

Y, agradezco también a nuestro tutor de tesis, Ing. Luis Chuquimarca, por su paciencia y por estar presto a brindarnos de su ayuda sin importar la fecha o el horario, este proyecto no habría tenido el nivel que tiene sin su colaboración.

Luis Arauz Pinela

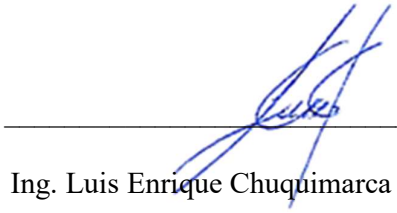
A mi compañero de tesis gracias por el apoyo, y a nuestro tutor Ing. Luis Chuquimarca.

Jaime Menoscal Saltos

APROBACIÓN DEL TUTOR

En calidad de tutor de la propuesta tecnológica con título "Implementación de un laboratorio remoto orientado al desarrollo de prácticas de automatización industrial para la carrera electrónica y automatización de la UPSE", presentado por los señores egresados Menoscal Saltos Jaime Enrique y Arauz Pinela Luis Miguel, ambos estudiantes de la carrera de Electrónica y Telecomunicaciones, me permito declarar que luego de haber orientado, analizado y revisado, es aprobado en todas sus partes.

Particular que informo para los fines consiguientes.



Ing. Luis Enrique Chuquimarca Jiménez, Mgt.
Docente tutor

La Libertad, de marzo de 2023

TRIBUNAL DE GRADO

Ing. Washington Torres Guin, Mgt.
DECANO DE FACULTAD

Ing. José Aquino Sánchez, Mgt.
DIRECTOR DE CARRERA

Ing. Luis Chuquimarca Jiménez, Mgt.
PROFESOR TUTOR

Ing. Luis Miguel Amaya Fariño, Mgt.
DOCENTE ESPECIALISTA

Ab. Luis Castro Martínez, Mgt.
SECRETARIO GENERAL

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA DE ELECTRÓNICA Y TELECOMUNICACIONES

Implementación de un laboratorio remoto orientado al desarrollo de prácticas de automatización industrial para la carrera electrónica y automatización de la UPSE

RESUMEN

La evolución de las telecomunicaciones luego de la pandemia suscitada a finales de 2019 fue notoria, obligando a la población mundial a un nuevo estilo de vida. Un ejemplo claro fue el ámbito laboral y estudiantil, donde fue común encontrar a personas adecuándose a trabajos remotos, teletrabajos y clases virtuales. En época de pandemia, las carreras técnicas fueron las más perjudicadas, dejando a los estudiantes sin acceso a los laboratorios para realizar sus prácticas y privándolos de una educación acorde a las exigencias del mundo laboral. Debido a esto, surgió la propuesta tecnológica titulado "Implementación de un laboratorio remoto orientado al desarrollo de prácticas de automatización industrial para la carrera electrónica y automatización de la UPSE", valiéndose de la tecnología VPN (*Virtual Private Network*) y del protocolo RDP (*Remote Desktop Protocol*) para lograr este objetivo.

El diseño del sistema para el laboratorio de automatización se basa en el uso de tecnologías VPN por medio de un router Mikrotik RB2011 UiAS-2HnD-IN, un servidor local y entre otros servicios, los cuales alojan el aplicativo web que permiten el ingreso controlado de cada usuario a las estaciones de trabajo dentro del laboratorio. Cada estación de trabajo se encuentra previamente adecuada con sus respectivas protecciones eléctricas, de control y su cableado estructurado de red. Además, el estudiante podrá tener acceso a los módulos del laboratorio de automatización como son: computadoras, controladores autómatas programables, variadores de frecuencia, Interfaces Hombre-Máquina, y demás dispositivos que se pudieran adecuar a las necesidades del docente y estudiante, para la realización de prácticas; haciendo uso del protocolo RDP y el túnel VPN, lo cual brindará una conexión optima, segura y controlada, entre el cliente y servidor. Por tanto, el proyecto consta de 4 prácticas desarrolladas de manera remota, que ayudarán al estudiante a obtener conocimientos profesionales en el uso de los controladores autómatas programables, manejo de variables, y redes industriales.

Palabras claves: Laboratorio remoto, VPN, Autómata programable, Prácticas de automatización industrial.

ABSTRACT

The evolution of telecommunications after the pandemic at the end of 2019 was notorious, forcing the world's population to a new lifestyle. A clear example was the work and student environment, where it was common to find people adapting to remote jobs, telecommuting and virtual classes. In times of pandemic, technical careers were the most affected, leaving students without access to laboratories to perform their practices and depriving them of an education according to the demands of the working world. Due to this, the technological proposal entitled "Implementation of a remote laboratory oriented to the development of industrial automation practices for the electronics and automation career at UPSE" was created, using VPN (Virtual Private Network) technology and RDP (Remote Desktop Protocol) to achieve this goal.

The system design for the automation laboratory is based on the use of VPN technologies through a Mikrotik RB2011 UiAS-2HnD-IN router, a local server and other services, which host the web application that allows the controlled access of each user to the workstations within the laboratory. Each workstation is previously equipped with its respective electrical and control protections and structured network cabling. In addition, the student will have access to the automation laboratory modules such as: computers, programmable automaton controllers, frequency variators, Man-Machine Interfaces, and other devices that could be adapted to the needs of the teacher and student, for the realization of practices; making use of the RDP protocol and VPN tunnel, which will provide an optimal, secure and controlled connection between the client and server. Therefore, the project consists of 4 practices developed remotely, which will help the student to obtain professional knowledge in the use of programmable logic controllers, variable management, and industrial networks.

Keywords: Remote laboratory, VPN, PLC, Industrial automation practices.

DECLARACIÓN

El contenido del presente Trabajo de Titulación es de nuestra responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.

Menoscal Saltos Jaime Enrique

Araúz Pinela Luis Miguel

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

En la actualidad, la modalidad hibrida en el ámbito educativo ha ganado mucha popularidad, esto se debe en gran parte a las comodidades de asistir a clases sin la necesidad de movilizarse físicamente a un centro de estudios. Desde los inicios de la pandemia del Covid-19 se presenció una transformación en la manera de comunicarnos y de realizar nuestras actividades diarias, migrándose a un estilo de vida donde el mundo digital y de internet se convirtió en una necesidad de suma importancia. De igual forma, en las universidades mediante los avances en las tecnologías de la información y la comunicación (TIC) y equipos de redes avanzados, han transformado la educación superior, ayudando a resolver estos problemas a través de nuevas formas de actividades prácticas como son realidad aumentada, realidad virtual, y laboratorios remotos, creando así nuevas alternativas para el aprendizaje de los estudiantes.

Con la finalidad de formar estudiantes con conocimientos sólidos en automatización, la Universidad Estatal Península de Santa Elena, cuenta con un espacio físico destinado a la ejecución de prácticas de laboratorio con Autómatas programables, HMI, variadores de frecuencia, etc. Por ende, la experimentación en el laboratorio donde los estudiantes aplican y exploran las técnicas aplicadas a las nuevas tecnologías, a través del desarrollo de trabajos prácticos, obteniendo los resultados de aprendizaje del programa de estudios de la Carrera de Ingeniería en Electrónica y Automatización. Sin embargo, el equipamiento tecnológico actual en el laboratorio solo puede ser utilizado por los estudiantes de forma presencial, sin la posibilidad de acceder a ellos de forma virtual o remota.

En el presente proyecto de titulación, se pretende realizar un sistema conformado por elementos hardware y software con la finalidad de desarrollar un aplicativo web que permite a los docentes y estudiantes, el acceso de forma remota hasta la red interna del laboratorio de automatización, donde pueden hacer uso de los módulos. Por tanto, las herramientas de automatización ofrecidas por el router MikroTik y las facilidades de desarrollo en los softwares libre (Linux, OpenVPN, MariaDB, php, API de MikroTik), logran la puesta en marcha del aplicativo web que sirve como interfaz para la administración de usuarios, el agendamiento y acceso a las estaciones de trabajo.

CAPITULO I

FUNDAMENTACIÓN

1.1 ANTECEDENTES

La pandemia suscitada a finales del año 2019 a nivel mundial provocó una evolución acelerada en el ámbito de las telecomunicaciones. Además, obligó a la población mundial a adaptarse a un nuevo estilo vida, tanto en la forma de relacionarse, como de trabajar, y en el caso de la educación, tuvo que migrar a una modalidad virtual. Según las Naciones Unidas en el año 2020, el COVID-19 provoco la mayor interrupción de la historia en los sistemas educativos, en donde se vieron afectados casi 1.600 millones de alumnos en más de 190 países en todos los continentes, el cierre de escuelas y otros centros de enseñanza, que afectaron al 94% de estudiantes en todo el mundo, y al 99% en países de bajo y mediano ingreso [1].

En tiempo de pandemia las instituciones educativas optaron por la educación virtual y la Universidad Estatal Península de Santa Elena no fue la excepción. Las carreras "Electrónica y Telecomunicaciones" y "Electrónica y Automatización" perteneciente a la Facultad de Sistemas y Telecomunicaciones cuentan con el Laboratorio de Automatización, el cual es un área designada para realizar prácticas de automatización y control, haciendo uso de autómatas programables, y con la modalidad de educación virtual, los estudiantes no tenían acceso a los espacios que brinda la universidad, restringiendo el uso de herramientas cruciales para una formación profesional completa y de calidad.

Los estudiantes al no tener acceso a estos laboratorios de manera presencial optaron por el uso de simuladores para solventar el desarrollo de las prácticas respectivas de las asignaturas. Cabe mencionar que, la instalación de los softwares necesarios para la simulación de prácticas con autómatas programables y plantas industriales, tienen una alta exigencia en cuanto a recursos de hardware, como, por ejemplo, TIA Portal y Factory I/O.

El mercado actual ofrece softwares comerciales para escritorios remotos que cuentan con una vasta gama de opciones, entre los más populares tenemos a AnyDesk y TeamViewer. Estas potentes aplicaciones de software pueden solventar la necesidad de conectarse de manera remota a otra computadora en cualquier parte del mundo, mientras ambos equipos cuenten con una conexión estable a internet. Sin embargo, éstos son softwares de pago, y

en su versión gratuita poseen limitantes para su uso, destacando el límite de tiempo por conexión y la falta control de acceso cuando se cuenta con más de un cliente remoto. Por tanto, es necesario la implementación de un sistema que permita el acceso remoto al laboratorio de automatización, con las debidas normas que permitan la seguridad e integridad en la comunicación entre los usuarios remotos y los módulos del laboratorio. Además, se considera las medidas de seguridad con respecto a protecciones eléctricas de los módulos que estarán en constante uso diario.

1.2 DESCRIPCIÓN DEL PROYECTO

El presente proyecto pretende solventar la necesidad de realizar prácticas de laboratorio de forma presencial por medio de sistema de acceso remoto, el cual estaría compuesto por los siguientes elementos:

1) Aplicación Web
2) Cliente/Servidor Web
3) Infraestructura de red
4) Hardware y Software para la gestión y protección de equipos
5) Guías de Prácticas de programación con Autómatas Programables

Estos elementos serán necesarios para la implementación del sistema que permitirá el acceso al laboratorio. Mediante el protocolo OpenVPN provisto por RouterOS, se quiere establecer la comunicación entre un usuario final y la red interna del laboratorio, donde se llevarán a cabo las prácticas. Posteriormente, se hace uso del protocolo RDP para la conexión remota al servidor de aplicación donde se realizará la programación en los autómatas programables.

1.3 OBJETIVO DEL PROYECTO

1.3.1 Objetivo general

Diseñar e implementar un Laboratorio remoto de automatización industrial para brindar servicios en el desarrollo de prácticas de control de procesos industriales a los estudiantes de la carrera de Electrónica y Automatización mediante el uso de tecnologías VPN y el protocolo RDP en la UPSE.

1.3.2 Objetivos específicos

- Diseñar e implementar un tablero de distribución para la protección de módulos de control y automatización del proyecto de Laboratorio de Automatización remoto.
- Diseñar e implementar un rack de comunicaciones para la ubicación de los equipos de red con su respectivas protecciones eléctricas y cableado estructurado.
- Desarrollar un sistema de red segura basado en tecnologías VPN y utilizando protocolos RDP que permitan una conexión óptima y controlada del estudiante hacia los dispositivos electrónicos del laboratorio de automatización remoto.
- Desarrollar un sistema remoto que adquiera los datos de un sensor y el control de un actuador industrial.
- Implementar una red de procesos industriales utilizando protocolo, estándares y normativas nacionales e internacionales.
- Elaborar prácticas de laboratorio de fácil comprensión y empleo, en las que se aplique técnicas de automatización y control aplicadas a procesos industriales, haciendo uso del sistema remoto.
- Desplegar un aplicativo web en PHP para la administración de los laboratorios remotos y control de acceso.

1.4 JUSTIFICACIÓN

La consolidación de procesos teóricos y técnicas a lo largo del proceso de aprendizaje son de suma importancia, y una forma de hacerlo es realizando pruebas en equipos de laboratorio. El Laboratorio de Automatización de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, es el lugar físico en donde los estudiantes realizan prácticas basadas en aplicaciones reales que se dan en el campo industrial, interactuando directamente con los módulos que utilizaran en su vida profesional.

El presente proyecto de titulación se orienta en brindar una alternativa de acceso remoto para los docentes y estudiantes a los módulos de los laboratorios, haciendo uso de un túnel *Virtual Private Network* (VPN) por medio de un router Mikrotik, el cual nos garantiza seguridad en el intercambio de datos. Además, cada estudiante contará con credenciales únicas para autenticar el enlace con el router Mikrotik, con la finalidad de dar acceso al servidor local que cuenta con una interfaz visual (escritorio remoto) de un computador, que ejecutará el software requerido para la programación del autómata programable.

El uso de softwares remotos comerciales en sus versiones gratuitas, presentan falencias a la hora de la administración y otorgamientos de credenciales a los estudiantes, por lo que, se desarrolló un control de acceso y agendamiento de horarios en un aplicativo web, que se ejecuta sobre un servidor Linux ubicado dentro de las instalaciones del Laboratorio de automatización. Este cumple con la función de "logueo" de usuarios y envío de instrucciones al router Mikrotik para permitir el acceso a los servidores de aplicación.

Adicionalmente, en el desarrollo de sistema se pretende implementar una cámara que permita visualizar en tiempo real, los cambios de estado de los módulos, con ello permitir al docente y al estudiante verificar el buen desarrollo de las prácticas de automatización de procesos, utilizando la infraestructura tecnológica que posee el laboratorio, como son autómatas programables, variadores de frecuencia, sensores, actuadores, etc.

1.5 ALCANCE DEL PROYECTO

El actual proyecto de titulación tiene como alcance la ejecución de prácticas con autómatas programables mediante un servidor de escritorio remoto, con la finalidad de evaluar la destreza del estudiante, para aplicar los conocimientos adquiridos en la asignatura de Automatización Industrial, realizando programación de procesos que cumplan con las normas y estándares mínimos en el campo de la automatización que

demanda el sector industrial en la actualidad. Por lo tanto, se implementa la opción para que los docentes y estudiantes puedan realizar dichas prácticas, mediante la conexión a internet, lo cual permite un acceso remoto a los módulos del Laboratorio de automatización.

1.6 METODOLOGÍA

Este proyecto requiere de la utilización de los tipos de investigación, que se detallan a continuación:

INVESTIGACIÓN APLICADA TECNOLÓGICA

Se trata de probar la viabilidad del uso del software libre para la conexión remota segura a través del protocolo OpenVPN.

INVESTIGACIÓN EVALUATIVA

Reside en la evaluación a los estudiantes con respecto a la consolidación del conocimiento en relación con el manejo y programación de autómatas programables.

1.7 RESULTADOS ESPERADOS

Los resultados esperados para este proyecto son los listados a continuación:

- Se contará con las protecciones eléctricas adecuadas para garantizar el correcto funcionamiento de los equipos dentro del laboratorio
- Se implementará un rack de comunicaciones para organizar los dispositivos de red y peinar el cableado estructurado
- Se brindará una conexión segura y cifrada desde el laboratorio hasta los estudiantes haciendo uso de tecnologías VPN.
- Se obtendrá una red de procesos industriales que cumpla con los protocolos, estándares y normativas tanto nacionales como internacionales, ésta permitirá la correcta conexión de todos los elementos dentro del laboratorio.
- Se obtendrá un sistema de agendamiento que permita el acceso seguro y controlado de los estudiantes hacia el laboratorio.

CAPITULO II

2 LA PROPUESTA

2.1 MARCO CONTEXTUAL

2.1.1 Laboratorios Remotos a nivel mundial

En el ámbito educativo, cuando se presentan situaciones en las que no puede asistir a las aulas de forma física, o cuando el tiempo requerido para realizar las actividades en un laboratorio excede al permitido, tenemos como alternativa a los Laboratorios Virtuales (LV) y a los Laboratorios Remotos (LR). Los LV son aquellos en donde se realizan las prácticas en simuladores que tratan de asimilar una situación real con condiciones determinadas, en cambio en los LR los estudiantes realizan las prácticas en un laboratorio real localizado en algún lugar remoto y lo manipula a distancia a través de internet [2].

Los laboratorios remotos han ido incrementando según avanza la tecnología. Según un estudio realizado entre 2004 y 2006 por un grupo de investigadores de Alemania con la finalidad de conocer la cantidad de LR a nivel mundial, se obtuvo que para 2004 había 70 LR y en 2006 se había incrementado ese número a 120 con acceso remoto [3].

A nivel mundial existen diferentes tipos de laboratorios remotos, en su mayoría dedicados a la enseñanza de temas relacionados con ingeniería. El Instituto Tecnológico de Monterrey cuenta con tres tipos de plataforma para sus clases en modalidad a distancia. MOOC Lab es un laboratorio público y de uso masivo de circuitos y mediciones eléctricas, éste cuenta con 10 estaciones de trabajo con una capacidad de más de 1600 sesiones semanales. La segunda es eLab/TeleLab, un espacio virtual de ingeniería eléctrica, electrónica y mecatrónica, en este espacio remoto pueden trabajar en áreas de instrumentación, circuitos eléctricos, electrónica, maquinas eléctricas, así como automatizaciones, redes industriales, robótica y control. Su tercera plataforma es RemoteLabs, la cual fue exclusivamente diseñada para investigadores y alumnos de posgrado, se trata de un sitio especializado donde los usuarios pueden trabajar y experimentar las áreas de teorías de potencia, electrónica de potencia y motores y generadores eléctricos [4].

Debido al éxito de este tipo de laboratorios, en la actualidad hay empresas que tienen como objetivo brindar el acceso a un laboratorio real a cualquier computadora del mundo, teniendo como requisito una conexión a internet. Una de ellas es LabsLand, una empresa que brinda la posibilidad que el aprendizaje experimental se realice de forma remota

usando laboratorios reales, las posibilidades de aprendizaje van desde laboratorios de física y cinemática hasta laboratorios de radioactividad [5].

Lo que tienen en común estos laboratorios es que, para tener acceso completo a cualquiera de ellos, se requiere de un pago o suscripción, lo cual se retribuye de forma económica, cabe recalcar que algunos laboratorios permiten acceso limitado para pruebas gratuitas y que otros permiten el acceso privilegiado solo a miembros de ciertas instituciones educativas que participan en el desarrollo de los LR.

2.1.2 Laboratorios Remotos en Ecuador

En Ecuador también se cuenta con laboratorios remotos, que en su mayoría son proyectos realizados por universitarios en temas relacionados con titulación de tercer y cuarto nivel. Por mencionar uno de los casos de los temas de titulación, podemos mencionar un laboratorio remoto con Arduino para la realización de prácticas de electrónica en la escuela de sistemas de la Pontificia Universidad Católica del Ecuador realizada en 2017. El proyecto se caracteriza por dotar a los estudiantes de una herramienta integradora que facilite el proceso de enseñanza práctica en las asignaturas afines a la electrónica, dicho instrumento ha sido construido con un microcontrolador Arduino y un microprocesador Raspberry. Como resultado se obtuvo una herramienta confiable, escalable, robusta e interactiva; capaz de manipular remotamente dispositivos electrónicos para realizar la experimentación a través de una interfaz web, a la cual el estudiante accede de forma organizada y controlada [6].

En el área comercial de laboratorios remotos, en Ecuador contamos con la empresa Nodo. Nodo es una empresa dedicada a la provisión y desarrollo de proyectos integrales en las ramas de ingeniera electrónica y telecomunicaciones [7]. Dentro de los proyectos de Nodo esta NodoLabs, en los cuales se imparten clases online de robótica y permiten manipular los componentes de un robot, el cual está ubicado en las instalaciones de la Universidad Técnica Particular de Loja. Con este programa de capacitación remota, los estudiantes serán capaces de dominar nociones básicas de informática, programación y electrónica, leer sensores, controlar actuadores, diseñar sistemas básicos de control de temperatura, luz y movimiento, entre otras actividades [8].

2.2 MARCO CONCEPTUAL

2.2.1 Laboratorios remotos

Los laboratorios remotos son la temática principal del presente documento, y serán tomados como herramienta para brindar acceso a cualquier estudiante a realizar las respectivas prácticas sin importar el lugar físico donde se encuentre, recalcando que para ello se requiere que cuente con una computadora con acceso a internet.

Una definición básica y sencilla de un Laboratorio Remoto se puede enunciar de la siguiente manera: sistema a través del cual el estudiante o investigador puede acceder o tele operar desde un sitio remoto los dispositivos o equipos de laboratorio que se encuentran físicamente en la universidad o centro de investigaciones [9].

2.2.1.1 Modo de operación

A diferencia de un laboratorio físico o tradicional, donde el estudiante puede interactuar físicamente con los elementos afianzando de esta forma el conocimiento a través del aprendizaje kinestésico, en un laboratorio remoto o virtual no hay contacto físico entre el estudiante y los elementos, sino que se adiciona una capa de infraestructura remota, la cual es la encargada de llevar las instrucciones del usuario hacia los equipos del laboratorio y retornar con los resultados o evidencia de la acción realizada. En las Figuras 1 y 2 se puede apreciar esta diferencia.

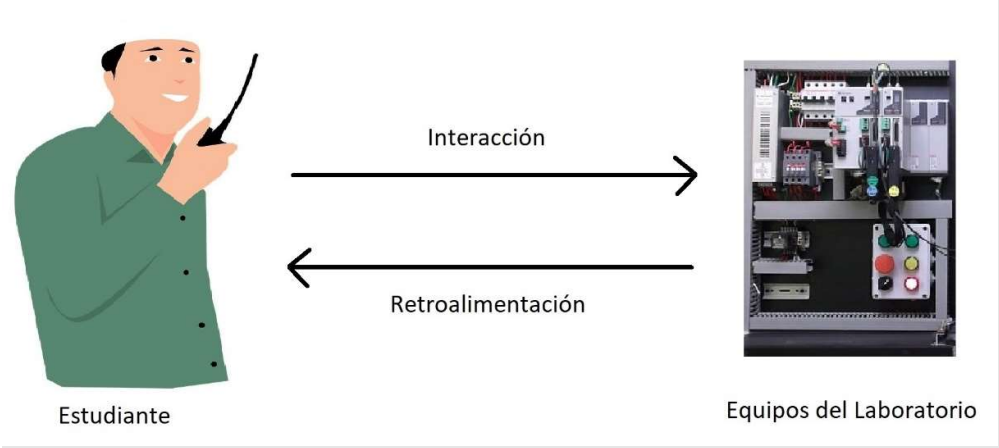


Fig. 1. Diagrama de un laboratorio tradicional.

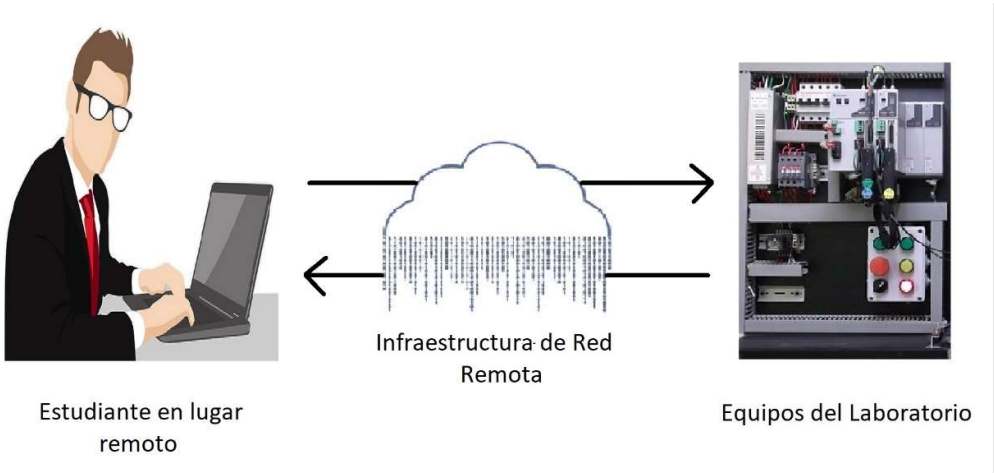


Fig. 2. Diagrama de un Laboratorio Remoto.

2.2.1.2 Arquitectura del laboratorio remoto

Los Laboratorios Remotos buscan responder a la necesidad de no alejar la práctica de laboratorio de la realidad, como requerimiento fundamental en la formación del Ingeniero, pero sin la demanda de desplazamientos físicos que generan pérdida de tiempo para el usuario y costos significativos [10].

Se exige una infraestructura tecnológica como se ve en la Figura 3, por lo que, es necesario diseñar una arquitectura que defina unas unidades funcionales, redes de telecomunicaciones, protocolo de comunicación y desarrollo de un software que permita la integración del sistema y el ambiente de interacción usuario – LR., de manera transparente y en tiempo real [10].

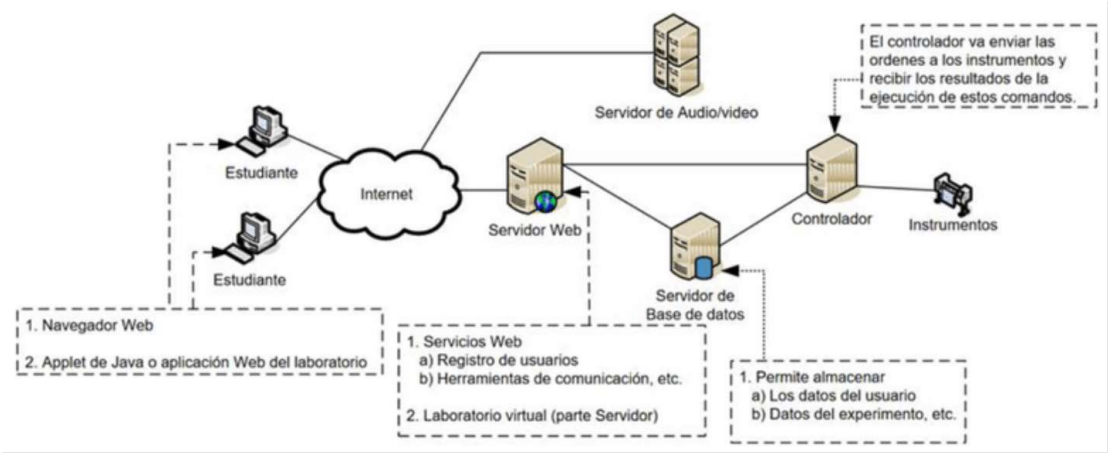


Fig. 3. Esquema básico de un Laboratorio Remoto [10].

2.2.2 Automatización

Automatización es un concepto vinculado a un flujo de trabajo, en el cual la información o la tarea (acción concreta) pasa de un punto al siguiente de acuerdo con un procedimiento establecido y controlado por un sistema de información. Más allá de los procesos de automatización industriales, el concepto asociado al entorno administrativo o de oficina, proviene ya de 1970, cuando se refería a la reducción de papel y eliminación de tareas repetitivas [11], debido a esto se planteaba la búsqueda de soluciones que permitan reducir el uso de recursos naturales, y así evitar el cansancio y molestias en los trabajadores a causa de la realización de tareas monótonas y repetitivas.

En términos generales, automatización debe entenderse como una ingeniería de procesos, tanto internos como externos para la organización, que pretenden la eliminación de tiempos de espera o tareas innecesarias [11].

En el área industrial, se puede decir que la automatización de procesos consiste en la eliminación de tareas repetitivas mediante el uso de mecanismos electrónicos especializados para llevar a cabo el control de otros elementos actuadores que serán los encargados de llevar a cabo una tarea específica para la que hayan sido programados.

2.2.3 Equipos industriales

Una parte fundamental dentro del proceso de automatización de procesos, son los equipos industriales, los cuales brindan la autonomía necesaria a dichos procesos.
Dichas herramientas son utilizadas para una correcta optimización entre el operario y la máquina, cada proceso responde a necesidades únicas al igual de las características de cada uno de los equipos, entre ellos se tiene:

2.2.3.1 Controlador lógico programable

Programmable Logic Controller (PLC) son equipos electrónicos comúnmente aplicados en la Industria para controlar procesos y monitorearlos en tiempo real, mediante sus canales de entradas y salidas facilitan la conexión de sensores o actuadores u otros componentes, tal como el nombre lo indica, el dispositivo debe ser programado en su propio software, tomando en cuenta las variables de un proceso para adquirir, guardar y restablecer sus valores cíclicamente y a su vez, realizar el control [11].

2.2.3.2 Variadores de frecuencia

Los variadores de frecuencia son dispositivos que permiten llevar un control de la velocidad del motor de corriente alterna, modificando la frecuencia de alimentación del motor [12], cuenta con una pantalla que permite llevar a cabo una supervisión de las corrientes, velocidades y tensiones que provocan que el motor este en marcha. Estos dispositivos son manejados a través de una serie de parámetros, que varían dependiendo del modelo y marca de este, su programación puede ser a través del panel de operaciones con el que cuenta, mediante un software y programación que se pueda adquirir por separado o través de un cable con un programa que solamente permite modificar parámetros del variador.

2.2.3.3 Motores

Los motores ejercen un movimiento rotatorio en su eje, en el cual se pueden ajustar sistemas mecánicos enfocados directamente al sector industrial y doméstico. Comúnmente son usados en ámbito de la automatización y de acuerdo con el sistema de alimentación, estos motores pueden ser de corriente alterna o continua.

Estos equipos tienen un rol importante dependiendo del suministro de potencia que este disponga, siendo útiles en aplicaciones casera, comerciales además del sector industrial.

Motores de corriente alterna trifásico

Los motores de corriente alterna trifásico son utilizados en el área industrial, y pueden tener desde fracciones de HP (Horse Power) hasta miles de HP. Pueden venir de varios tamaños y con diferentes características según las necesidades que se requiera solventar en la empresa, aunque normalmente los podemos ver en bandas trasportadoras de productos y agitadores de mezclas. Su principal ventaja es el coste bajo de operación y el poco mantenimiento que estas máquinas requieren a lo largo de su vida útil.

2.2.3.4 Sensores

Es el conjunto de elementos electrónicos (resistencias, inductancias, capacitores, ultrasonidos) capaces de convertir una señal física no eléctrica a una eléctrica.

Sensor de temperatura

Los sensores de temperatura se utilizan en diversas aplicaciones tales como aplicaciones para la elaboración de alimentos, climatización para control ambiental, dispositivos médicos, manipulación de productos químicos y control de dispositivos en el sector automotriz (p. ej., refrigerantes, ingreso de aire, temperaturas del cabezal de cilindro, etc.). Los sensores de temperatura se utilizan para medir el calor para asegurar que el proceso se encuentre, o bien dentro de un cierto rango, lo que proporciona seguridad en el uso de la aplicación, o bien en cumplimiento de una condición obligatoria cuando se trata de calor extremo, riesgos, o puntos de medición inaccesibles [13].

Sensor de nivel

Un sensor de nivel, también conocido como interruptor de nivel, es un dispositivo electrónico que realiza la medición de la altura de un líquido en un tanque. Para esto, emplea un *reed switch* (interruptor de lengüeta) y un flotador magnético. El flotador es el encargado de abrir o cerrar el contacto eléctrico. Una vez que el sensor detecta el nivel de líquido, emite una señal on/off al alcanzar el llenado o vaciado.

Los sensores de nivel no se ven afectados por ondulación o vibraciones, lo que genera más confiabilidad.

Resistencia eléctrica

La resistencia eléctrica es un dispositivo electrónico el cual su principal objetivo es producir calor, su funcionamiento se basa en el efecto Joule.

Las resistencias eléctricas calefactoras pueden realizar calentamiento tanto por convección, conducción o radiación [14].

2.2.3.5 Contactor

Dispositivo eléctrico que cumple la función de apertura y cierre de circuitos eléctricos, mediante la conexión y desconexión de sus contactos a través de una señal externa.

2.2.3.6 Interruptor termomagnético

Dispositivo que se encarga de la protección de circuitos eléctricos, ejecutando un corte del paso de corriente ante eventos térmicos y cortocircuitos.

2.2.3.7 Relé térmico

Los relés térmicos son elementos destinados a la protección de los motores eléctricos contra sobreintensidades o pérdida de alguna de las fases y evitar así la degradación o destrucción de los bobinados del motor [15].

2.2.4 Comunicación en la Industria

En la industria moderna, las comunicaciones de datos entre diferentes sistemas, procesos e instalaciones suponen uno de los pilares fundamentales para que ésta se encuentre en un nivel de competitividad exigida en los procesos productivos actuales. En un sistema de comunicación de datos industrial es tanto más exigente cuanto más cerca del proceso nos encontramos. Si realizamos una comparativa entre tres de las principales características que determinan la aplicación de las diferentes redes de comunicación, como son:

- Volumen de datos.
- Volumen de transmisión.
- Velocidad de respuesta [16].

2.2.5 Protocolos de Comunicación

Para lograr la interconexión de sistemas de una red básica, como por ejemplo dos computadoras interconectadas entre sí, hasta una red compleja como internet, se requiere de un sistema sofisticado que permita que la comunicación fluya de manera adecuada, por ello existen un conjunto de normas y protocolos que hacen que la conexión se establezca, y dependiendo de tipo de servicio o aplicación especifica a la que se requiera acceder se procederá a hacer uso de uno u otro protocolo (o un conjunto de ellos).

Un protocolo de red es un conjunto de normas o estándares que dictan la forma en que se transfieren los bits con la información adecuada para asegurar la comunicación entre dos o más dispositivos finales a través de una red.

2.2.5.1 Suite de Protocolos TCP/IP

Los protocolos más importantes que permiten la transmisión de datos en internet son TCP (*Transmission Control Protocol*) e IP (*Internet Protocol*). Ambos protocolos son los encargados de controlar la interconexión de dos dispositivos remotos, permitiendo o rechazando el flujo de datos.

TCP

TCP es un protocolo de transporte orientado a la conexión que envía datos como un flujo no estructurado de bytes. Mediante el uso de números de secuencia y mensajes de confirmación, TCP puede proporcionar a un nodo de envío información de entrega sobre los paquetes transmitidos a un nodo de destino. Cuando los datos se han perdido en tránsito desde el origen hasta el destino, TCP puede retransmitir los datos hasta que se alcance una condición de tiempo de espera o hasta que se haya logrado una entrega exitosa. TCP también puede reconocer mensajes duplicados y los descartará adecuadamente. Si la computadora emisora está transmitiendo demasiado rápido para la computadora receptora, TCP puede emplear mecanismos de control de flujo para ralentizar la transferencia de datos. TCP también puede comunicar la información de entrega a los protocolos de capa superior y las aplicaciones que admite. Todas estas características hacen de TCP un protocolo de transporte fiable de extremo a extremo. TCP se especifica en RFC 793 [17].

IP

IP es el protocolo principal de capa 3 en la suite de Internet. Además del enrutamiento de interredes, IP proporciona informes de errores y fragmentación y reensamblaje de unidades de información llamadas datagramas para la transmisión a través de redes con diferentes tamaños máximos de unidades de datos. IP representa el corazón del conjunto de protocolos de Internet.

El término IP en la sección se refiere a IPv4 a menos que se indique explícitamente lo contrario.

Las direcciones IP son números únicos a nivel mundial, de 32 bits asignados por el Centro de información de red. Las direcciones únicas a nivel mundial permiten que las redes IP

en cualquier parte del mundo se comuniquen entre sí. Una dirección IP se divide en dos partes. La primera parte designa la dirección de red, mientras que la segunda parte designa la dirección del host.

El espacio de direcciones IP se divide en diferentes clases de red. Las redes de clase A están diseñadas principalmente para su uso con unas pocas redes muy grandes, ya que proporcionan solo 8 bits para el campo de dirección de red. Las redes de clase B asignan 16 bits y las redes de clase C asignan 24 bits para el campo de dirección de red. Sin embargo, las redes de clase C solo proporcionan 8 bits para el campo de host, por lo que el número de hosts por red puede ser un factor limitante. En los tres casos, la mayoría de los bits de la izquierda indican la clase de red. Las direcciones IP se escriben en formato decimal punteado; por ejemplo, 34.0.0.1. La Figura 4 muestra los formatos de dirección para las redes IP de clase A, B y C [17].

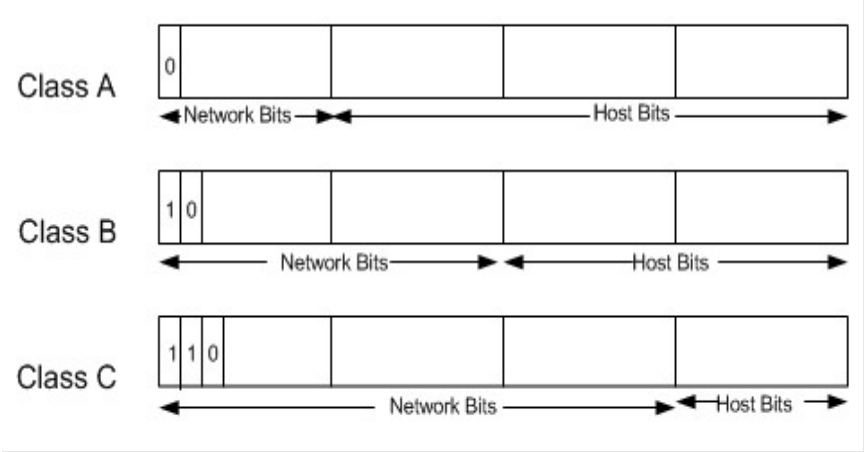


Fig. 4. Formatos de dirección IP de clase A, B y C [17].

ICMP

Internet Control Message Protocol (ICMP) es un protocolo que tiene como base el protocolo IP dentro de la arquitectura TCP/IP y su objetivo principal es dar información del estado y situaciones de error en el funcionamiento de la capa de red, en especial en routing, congestión, fragmentación, etc. [18].

El protocolo ICMP es de características semejantes al protocolo UDP (*User Datagram Protocol*) cuyo uso se centra más en el control de paquetes de datos (ver Figura 5).

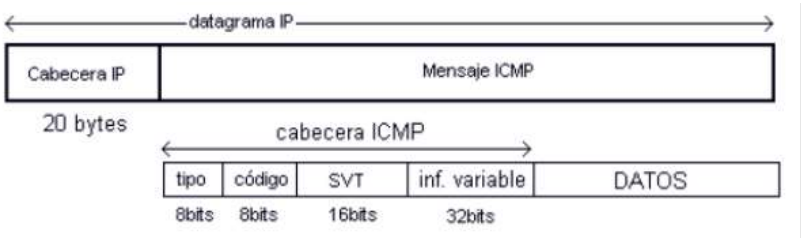


Fig. 5. Encapsulación de un mensaje ICMP dentro de un paquete IP [18].

A continuación, se redacta algunos de los principales y más comunes mensajes ICMP:

- Tipo 0: *Echo Reply* (respuesta de eco)
- Tipo 3: *Destination Unreachable* (destino inaccesible)
- Tipo 4: *Source Quench* (cadencia de envío demasiado elevada)
- Tipo 5: *Redirect* (redireccionar)
- Tipo 8: *Echo Request* (petición de eco)
- Tipo 9: *Router Adverstisement* (aviso de router)
- Tipo 10: *Router Solicitation* (solicitud de router)
- Tipo 11: *Time Exceded* (tiempo excedido)
- Tipo 12: *Parameter problema* (problemas de parámetros)
- Tipo 13: *Timestamp Request* (petición de marca de tiempo)
- Tipo 14: *Timestamp Reply* (respuesta de marca de tiempo)
- Tipo 17: *Address Mask Request* (petición de máscara de dirección)
- Tipo 18: *Address Mask Reply* (respuesta de máscara de dirección)
- Tipo 30: *Traceroute Reply* (respuesta de camino)

2.2.5.2 Wake on LAN

Wake on LAN (WoL) es el protocolo que utiliza tecnología *Magic Packet* y que fue desarrollada por AMD (*Advanced Micro Devices*) y HP (Hewlett Packard) para encender a distancia un host remoto que pudiera haber sido apagado automáticamente debido a la gestión de energía (ver Figura 6), aunque la misma permite a las empresas o particulares reducir costos de energía pero supone un problema para los departamentos de tecnologías de información, en especial a la hora de gestionar de forma rápida y eficaz los PCs a distancia, sobre todo en el horario no laboral cuando estas se encuentren apagadas o en

estado de suspensión, suponiendo que las funciones de gestión de energía estén activadas [19].

El funcionamiento del *Magic Packet* es la base del protocolo WoL donde se envía paquetes a la tarjeta de red del host por medio de ethernet, entre los cuales se tiene:

- Dirección de broadcast de la red.
- Dirección de broadcast.
- Dirección MAC de la tarjeta de red.
- Paquete de datos.

Estos paquetes se dirigen a los puertos UDP 7 – 9 del host y es aplicable a cualquier plataforma como Intel, AMD, Apple [20].

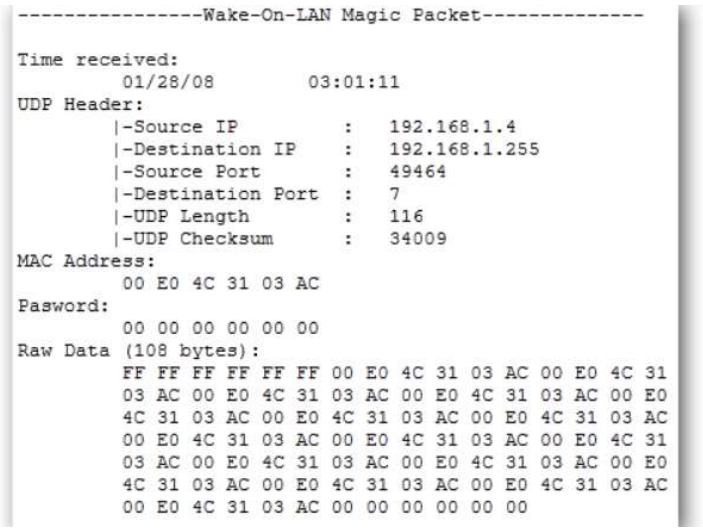


Fig. 6. Magic Packet Wake on LAN [21].

2.2.5.3 NAT

Network Address Translator (NAT) es un traductor de direcciones de red y su función principal es esa, traducir una dirección IP en otra totalmente diferente. Por otro lado, también se denomina a este proceso enmascaramiento de IP, y brinda una capa de protección extra a la seguridad de los dispositivos internos de nuestra red ya sean en entornos domésticos o empresariales. NAT puede ser utilizado en cualquiera de sus tres tipos: NAT estático, NAT dinámico y PAT (*Port address Traslation*).

NAT estático

El NAT estático, como su nombre lo indica, es aquel en que la traducción de direcciones se da de forma estática de uno a uno, dicho de otro modo, la dirección IP interna de cada dispositivo se traduce a una única dirección IP global configurada permanentemente (ver Figura 7).

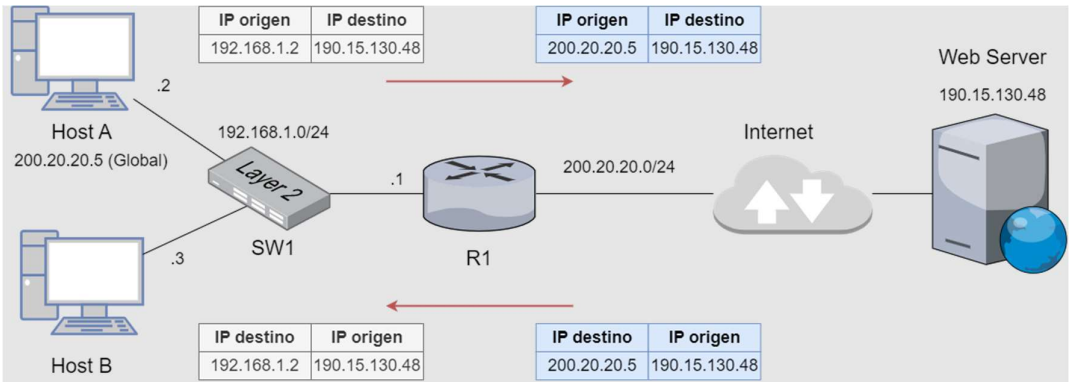


Fig. 7. NAT estático.

NAT dinámico

En el NAT dinámico, se cuenta con un conjunto de direcciones IP disponibles para ser utilizadas como IP global de cualquier dirección IP interna que lo requiera (ver Figura 8).

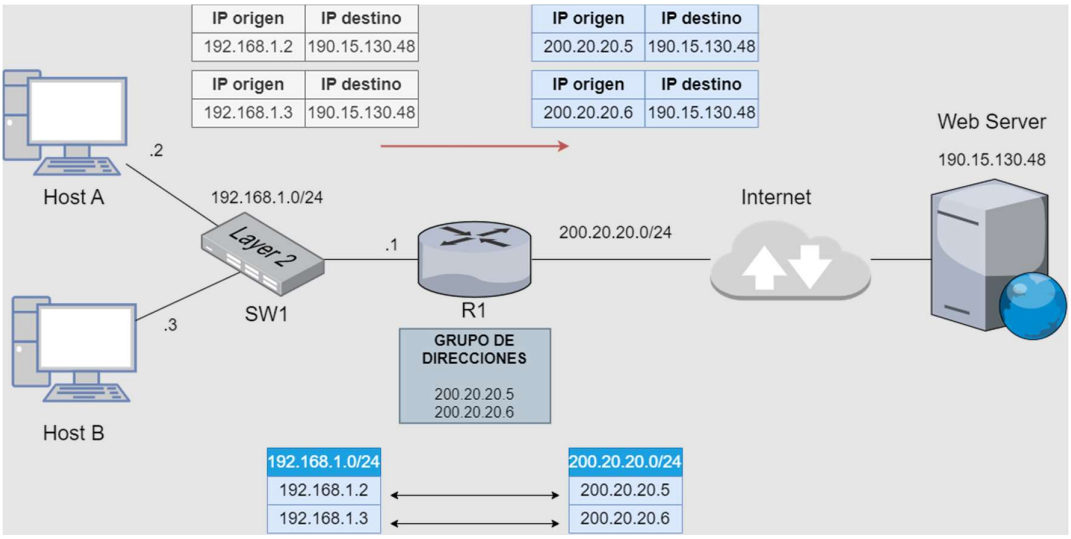


Fig. 8. NAT dinámico.

PAT

PAT realiza la traducción de varias direcciones IP locales en una o varias direcciones globales haciendo uso de una característica de TCP/IP que es el número de puerto asignado a la sesión (TCP/UDP), con esta información un router con PAT habilitado puede identificar a que dispositivo debe de regresar los paquetes recibidos en respuesta a alguna solicitud. Este es el NAT más utilizado debido a ahorro de direcciones IP públicas, es necesario resaltar, que PAT es lo que permite que varios dispositivos estén conectados a internet de forma simultánea compartiendo la misma IP pública (ver Figura 9).

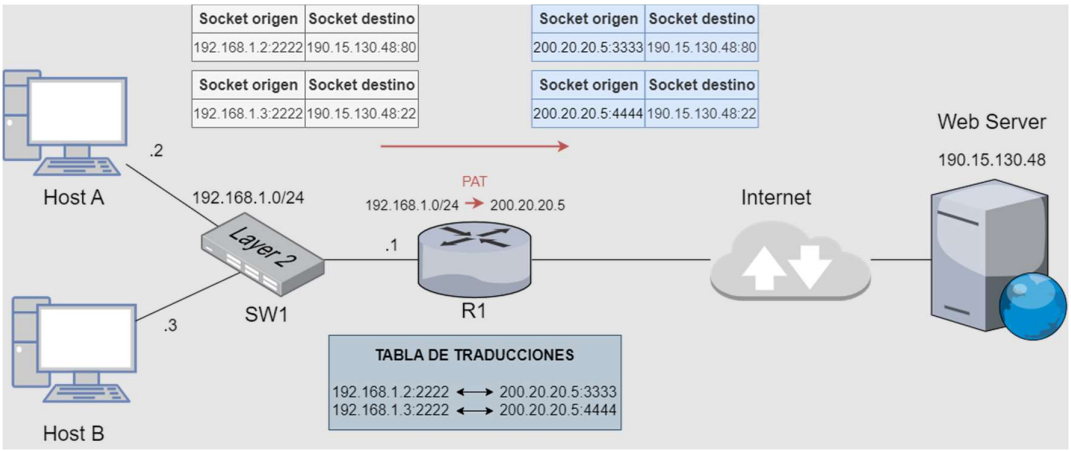


Fig. 9. PAT.

2.2.5.4 IEEE 802.3

Ethernet fue desarrollado a principios de los 1970, época en la que solo se utilizaba como sistema interno de red en la empresa Xerox, y no fue hasta principios de los ochenta que Ethernet se convirtió en un producto estandarizado. Con todo, aún habría que esperar hasta mediados de la década para que empezara a utilizarse más ampliamente. Fue cuando los fabricantes comenzaron a trabajar con Ethernet y con productos relacionados. Así, dicha tecnología contribuyó de manera significativa a que los ordenadores personales revolucionaran el mundo laboral. El estándar IEEE 802.3 tan popular actualmente se utiliza, por ejemplo, en oficinas, viviendas particulares, contenedores y portadores (carrier). Mientras que la primera versión de esta tecnología solo tenía una velocidad de 3 Mbit/s, los protocolos Ethernet actuales permiten alcanzar velocidades de hasta 1 000 megabits por segundo. Por otro lado, los estándares Ethernet antiguos se restringían a un solo edificio, mientras que hoy en día pueden alcanzar hasta los 10 km gracias a la

utilización de la fibra de vidrio. En el transcurso de su desarrollo, Ethernet ha tenido el rol dominante entre las tecnologías LAN y ha destacado entre sus numerosos competidores. La conocida como Ethernet en tiempo real es en la actualidad un estándar industrial para aplicaciones de comunicación [22].

2.2.5.5 IEEE 802.11

El estándar IEEE 802.11 es quien establece el modo de acceso a la red local de forma inalámbrica, esto permite la interconexión de otros dispositivos como laptops, tabletas, teléfonos inteligentes, y otros dispositivos compatibles con la tecnología Wifi [23].

802.11a

Establecido en 1999. Utiliza la banda de frecuencia de 5 GHz en un ancho de banda de 20 MHz. Rango de 35 Mbps en interiores, 119 Mbps de 11 a 54 Mbps en exteriores [23].

802.11b

Establecido en 1999. Utiliza la banda de frecuencia de 2,4 GHz en un ancho de banda de 20 MHz. Rango de 35 Mbps en interiores, 140 Mbps en exteriores 140 Mbps de velocidad [23].

802.11g

Establecido en 2003. Utiliza la banda de frecuencia de 2,4 GHz en un ancho de banda de .20 MHz. Rango de 38 en interiores, 140 Mbps de velocidad en exteriores 54 Mbps [23].

802.11n

Establecido en 2009. Utiliza la banda de frecuencia de 2,4/5 GHz en un ancho de banda de 20/40 MHz. Rango de 70 en interiores, 250 Mbps en exteriores y 150 Mbps de velocidad [23].

802.11ac (versión preliminar)

Establecida en 2012. Utiliza la banda de frecuencia de 5 GHz en un ancho de banda de 160 MHz. Rango de 70 Mbps en interiores, 250 En exteriores, 250 Mbps Velocidad máxima de 866 Mbps a 6,93 Gbps (basado en hasta 8 flujos de datos) [23].

802.11ad (WiGig)

Establecida en 2013. Utiliza la banda de frecuencia de 2,4/5/60 GHz. Rango de 1 a 10 velocidades de 6,75 Gbps (transmisión de video inalámbrico de calidad HD) [23].

2.2.5.6 HTTP

Hypertext Transfer Protocol (HTTP) es un protocolo de capa de aplicación para transferir información entre los dispositivos conectados a una red. Todos los sitios web y aplicaciones accesibles para los usuarios normales se ejecutan en HTTP. La transferencia de datos a través de HTTP se basa habitualmente en solicitudes y respuestas. Casi todos los mensajes HTTP son una solicitud o una respuesta a una solicitud [24].

2.2.6 RouterOS

RouterOS es el sistema operativo de RouterBoard, el cual ha sido continuamente mejorado a través de 15 años. Con un vasto número de capacidades el RouterOS también puede ser instalado en una PC lo que la convertirá en un router con todas las características necesarias, tales como, Enrutamiento, Firewall, Gestión de ancho de banda, Punto de Acceso Inalámbrico, Enlace Backhaul, Hotspot, Servidor VPN, etc. [25].

2.2.6.1 Scripts

El manual proporcionado por Mikrotik en donde nos da una introducción hacia la programación por medio de scripts dentro de RouterOS. El scripting proporciona una forma de automatizar algunas tareas de mantenimiento del router por medio de la ejecución de scripts, definidos por el usuario y limitados a cuando se suscite algún evento en particular [26].

Los scripts pueden ser almacenados en el apartado de scripts o pueden ser escritos directamente en la consola. Los eventos utilizados para desencadenar la ejecución de scripts incluyen, entre otros, el system Scheduler, la herramienta de monitoreo de tráfico, etc.

Los scripts pueden ser ejecutados de las siguientes formas:

- **on event**. - se ejecutan automáticamente en algunos eventos de la instalación (Schedule, netwatch, VRRP).
- **by another script**. - se ejecuta un script dentro de otro
- **manually**. - se ejecuta desde la consola, ejecutando el comando run o en Winbox.

2.2.6.2 Scheduler

El Scheduler o programador, puede desencadenar la ejecución de scripts en un momento determinado, después de un intervalo de tiempo específico o ambos [26].

Entre algunas de sus propiedades principales existe:

- **Interval.** - intervalo entre dos ejecuciones de secuencias de comandos, si el intervalo de tiempo se establece en cero, la secuencia de comandos solo se ejecuta a la hora de inicio; de lo contrario de ejecuta repetidamente en el intervalo de tiempo especificado.
- **Name**. - nombre de la tarea.
- **On-event**. - nombre del script a ejecutar.
- **Run-count**. - contador se incrementa cada vez que se ejecuta el script
- **Startup**. - ejecuta el script, tres segundos después del inicio del sistema.

2.2.6.3 Bridge

Un bridge es una interconexión entre varias interfaces físicas o virtuales para que compartan el mismo dominio de broadcast. Una red bridge entre las eth1 y eth2 comparte los recursos como DHCP, en la interfaz virtual que se crea como bridge-eth1-eth2 [27].

2.2.7 Redes de comunicación industrial

Cuando los sistemas industriales se hicieron más complejos, también el cableado, entre ellos, requería de una inmensa cantidad de cables. Ese fue uno de los principales motivos por los que se implementaron las comunicaciones en la industria; el objetivo era reducir el cableado y no cabe duda de que, de este modo, se solucionó [28].

En la actualidad se considera comunicación al intercambio de información entre dos o más elementos involucrados. Dicha información puede ser procesada y almacenada o

descartada a criterio del receptor. Ahora cuando la industria se ve involucrada en este proceso, entonces nos estamos refiriendo a la comunicación industrial.

2.2.7.1 Elementos básicos para la interconexión de redes

Switch

Switch o conmutador es un dispositivo que a diferencia de un HUB no envía la información a todos los dispositivos conectados. Realiza una selección y solo lo envía al nodo al que va dirigido (ver Figura 10) [28].

Fig. 10. Switch [28].

Router (encaminador)

Router o encaminador opera entre redes aisladas que utilizan protocolos similares (por ejemplo, TCP/IP) y direccionan o encaminan la información de acuerdo con la mejor ruta posible (ver Figura 11) [28].

Fig. 11 . Router. [28]

La primera función de un Router es conocer si el destinatario de un paquete de información se halla en nuestra propia red o en una remota. El Router encamina los datos hacia la red de destino si se encuentra en su grupo; si no fuera así, conectará con otros Router para realizar la comunicación [28].

2.2.7.2 Protocolos de comunicación industriales

Profibus

Profibus es un bus de campo abierto que se utiliza en las aplicaciones más bajas de la pirámide de automatización, proceso y campo. Es un estándar que sigue la norma UNE IEC 61158 y las normas internacionales IEC 61784. Profibus puede utilizarse para aplicaciones críticas de alta velocidad y tareas de comunicación complejas y para transmitir pequeñas y medianas cantidades de datos entre los dispositivos que participan en la red [28].

Hoy día, este bus se encuentra en una clara decadencia al ser superado por la red de Profinet. Pero no se puede decir que Profibus haya muerto, porque hay muchos sistemas que lo siguen utilizando y aún se sigue instalando [28].

Profinet

Profinet nace como una continuación de Profibus; adquiere la experiencia con Profibus y las ventajas de las redes de Ethernet. Se considera el auténtico bus en tiempo real. Mucho tiempo antes de aparecer Profinet, ya existía una red muy parecida que se llamaba Ethernet Industrial. De hecho, Profinet constituye una variante de Ethernet Industrial. Pero no fue, hasta la aparición de Profinet, cuando estas redes alcanzaron el éxito.

Con lo dicho anteriormente, se puede definir Profinet como el estándar abierto de Ethernet Industrial de la asociación Profibus Internacional (PI), según la norma IEC 61784-2. Constituye el estándar de comunicación actualmente más utilizado en redes de automatización [28].

Los tipos de comunicación Profinet que existen son [28]:

- **Standard TCP/IP:** este servicio se utiliza para funciones no deterministas, como parametrización, transmisiones de vídeo/audio y transferencia de datos a sistemas TI de nivel superior.
- **Real Time**: las capas TCP/IP no se emplean para ofrecer un rendimiento determinista a las aplicaciones de automatización, pues funcionan con unos tiempos de retardo en el rango de 1-10 ms. Este hecho representa una solución basada en software adecuada para aplicaciones típicas de E/S; se incluyen control de movimiento y requisitos de alto rendimiento.
- **Isochronous Real Time**: la priorización de señal y la conmutación programa da proporcionan una sincronización de alta precisión para aplicaciones como el control de movimiento. Las velocidades de ciclo en rangos de fracciones de milisegundos son posibles, con jitter (variabilidad temporal durante el envío de señales digitales) en el rango de fracciones de microsegundos.

2.2.7.3 Topología de red Profinet

PROFINET le ofrece flexibilidad para el diseño de la red. Además, es compatible con topologías de línea, árbol, anillo y estrella. Además, es compatible con conexiones inalámbricas mediante Bluetooth o Wifi [29].

Línea

La mayoría de los dispositivos PROFINET tiene por lo menos dos puertos que son parte de un conmutador incorporado en el dispositivo. Los conmutadores incorporados permiten a los usuarios conectar dispositivos en una topología en línea sin necesidad de conmutadores externos [29].

- Ventajas: Por lo general los dispositivos tienen conmutadores incorporados. Los conmutadores externos son opcionales. El costo se reduce debido a que se necesitan menos cables y no se necesitan conmutadores externos.
- Desventajas: Si un nodo de la línea falla, todos los nodos dependientes pierden la comunicación. Igualmente, el usuario debe tener en cuenta las limitaciones de profundidad de la línea.

Estrella y árbol

Los conmutadores incorporados o autónomos permiten topologías de estrella o árbol [29], como se ve en la Figura 12.

- Ventajas: Si falla un solo nodo, no se afecta el funcionamiento de toda la red.
- Desventajas: Si falla un conmutador central de la estrella o árbol, se afecta la comunicación con todos los nodos de esa área. Igualmente, estas topologías necesitan más cables y conmutadores externos, lo que cuesta más.

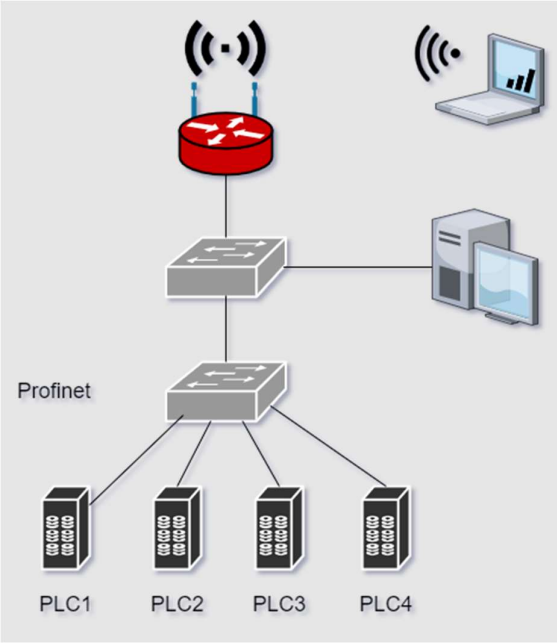


Fig. 12. Topología estrella árbol.

Anillo

Generalmente Ethernet no permite una topología de bucle o anillo. Pero, PROFINET permite que se implemente una topología de anillo administrándola con dos clases definidas de redundancia de medios: Protocolo de Redundancia de Medios (MRP) y Redundancia de Medios para Duplicación Planificada (MRPD) [29].

- Ventajas: Las topologías de anillo ofrecen redundancia de medios. Hay dos rutas para la comunicación. En caso de que falle un cable o nodo en el anillo, el funcionamiento continúa.

- Desventajas: Requiere dispositivos compatibles con redundancia MRP y MRPD. También necesita más cableado y configuración adicional de los nodos redundantes.

2.2.8 Escritorio remoto

Un escritorio remoto se puede definir como un software que permite acceder de forma remota a un ordenador desde otro ordenador. Para la conexión remota se establezca, se requiere que ambos equipos cuenten con su propia dirección IP y que además cuenten con acceso a internet en caso de pertenecer a redes distantes en términos geográficos y que se encuentren encendidos al instante de ejecutar la aplicación. Todo esto, en el ámbito empresarial y educativo, permite un gran ahorro económico y sobre todo ahorro de tiempo, al no depender de traslados de capital humano de forma innecesaria.

2.2.9 VPN

Una VPN es un servicio que permite el acceso remoto a la red interna de la organización y a los recursos corporativos, como pueden ser el correo electrónico, el servidor de ficheros o incluso aplicaciones de escritorio como el CRM (*Customer Relationship Management*), ERP (*Enterprise Resource Planning*) o cualquier otra aplicación departamental (ver Figura 13) [30].

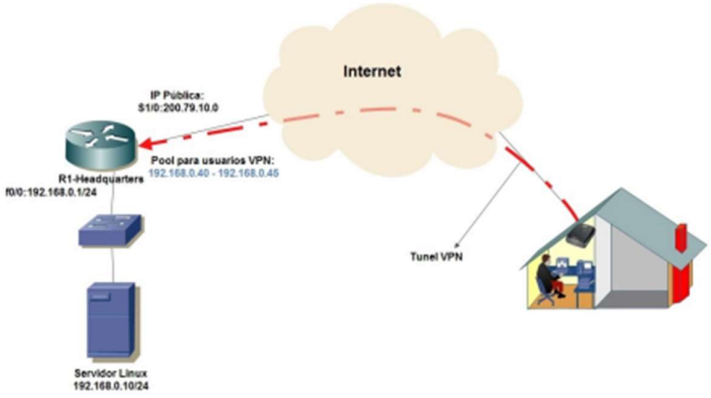


Fig. 13. Esquema de una red VPN [30].

2.2.9.1 Estructura de una red VPN

Para realizar la conexión virtual de un punto a otro, se requiere de protocolos como L2TP, PPTP, IKEv2 u OpenVPN. Dicha conexión se establece a nivel de una red WAN (*Wide*

Area Network), pero para el usuario final se comportará como una LAN (*Local Área Network*), esto es posible gracias a la dirección IP virtual suministrada por el servidor de forma dinámica o se deberá configurar previamente de forma estática en el cliente VPN [31].

La conexión física se realiza de distintas formas, una de ellas es mediante túneles cifrados o *tunneling*. Se crea un túnel virtual en donde los datos se transfieren en encapsulados dentro de PDU (*Protocol Data Unit*). Todo se realiza a través de conexión cableada y acceso remoto, en donde se utiliza la infraestructura existente para transmitir los datos.

A continuación, se explica los elementos [31]:

- **Cliente VPN:** el cliente será nuestro equipo provisto de una aplicación o extensión cliente que inicia la conexión a través de unas credenciales hacia el servidor. En OpenVPN ya veremos que se utiliza claves pre-compartidas o certificados SSL/TLS + RSA.
- **Servidor VPN:** las credenciales de acceso se envían a un servidor VPN el cual proporcionará una dirección IP privada al equipo para transmitir dentro de la red.
- **Túnel VPN:** para esta transmisión se utiliza un túnel virtual por el que la información viaja encriptada en PDU. Esta conexión se realizar entre cliente y servidor.
- **Acceso al contenido:** cuando el servidor recibe la petición la desencripta, y se conecta con el servicio que hemos demandado, por ejemplo, una página web, un servicio de streaming o el servidor de nuestra empresa si estamos trabajando fuera. Luego encripta de nuevo los datos y nos lo envía.

2.2.9.2 Arquitecturas VPN

VPN Site to site

Este tipo de VPN permite una conexión VPN entre dos o más *peers* o *gateways* para establecer una transmisión de datos de forma segura y confiable. Estos *peers* participantes para establecer la VPN pueden estar representado por un dispositivo dedicado para brindar el servicio de VPN o puede ser un dispositivo que a parte de sus funciones principales también brinde el servicio de VPN como podrían ser un Firewall o un Router [32], como se ve en la Figura 14.

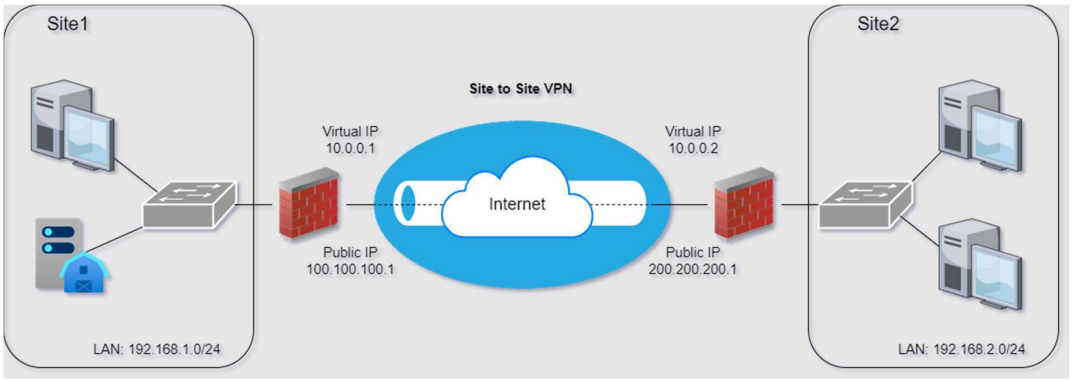


Fig. 14. VPN Site to Site.

VPN Client to site

Las VPN de tipo cliente son redes privadas virtuales que se establecen entre un endpoint, laptop o PC de un usuario final, y la red LAN de la empresa u organización. Las VPN tipo clientes son utilizadas por los trabajadores que viajan o que trabajan desde casa, como es el caso de nuestra realidad en estos años. El dispositivo que brinda el servicio de VPN puede ser un Firewall de perímetro de la organización o puede ser un servidor de VPN dedicado [32], como se ve en la Figura 15.

Una ventaja del uso de este tipo de VPN es que en el servidor se puede permitir o restringir el acceso a los recursos de la red interna dependiendo del nivel de usuario del cliente remoto.

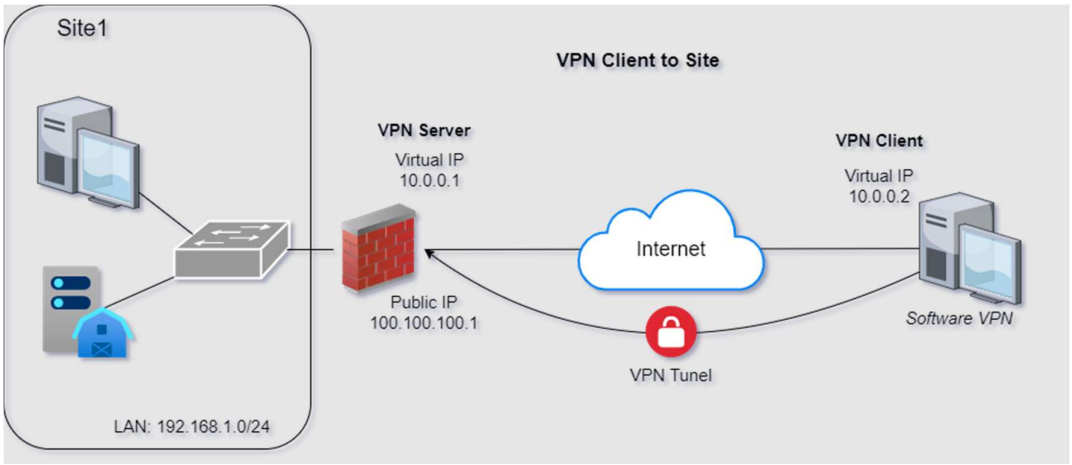


Fig. 15. VPN Client to Site.

VPN Client to client

Este tipo de VPN es el que se utiliza menos en las organizaciones, ya que solo permite la conexión a un único destino dentro de la organización, es decir el usuario remoto solo podrá conectarse a un servidor o aplicación.

Este tipo de conexión VPN se utiliza generalmente para administración o soporte de un servidor de forma remota. Se requiere que el usuario remoto ingrese sus credenciales correctamente antes de usar el servicio y para esto se requiere que el cliente remoto tenga software VPN cliente instalado y correctamente configurado con los parámetros de la organización. Por parte del servidor debe tener instalado un software que brinde el servicio de VPN [32], como se ve en la Figura 16.

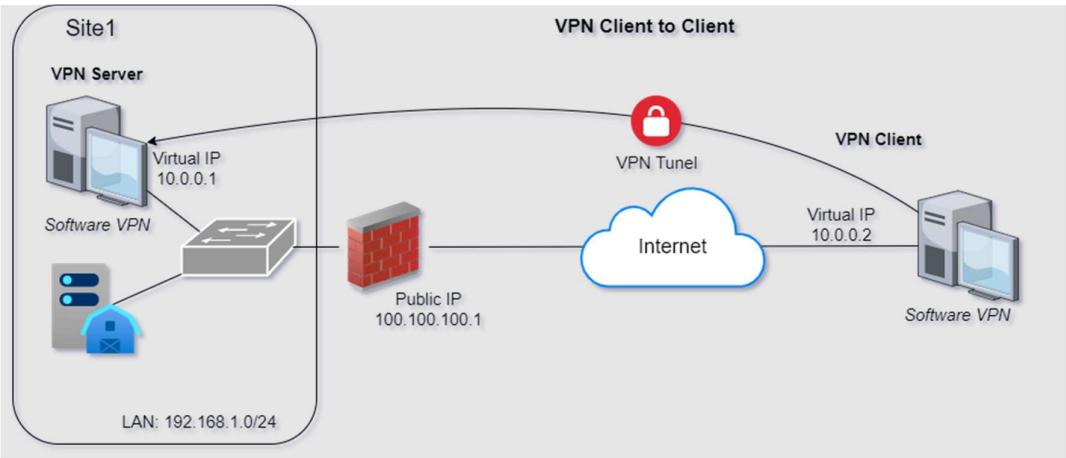


Fig. 16. VPN Client to Client.

2.2.10 Streaming

El streaming es una forma de ofrecer medios visuales y de audio a los usuarios a través de Internet. Funciona mediante el envío continuo del archivo multimedia al dispositivo de un usuario, pero no todo a la vez sino poco a poco. El archivo multimedia original se almacena en remoto o, en el caso del streaming en directo, se crea en tiempo real con una cámara o un micrófono en remoto. De este modo, se puede reproducir el vídeo o el audio sin que sea necesario que el dispositivo del usuario se descargue primero el archivo completo [24].

2.2.10.1 HLS

El streaming en directo HTTP (HLS) es uno de los protocolos de streaming de vídeo más ampliamente utilizados. Aunque se conoce como streaming "en directo" HTTP, se usa tanto para streaming a la carta como para streaming en directo. HLS convierte los archivos de vídeo en archivos HTTP descargables más pequeños y los entrega mediante el protocolo HTTP. Los dispositivos cliente cargan estos archivos HTTP y luego los reproducen como vídeo [24].

2.2.10.2 FFmpeg

Framework capaz de decodificar, codificar, transcodificar, multiplexar, demultiplexar, transmitir, filtrar y reproducir casi cualquier cosa que los humanos y las máquinas han creado. Soporta los más oscuros Formatos antiguos hasta la vanguardia. No importa si eran diseñado por algún comité de estándares, la comunidad o una corporación [33]. Muchos programas comunes y sitios web usan FFmpeg para leer y escribir archivos audiovisuales, por ejemplo, VLC, Google Chrome, YouTube y muchos más. Además de ser una herramienta de programa y de desarrollo web, FFmpeg se puede usar en la interfaz de la línea de comandos para realizar muchas tareas comunes, complejas e importantes, relacionadas con la gestión, modificación y análisis de archivos audiovisuales [34].

2.2.11 Laboratorio de prácticas industriales

El Laboratorio de prácticas industriales es un espacio dotado de varios elementos que sirven para la realización de prácticas de control de procesos industriales, tales como giros de motores, cintas transportadoras, sistemas de llenado de líquidos, controles de temperatura, etc.

La automatización combinación los elementos de la neumática, electroneumática, hidráulica y electricidad para obtener un proceso controlado donde se evalúan las variables de nivel, presión, flujo y temperatura [35].

Para tener la capacidad de hacer un uso correcto de un laboratorio con estas características, primero debe de entender el funcionamiento de los equipos y las debidas protecciones físicas con las que debe de contar, además de tener pleno conocimiento de la lectura de planos eléctricos y diseño de redes industriales.

2.2.12 Lenguaje de programación Ladder

El Lenguaje de programación Ladder es un lenguaje grafico basado en los esquemas de control de conmutación clásico siguiendo lógica matemática. La programación Ladder se encuentra presente en la mayoría de los autómatas o PLCs debido a su simplicidad y amplio abanico de posibilidades [36].

En este lenguaje de programación cada símbolo representa una variable que puede ser verdadero o falso.

2.3 MARCO TEÓRICO

A continuación, se detallan artículos y proyectos de titulación, de las cuales se tomó como base para el desarrollo de esta propuesta tecnológica.

"Diseño e implementación de un entorno virtual y laboratorio remoto para el aprendizaje de la cátedra de teoría electromagnética". Publicado por la Universidad Nacional de Chimborazo en el año 2019, proyecto de titulación de los estudiantes Carlos Calderón Ruiz y Pamela Inca Ortiz, para la Facultad de Ingeniería, carrera de Electrónica y Telecomunicaciones. Nos presenta un laboratorio remoto que posee una comunicación servidor-laboratorio utilizando una VPN (Virtual Private Network) con protocolo SSTP (Secure Socket Tunneling Protocol) en RouterOS de Mikrotik, el cual permite la comunicación entre los laboratorios y una red privada. También se utilizó un entorno virtual para el registro de estudiantes, que a más de encargarse de su registro a dichos laboratorios también será el encargado de brindar la visualización de las Prácticas realizadas y videos referentes a la materia teoría electromagnética [37].

"Desarrollo de laboratorio remoto virtual para secuencias de cilindros hidráulicos de un banco de pruebas en el laboratorio de neumática y oleo hidráulica de la facultad de mecánica". Publicado por la Universidad Superior Politécnica de Chimborazo en el año 2019. Propuesta tecnológica de los estudiantes Estefanía Bravo López y Pamela Pino Pilco para la Facultad de Mecánica carrera de ingeniería mecánica. Detalla el desarrollo de un laboratorio remoto virtual para secuencias de cilindros hidráulicos en el laboratorio de neumática y oleo hidráulica, con el din de mejorar el aprendizaje cognitivo y practico de los estudiantes de la asignatura. Mediante el desarrollo del circuito de control conformado por un router con IP fija y publica para el acceso web desde cualquier punto, el uso de una cámara para el acceso remoto, una pantalla HMI para la manipulación de forma local, un PLC para el control y automatización del sistema hidráulico y una Raspberry Pi que cumple con la función de un servidor web y también el almacenamiento de datos de las Prácticas realizadas [38].

"Diseño y desarrollo de un Laboratorio Remoto para la enseñanza de la física en la UNED de Costa Rica". Publicado por la Universidad Nacional del Litoral de Costa Rica en el año 2017. Tesis de Carlos Arguedas Matarrita previo a la obtención del Grado Académico de Doctor en Educación de Ciencias Experimentales para la Facultad de Ciencias

Biológicas y Bioquímica. Detalla la importancia de la creación de laboratorios remotos para la enseñanza y aprendizaje utilizando tecnologías de la información y la comunicación (TIC), a partir de ese conocimiento se planteó el diseño de una propuesta para el desarrollo de un laboratorio remoto que reúna características educativas y tecnológicas acordes al modelo pedagógico de la institución y al desarrollo del estado actual de las tecnologías [39].

CAPITULO III

3 DESARROLLO DE LA PROPUESTA

3.1 COMPONENTES DE LA PROPUESTA

A continuación, se procede con la descripción de los elementos, tanto físicos como lógicos, necesarios para llevar a cabo la implementación de la propuesta.

3.1.1 COMPONENTES FÍSICOS

Para realizar la implementación del laboratorio remoto se requiere de varios componentes electrónicos para el control y automatización del sistema, además de las protecciones eléctricas requeridas para el correcto funcionamiento y prevención de fallos.

3.1.1.1 Router Mikrotik RB2011 UiAS-2HnD-IN

El RB2011 funciona con RouterOS, un sistema operativo de enrutamiento con todas las funciones que se ha mejorado continuamente durante quince años (ver Figura 17). Enrutamiento dinámico, hotspot, firewall, MPLS, VPN, calidad de servicio avanzada, equilibrio de carga y vinculación, configuración y monitoreo en tiempo real, son solo algunas de la gran cantidad de características compatibles con RouterOS [40]. En la Tabla I podemos observar sus características.

TABLA I. CARACTERÍSTICAS TÉCNICAS DEL ROUTER RB2011

DATOS TÉCNICOS	
Modelo	RB2011 UiAS-2HnD-IN
CPU	AR3944
Núcleos de la CPU	1
Frecuencia nominal de la CPU	600 MHz
Licencia RouterOS	Nivel 5
Tamaño de RAM	128 MB
Tamaño del Almacenamiento	128 MB
Estándares inalámbricos de 2,4 GHz	802.11 b/g/n
Ganancia de antena dBi	4
Generación inalámbrica	Wi-Fi 4

Nota: Descripción de datos técnicos de Router RB2011 [40].

Fig. 17. Router MikroTik RB2011 UiAS-2HnD-IN [40].

3.1.1.2 Switch HPE 1920-24G

La serie 1920 de los switch HPE consta de switch Gigabit avanzados con administración inteligente y de configuración fija, diseñados para aplicativos en pequeñas empresas o instituciones al poseer una administración sencilla (ver Figura 18). Posee características personalizables que incluyen características básicas de Capa 2 como VLAN (*Virtual Local Area Network*) y características de Capa 3 como IPv6, ACLs (Access Control List) y Spanning Tree Protocols. En la tabla II se muestran sus características técnicas.

TABLA II. CARACTERÍSTICAS TÉCNICAS DE SWITCH HPE OFFICECONNECT 1920 24G

DATOS TÉCNICOS	
Modelo	Switch HPE OfficeConnect 1920 24G
Puertos y ranuras I/O	24 puertos RJ-45 *auto-negotiating* 10/100/1000
Puertos y ranuras adicionales	1 RJ-45 *console port to access limited* CLI port
Características físicas	Dimensiones 17.32(w) x 6.81(d) x 1.73(h) in (44 x 17.3 x 4.4 cm) (1U height) Peso 4.96 lb (2.25 kg)
Memoria y procesador	MIPS @ 500 MHz, 32 MB flash, 128 MB SDRAM; packet buffer size: 512 KB
Montaje y recinto	*Mounts in an EIA standard 19-inch telco rack or equipment cabinet (hardware included)*

Características eléctricas	Frecuencia 50/60 Hz Voltaje AC 100 - 240 VAC Calificación máxima de potencia PoE (*Power Over Ethernet*) 19 W
Seguridad	UL 60950; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1-03
Administración	IMC—*Intelligent Management Center; limited command-line interface*; navegador Web; SNMP Manager; IEEE 802.3 Ethernet MIB
Notas	Los puertos SFP y los puertos de cobre pueden trabajar simultáneamente, independientes entre sí, para proporcionar un total de 20 puertos con capacidad Gigabit Ethernet

Nota: Se detalla características del Switch HPE [41].

Fig. 18. Switch HPE OfficeConnect 1920 24G [41].

3.1.1.3 PC Servidor Linux

Este es el dispositivo encargado de ejecutar los servicios necesarios para levantar la aplicación web con su respectiva base de datos de los estudiantes, docentes y administradores, cada uno de ellos con un nivel de permisos diferentes según su rol (ver Figura 19). Además, el servidor también es el encargado de comunicarse mediante una API con el Router Mikrotik con la finalidad de darle instrucciones para permitir el acceso

de un estudiante a la PC cliente según el agendamiento previo. A continuación, se puede apreciar las características del servidor en la Tabla III.

TABLA III. CARACTERÍSTICAS TÉCNICAS DEL SERVIDOR LINUX

DATOS TÉCNICOS	
Modelo	Genérico
Mainboard	ASUS H110-D
RAM	2 x 4GB A-DATA DDR4
CPU	Intel Core i5-7400 @ 4x 3.5GHz
Disco Duro	HIKVISION SSD 960GB C100
Sistema Operativo	Ubuntu 22.04 jammy
Kernel Linux	x86_64 Linux 5.15.0-46-generic

Fig. 19. Servidor Linux.

3.1.1.4 PC Cliente

El PC cliente es el equipo al cual las y los estudiantes se conectarán de forma remota para realizar sus prácticas de automatización (ver Figura 20). Este dispositivo contara con el software necesario para realizar la práctica a su plenitud sin necesidad de requerir la instalación de otro programa adicional, además, contara con el hardware suficiente para

ejecutar programas como TIA Portal, LabVIEW y FACTORY IO, los cuales son muy exigentes en cuanto a recursos de procesamiento y consumo de memoria. Las características de la PC cliente se muestra en la tabla IV.

TABLA IV. CARACTERÍSTICAS TÉCNICAS DE LAS PC CLIENTES

DATOS TÉCNICOS	
Modelo	Genérico
Mainboard	ASUS PRIME B365M-A
RAM	16GB DDR4
CPU	Intel Core i7-9700 3GHz
Disco Duro	WDC WD10EZEX-22M 1000GB
Sistema Operativo	Windows 10 Pro
Tarjeta Grafica	NVIDIA GeForce GTX 1650 SUPER 4GB

Fig. 20. PC Cliente.

3.1.1.5 PLC Simatic s7-1200 Siemens AC/DC/Rly

PLC s7-1200 es un dispositivo controlador diseñado para el uso en la industria debido a la robustez con la que fue fabricado, este modelo en particular puede ser utilizado para el control de actuadores según los valores que perciba en sus entradas. Para indicar el estado

tanto de sus salidas como entradas, cuenta con leds en la parte frontal del dispositivo (ver Figura 21). Las características del equipo se muestran en la tabla V.

Fig. 21. PLC 1200 AC/DC/RLY [42].

TABLA V. CARACTERÍSTICAS TÉCNICAS DEL PLC S7-1200

DATOS TÉCNICOS	
Modelo	SIMATIC S7-1200
CPU	1212C
Alimentación AC	120V – 230V
Entradas Digitales	8, 24V
Salidas Relé	6, 2A (30 W DC, 200 W AC)
Entradas Analógicas	2, 0-10 V
Memoria de datos de programación	128 MB
Interfaz	PROFINET 100Mbit/s, MODBUS
Protocolos Ethernet	TCP/IP, DHCP, SNMP, DCP, LLDP
Generación inalámbrica	Wi-Fi 4

Nota: Detalles de PLC S7-1200 [43].

3.1.1.6 Variador de frecuencia modular SINAMICS G120

SINAMICS G120 es el accionamiento universal para las exigencias más diversas en el ámbito industrial y empresarial (ver Figura 22). El diseño modular está compuesto por

una unidad de regulación (*Control Unit, CU*) y un módulo de potencia (*Power Module, PM*), que ofrece un intervalo de potencia de 0.37 W hasta 250 kW.

También cuenta con un panel de operación inteligente IOP (*Intelligent Operator Panel*). Las características técnicas del módulo de potencia y de la unidad de regulación se detallan en la tabla VI y VII respectivamente.

Fig. 22. Variador de frecuencia modular SINAMICS G120 [44].

TABLA VI. CARACTERÍSTICAS TÉCNICAS DE MODULO DE POTENCIA PM240 – 2

DATOS TÉCNICOS	
Designación del tipo de producto	PM240/PM240-2 IP20
Tensión de red	380 – 480 V 3 AC ± 10%
Potencia	0.37 – 200 kW (HO) (Sin Filtrar) 0.37 – 75 kW (LO)(Filtrado)
Compatibilidad electromagnética	Filtro de red opcional disponible clase A o B
Función de freno	Freno resistivo, freno no corriente continua, freno de mantenimiento del motor.
Motores compatibles	Motores trifásicos síncronos y asíncronos
Grado de protección	IP20

Nota: Se detalla las características del módulo PM240-2 [44].

TABLA VII. CARACTERÍSTICAS TÉCNICAS DE LA UNIDAD DE CONTROL CU250S-2 PN

DATOS TÉCNICOS	
Designación del tipo de producto	SINAMICS Control Unit CU250S-2 PN
E/S Digitales	6 ED (3 ED F) 3 SD (1 SD F) 5 ED
E/S Analógica	2 entradas analógicas, 2 Salidas analógicas.
Dimensiones	192x73x165 mm
Comunicación	Profibus, Profinet, Can, RS485

Nota: Se detalla las características técnicas del CU250S-2 PN [44].

3.1.1.7 Raspberry Pi

Raspberry Pi es un microordenador desarrollado para fomentar el aprendizaje de programación e informática y gracias a su bajo costo está al alcance de todos en especial las escuelas y colegios (ver Figura 23).

A pesar de ser un dispositivo muy pequeño del tamaño de una tarjeta de crédito, es potente y en este caso puntual del desarrollo de la propuesta nos ayudará con el control de forma remota del PLC y variador de forma puntual.

A continuación, se presenta una tabla con las características del Raspberry Pi Model B+.

TABLA VIII. CARACTERÍSTICAS TÉCNICAS DE RASPBERRY PI MODEL B+

DATOS TÉCNICOS	
Modelo	Raspberry Pi Model B+.
Sistema en chip o SoC	Broadcom BCM2835 (CPU + GPU + DSP + SDRAM + puerto USB).
CPU	ARM1176JZFS a 700 MHz, con aritmética de punto flotante, arquitectura de 32 bits.
GPU	Broadcom Video Core IV a 250 MHz OpenGL ES 2.0
Vídeo Digital	HDMI 1.4 1920x1200
Vídeo Analógico	RCA vídeo en B y Jack en B+

Memoria RAM	512 MB LPDDR SDRAM a 400 MH
Puertos USB	2 en B y 4 en B+
Salida audio analógico	Conector Jack en B y en B+ incluye también el vídeo analógico
Ethernet	Si
GPIO	26 pines en B y 40 pines en B+
Tamaño	85,6 x 56,5 mm
Almacenamiento	SD-card en B y microSD en B+
Peso	45 gramos

Nota: Se detalla las características de Raspberry Pi Model B+ [45].

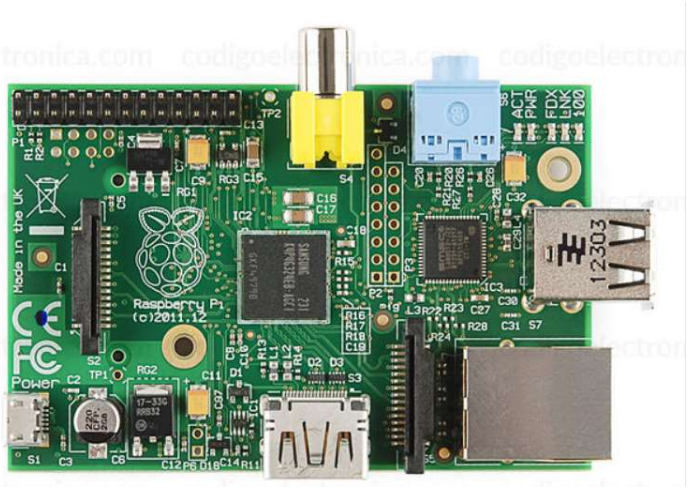


Fig. 23. Raspberry Pi Model B+ [45].

3.1.1.8 Pantalla HMI DOP-B03E211

Para establecer una comunicación directa entre el usuario y la maquina existen las pantallas HMI, el cual posee una interfaz gráfica que le permite al usuario visualizar, monitorear y manipular los debidos procesos que estén ocurriendo en la estación de trabajo, para ello DELTA utiliza DOPSOFT, un programa que ayuda su configuración y programación visual (ver Figura 24). Por lo tanto, los parámetros técnicos se encuentran en la Tabla IX.

Fig. 24. HMI DOP-B03E211 [46].

TABLA IX. CARACTERÍSTICAS TÉCNICAS DE HMI DOP-B03E211

DATOS TÉCNICOS	
Designación del tipo de producto	HMI DOP-B03E211
Tensión de alimentación	24 V
Tipo de display	TFT LCD
Display size	4.3 pulgadas
Resolución del display	480 x 272 pixeles
Display color	TFT LCD
Numero de puertos	2 x 16 bit
Tipo de puerto	COM, Ethernet
Memoria integrada	128 MB
Retroiluminación	Si
Índice de protección IP	IP54
Dimensiones del cuerpo	129 x 103 x 39 mm

Nota: Se detalla las características de HMI DOP-B03E211 [47].

3.1.1.9 Módulo de salidas digitales tipo relé SM 1222

Modulo que permite la expansión de 8 salidas digitales, que permite la interacción con varios actuadores cuando las salidas del PLC utilizado no son suficientes (ver Figura 25), a continuación, en la tabla X se presentan las características técnicas de dicho modulo.

Fig. 25. Siemens S7-1200, DIGITAL OUTPUT SM 1222 [48].

TABLA X. CARACTERÍSTICAS TÉCNICAS DE MÓDULO DE SALIDAS DIGITALES SM 1222

DATOS TÉCNICOS	
Designación del tipo de producto	SM 1222, DQ 8x Relais/2 A
Tensión de alimentación	20.4 V – 28.8 V
Intensidad de entrada	120 mA
Salidas digitales	8
Tensión de salida	5 V DC a 30 V DC
Intensidad de salida	2 A
Retardo a la salida con carga resistiva	10 ms
Interfaz	PROFINET 100Mbit/s, MODBUS
Grado de protección	IP20
Peso	190 g

Nota: Se detalla las características del módulo de salidas digitales SM 1222 [48].

3.1.1.10 Módulo de comunicación MODBUS CM 1241 RS485

Modulo que permite a los dispositivos de la familia S7-1200 tener disponible una capa física RS232 para la comunicación con otros dispositivos e intercambiar datos de manera serial a través de mensajes tipos ASCII, utilizando cable PROFIBUS para su conexión (ver Figura 26). A continuación de detalla las características técnicas del módulo en la Tabla XI.

Fig. 26 Módulo de comunicación CM 1241, RS422/485 [44].

TABLA XI. CARACTERÍSTICAS TÉCNICAS DE MÓDULO DE COMUNICACIÓN CM 1241, RS422/485

DATOS TÉCNICOS	
Designación del tipo de producto	CM 1241 RS 422 / 485
Tensión de alimentación	20.4 V – 28.8 V
Intensidad de entrada	220 mA; de bus de fondo 5 V DC
Pérdidas	1.1 W
Interfaces	RS 422 / 485 (X.27)
Protocolos	Fireport, 3964(R), RTU maestro MODBUS, RTU esclavos MODBUS
Grado de protección	IP20
Alarmas/diagnósticos/información de estado	Si
Temperatura ambiente de servicio	-20 ºC (min) – 60 ºC (Max)
Peso	155 g

Nota: Se detalla las características del Módulo de comunicación CM 1241, RS422/485 [44].

3.1.1.11 Disyuntor SIEMENS 5SL3220-7

Este dispositivo es el encargado principal de la protección de determinado circuito, el cual interrumpe el flujo eléctrico si surge un problema, como por ejemplo que el amperaje el límite aceptable dado en la hoja de datos del producto y cortocircuitos (ver Figura 27).

Estos disyuntores sustituyen en su mayoría a las unidades con fusibles los cuales se utilizaron en posteriori en aplicaciones domesticas e industriales. Las características técnicas de este elemento se presentan en la Tabla XII.

Fig. 27. Módulo de comunicación Disyuntor SIEMENS 5SL3220-7 [49].

TABLA XII. CARACTERÍSTICAS TÉCNICAS DE DISYUNTOR SIEMENS 5SL3220-7

DATOS TÉCNICOS	
Designación del tipo de producto	Miniature circuit breaker 400 V 4.5 kA, 2-pole, C, 20 A
Números de polos	2
Voltaje	440 V AC
Voltaje soportado	400 V Max, 72 V min
Frecuencia	50/60 Hz
Protección	IP20
Capacidad de switcheo	EN 60898 4.5kA
Disipación	2.2 W.
Corriente	20 A.
Peso	23 g

Nota: Se detalla las características del Disyuntor SIEMENS 5SL3220-7 [49].

3.1.1.12 Contactor

El contactor dentro de la estación de trabajo es debido a su uso para el correcto encendido del motor trifásico ya que este necesita de un sistema de protección previo (ver Figura

28), para evitar cortos o picos de amperaje, los que podrían afectar al funcionamiento del motor. Otro uso que se le dio al contactor es para el encendido del variador de frecuencia modular SINAMICS G120, éste por ser un dispositivo cuya alimentación es de 220v necesita de un sistema de protección, y se decidió usar el contactor para realizar un sistema de control a 120v, y un sistema de enclavamiento. Los datos técnicos del contactor a utilizar se detallan en la Tabla XIII.

Fig. 28. Contactor CHINT NXC-12.

TABLA XIII. CONTACTOR CHINT NXC-12

DATOS TÉCNICOS	
Designación del tipo de producto	AC CONTACTOR NXC-12
Tipo de producto	CONTACTOR
Número de polos	3
Contactos auxiliares	1 NA + 1 NC
Frecuencia	50/60 Hz
Amperio operativo	12 amperios
Voltaje nominal	120 v AC
Montaje	Riel DIN de 35mm
Estándar	IEC/EN60947-4-1

Nota: Se detalla las características del Contactor CHINT NXC-12.

3.1.1.13 Sensor de Temperatura PT100

Los sensores de temperatura o termorresistencias operan en base al principio de variación de dicha resistencia eléctrica en función a la temperatura. La conocida PT100 o RTD

(Resistance Temperature Detector) es una termorresistencia de platino cuya resistencia óhmica es de 100 ohm a 0 C, con escala de trabajo que oscila entre los -200 a 400 C.
En la medición de temperatura con termorresistencia a 3 hilos la distancia puede ser hasta 30 metros aproximadamente (ver Figura 29).

Fig. 29 Sensor de Temperatura PT100.

3.1.1.14 Controlador de temperatura DTB4848

El uso de este controlador de temperatura es debido a que las entradas analógicas del PLC ubicado en la estación de trabajo ya tienen dichas salidas ocupadas para las prácticas realizadas de manera presencial en el laboratorio, se realizó la comunicación MODBUS RTU RS485 de este controlador de temperatura hacia el módulo de comunicación CM 1241 RS422/485 del PLC S71200.

Algunas características de este controlador (ver Figura 30) son [50]:

- Control de los modos de entrada PID/ON-OFF/manual
- Construido en 2 grupos de interruptores de alarma con 13 modos de alarma de temperatura Celsius y Fahrenheit.
- Interfaz de comunicación opcional RS485 (Modbus ASCII, RTU, la tasa de baudios: 2400-38400).
- Toma de muestras del sensor: 0,5 segundos/hora
- Certificaciones: IP5X, CE, UL

Fig. 30. Controlador de Temperatura DTB4848 [50].

3.1.1.15 Motor eléctrico trifásico Siemens D80

Debido a su potencia y tamaño este tipo de motores son usados mayormente en la industria (ver Figura 31), diseñados para ser resistentes en el trabajo, a continuación, se presenta una tabla con las características principales de este motor.

Fig. 31. Motor trifásico 1LE0142-0DB26-4AA4-Z D80 [51].

TABLA XIV. CARACTERÍSTICAS TÉCNICAS DE SIMOTICS GP 1LE0142-ODB26-4AA4-Z D80

DATOS TÉCNICOS	
Designación del tipo de producto	1LE0142-0DB26-4AA4-Z D80
Tipo de producto	Motor de jaula de ardilla trifásico

Número de polos	4
Tensión nominal	400 V
Frecuencia	60 Hz
Velocidad nominal	1735 rpm
Torque nominal	3Nm
Corriente nominal	1.49 A en 440 V
Corriente de arranque	6 A.
Clase de eficiencia	IEC 60034-30
Factor de potencia	0.77
Factor de servicio	1.15

Nota: Se detalla las características del SIMOTICS GP 1LE0142-ODB26-4AA4-Z D80 [44].

3.1.2 COMPONENTES LÓGICOS

En este segmento se detallan los diferentes programas o softwares que son necesarios tanto para el diseño de la propuesta como para el funcionamiento y posterior mantenimiento o actualización de los diferentes sistemas.

3.1.2.1 Winbox

WinBox es una pequeña aplicación que nos permite la administración de Mikrotik RouterOS usando una interfaz gráfica (ver Figura 32).

Incluye una sofisticada tecnología para realizar estas conexiones basada en el sistema operativo RouterOS.

Este software permite a sus usuarios realizar conexiones vía FTP, Telnet y SSH (*Secure Shell*). Incluye también una API que permite crear aplicaciones personalizadas para monitorizar y administrar [52].

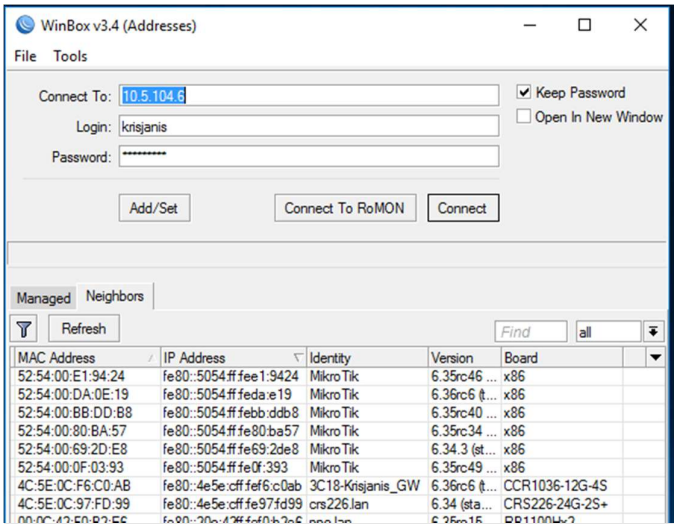


Fig. 32. Software WinBox [40].

3.1.2.2 RouterOS API

La API (*Application Programable Interface*) de MikroTik permite desarrollar aplicaciones para comunicarse con RouterOS con el propósito de recopilar y ajustar información, y administrar los equipos que tengan ese sistema operativo.

Este servicio se encuentra deshabilitado por defecto dentro de la configuración del router, utilizando el puerto TCP 8798 para su comunicación [53].

La comunicación con el router es realizada por medio de la secuencia orden/respuesta, es decir, el usuario que quiere acceder a la terminal del equipo realiza una serie de órdenes y el equipo responde en la medida que estas órdenes son realizadas [54]. La codificación de instrucciones o palabras de la API se muestran en la tabla XV.

TABLA XV. CODIFICACIÓN DE PALABRAS EN LA API MIKROTIK.

Value of length	# of bytes	Encoding
0 <= len <= 0x7F	1	len, lowest byte
0x80 <= len <= 0x3FFF	2	len | 0x8000, two lower bytes
0x4000 <= len <= 0x1FFFFF	3	len | 0xC00000, three lower bytes
0x200000 <= len <= 0xFFFFFFF	4	len | 0xE0000000
len >= 0x10000000	5	0xF0 and len as four bytes

Nota: Codificación de palabras en la API Mikrotik [53].

3.1.2.3 MobaXterm

Es una de las aplicaciones más utilizadas por administradores de redes y sistemas a nivel global.

Mobaxterm es un potente terminal que sirve para el sistema operativo Windows. Entre sus características principales se encuentran herramientas muy útiles para administradores tales como: cliente SSH, RDP, FTP, VNC, etc., además cuenta también con la posibilidad de levantar servidores SSH/SFTP, FTP, HTTP, Telnet, entre otros, aunque todos estos servicios funcionan de forma limitada en la versión gratuita de la aplicación (ver Figura 33).

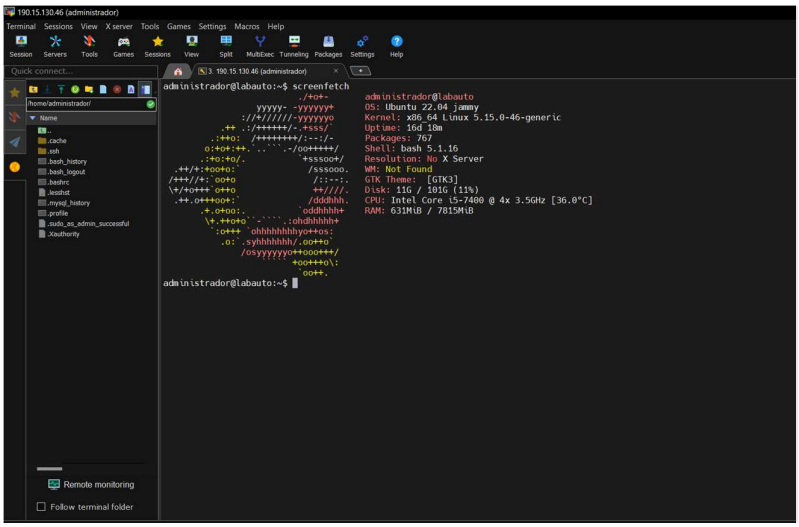


Fig. 33. Software MobaXterm.

3.1.2.1 OpenVPN

OpenVPN es un protocolo VPN de código abierto que utiliza técnicas de red privada virtual (VPN) para establecer conexiones seguras de sitio a sitio o de punto a punto.

OpenVPN utiliza el protocolo TLS/SSL para el intercambio de claves y puede atravesar cortafuegos y traductores de direcciones de red (NAT). Lo escribió James Yonan y se publicó bajo la Licencia Pública General de GNU (GPL).

OpenVPN permite que los pares se autentiquen entre sí mediante un nombre de usuario y una contraseña, certificados o una clave secreta previamente compartida. Cuando se utiliza en una configuración de servidor multi cliente, permite que el servidor inicie un

certificado de autenticación para cada usuario, utilizando una autoridad de certificación y una firma. Utiliza la biblioteca de cifrado OpenSSL, así como los protocolos TLSv1/SSLv3 y tiene una serie de características de control y seguridad [55].

OpenVPN ha sido portado a varias plataformas, incluyendo Linux y Windows, y su configuración también está en cada uno de estos sistemas, por lo que facilita su soporte y mantenimiento. OpenVPN puede ejecutarse a través de transportes de UDP (*User Datagram Protocol*) o TCP (Transfer Control Protocol), multiplexando túneles SSL creados en un solo puerto TCP / UDP. OpenVPN es uno de los pocos protocolos VPN que puede hacer uso de un proxy, lo que a veces puede ser útil.

Actualmente, las características no compatibles de OpenVPN:

- Compresión LZO
- Autenticación TLS
- Autenticación sin nombre de usuario/contraseña

El nombre de usuario de OpenVPN está limitado a 27 caracteres y la contraseña a 233 caracteres [56].

En la Figura 34 se muestra un ejemplo donde una oficina cuenta con la dirección IP publica 2.2.2.2 y se requiere que dos clientes remotos tengan acceso a las redes internas del Router, esta tarea puede ser solventada mediante la implementación del protocolo OpenVPN que incluye RouterOS cualquier Router empresarial Mikrotik.

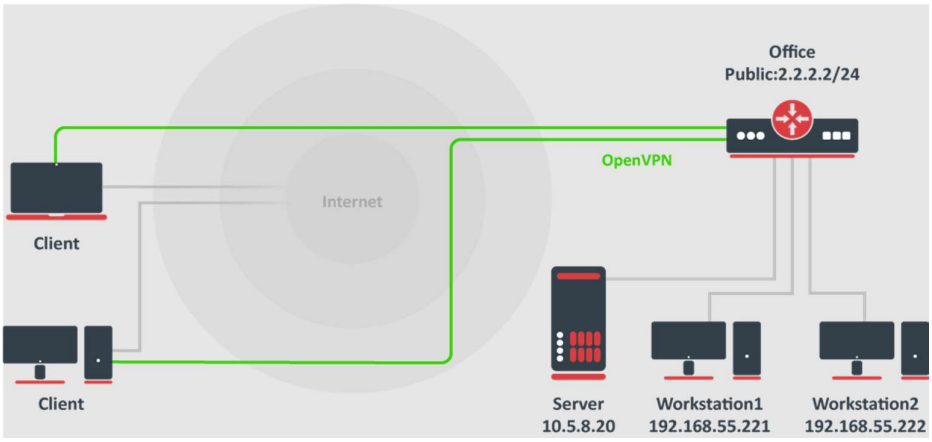


Fig. 34. Funcionamiento de OpenVPN [56].

3.1.2.2 Servidor LNMP

LNMP es el acrónimo para Linux, Nginx, MySQL, PHP, cuatro tecnologías que son parte de esta plataforma que corre desde el lado del servidor [57].

- **Linux:** Sistema operativo y base de la plataforma.
- **Nginx:** Servidor web, open source de alta perfomance.
- **MySQL:** Servidor de base de datos.
- **PHP:** Lenguaje de programación web.

SQL

El lenguaje de consulta estructurado SQL (*Structured Query Language*), es un lenguaje normalizado de base de datos, de los que hacen uso los diferentes motores de bases de datos al efectuar consultas, operaciones sobre los datos o sobre la estructura en sí [58].

Entre las componentes de este lenguaje tenemos lo siguiente:

Comandos

- **DDL:** Permite crear y definir nuevas bases de datos.
- **DML:** Permite generar consultas para ordenar, filtrar y extraer datos de la base de datos [59].

A continuación, se detallan algunos comandos DDL y DML:

- **CREATE:** crea tablas, campos e índices nuevos.
- **DROP:** Elimina tablas e índices
- **ALTER:** Modifica las tablas, agrega campos.
- **SELECT:** Consulta registros de la base de datos.
- **INSERT:** Carga datos en la base de datos.
- **UPDATE:** Modifica valores de los campos dentro de la base de datos.
- **DELETE:** Elimina registros de una tabla.

Cláusulas

Son condiciones que ayudan a modificar los datos seleccionados.

- **FROM:** Especifica la tabla de la cual se seleccionará los datos.
- **WHERE:** Especifica las condiciones que deben de poseer los registros para ser seleccionados.
- **ORDER BY:** Se utiliza para ordenar los registros.

Operadores Lógicos.

- **AND:** Evalúa dos condiciones y retorna un verdadero si las dos son verdaderas.
- **OR:** Evalúa dos condiciones y retorna un verdadero de una de las dos es verdadera.

PHP

Acrónimo recursivo para *Hypertext Preprocessor*, es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML.

PHP se distingue al resto de lenguaje de programación, ya que el código es ejecutado en el servidor, generando HTML y enviándolo al cliente [60].

PHP es lo que se denomina una tecnología del servidor, que ahora se suele englobar dentro de lo llamado “Backend”.

PHP en la actualidad es una multiplataforma, que fue inicialmente desarrollado para entornos Linux y es donde se le puede sacar el mayor provecho. El estilo de programación con PHP es totalmente libre, por lo que se puede usar programación estructurada como las funciones, programación orientada a objetos [61].

A continuación, se detallan algunas funciones que ofrece PHP:

- Funciones de correo electrónico.
- Gestión de bases de datos: PHP ofrece interfaces que permite el acceso a la mayoría de las bases de datos, así como los de sistemas Microsoft.

- Gestión de archivos: a través de librerías de funciones de PHP se puede crear, borrar, mover, modificar cualquier archivo.
- Tratamiento de imágenes.

3.1.2.1 RDP

Microsoft proporciona protocolo de RDP como una solución para conexiones remotas entre equipos y/o servidores. RDP está integrado en el sistema operativo y es compatible con los sistemas operativos Windows y Mac. RDP proporciona una interfaz gráfica fácil de usar para conectarse y acceder a la computadora remota. Se requieren dos versiones de software separadas. El equipo al que se tiene acceso debe ejecutar el software del servidor RDP, mientras que el usuario que desea acceder al servidor debe ejecutar la versión de cliente de RDP [62].

3.1.2.2 AnyDesk

AnyDesk es un software propietario que es compatible con todos los sistemas operativos comunes. AnyDesk es de uso gratuito para usuarios privados. Para conectarse de forma remota, ambas computadoras deben descargar y ejecutar AnyDesk. Cuando inicie AnyDesk, le mostrará el ID personal de esa computadora. Comparta esa ID con la persona a la que desea otorgar acceso a su máquina. AnyDesk le permite compartir el acceso al teclado y al ratón, así como capturas de pantalla del escritorio. Si bien hay otros productos similares disponibles en el mercado, AnyDesk los supera con la velocidad a la que se ejecuta.

3.1.2.3 TeamViewer

TeamViewer es una plataforma de conectividad remota basada en la nube que permite conectarte a cualquier dispositivo, desde cualquier lugar, en cualquier momento. TeamViewer conecta computadoras, smartphones, servidores, dispositivos del IoT, robots, etc., con conexiones rápidas y de alto rendimiento a través de una red de acceso global, incluso en el espacio exterior o en entornos con ancho de banda corto. La plataforma de acceso y asistencia remotos de TeamViewer es flexible y escalable sin requerir el uso de VPN [63].

3.1.2.4 Totally Integrated Automation (TIA) Portal

Totally Integrated Automation es la plataforma de ingeniería de Siemens que ofrece soluciones de automatización en todos los sectores industriales del mundo, integrando todas las tareas de automatización de un proceso industrial. Se trata de una aplicación modular a la que se le pueden ir añadiendo nuevas funcionalidades según las necesidades concretas de cada sector [64].

3.1.2.5 DOPSoft

DOPSoft es un software que sirve para que los usuarios puedan programar las pantallas HMI de la serie Delta y así lograr el control y monitoreo de los diferentes sistemas o plantas industriales donde vayan a implementarse.

3.1.2.6 CADe Simu

Se trata de un programa electrotécnico, en el que es posible introducir los símbolos de forma organizada como librerías. Posteriormente, el sistema trazará un esquema eléctrico de manera fácil y rápida a fin de realizar la simulación. Luego de esto, el programa visualizará el estado del componente eléctrico, así como resaltará los conductores eléctricos de la corriente eléctrica.

A través de la interfaz CAD, la persona o usuario podrá dibujar el esquema de una manera más rápida y fácil. Cuando se haya terminado de realizar el esquema completo con el uso de la simulación, se podrá analizar el funcionamiento correcto de la misma. [65]

3.1.2.7 GNS3

GNS3 es un software utilizado por cientos de miles de ingenieros de redes a nivel mundial para emular, configurar, probar y solucionar problemas de redes virtuales y reales. Le permite ejecutar una pequeña topología que consta de solo unos pocos dispositivos en su computadora portátil, a aquellos que tienen muchos dispositivos alojados en múltiples servidores o incluso alojados en la nube [66].

3.1.2.8 SketchUp

SketchUp es un programa de modelado 3D que puede utilizarse para crear objetos 3D en un entorno 2D. Ya sea que se planee modelar para impresiones 3D o para otros fines.

Este programa nos ofrece todas las herramientas necesarias para producir resultados profesionales y de calidad, inclusive si no se tiene mucha experiencia en modelado 3D [67].

3.1.2.9 Factory I/O

Factory I/O es un simulador de fabrica en 3D, para aprender sobre tecnologías de automatización (ver Figura 40). Diseñada para ser fácil de usar, permite construir rápidamente una fábrica virtual utilizando una gama de piezas industriales comunes. También incluye fabricas prediseñadas, inspiradas en aplicaciones industriales típicas, con niveles de dificultad que van desde principiantes hasta avanzado.

El escenario más común es utilizar Factory I/O para el uso de PLCs ya que son los controladores más comunes en aplicaciones industriales, sin embargo, también se puede usar microcontroladores, SoftPLC, Modbus, entre otras tecnologías [68].

3.2 DESARROLLO DE LA PROPUESTA

En la presente sección se explicará el diseño de los diferentes elementos que componen el sistema de laboratorio remoto, desde la elaboración de diagrama de red interna del laboratorio hasta infraestructura final del sistema de agendamiento, pasando por las debidas protecciones eléctricas requeridas en cada etapa de análisis.

3.2.1 DISEÑO RED INTERNA DEL LABORATORIO

3.2.1.1 Topología física de la red

En el diseño físico de la red se procedió a instalar un Router MikroTik dentro del laboratorio con la finalidad de usar las diferentes funcionalidades que éste ofrece tales como tener la capacidad de montar un servidor VPN, generación de certificados de autenticación, firewall embebido, y sobre todo por la capacidad de automatizar la red

realizando acciones como el encendido de las computadoras y el monitoreo de estas, todo ello a través de la API desarrollada para PHP (ver Figura 35).

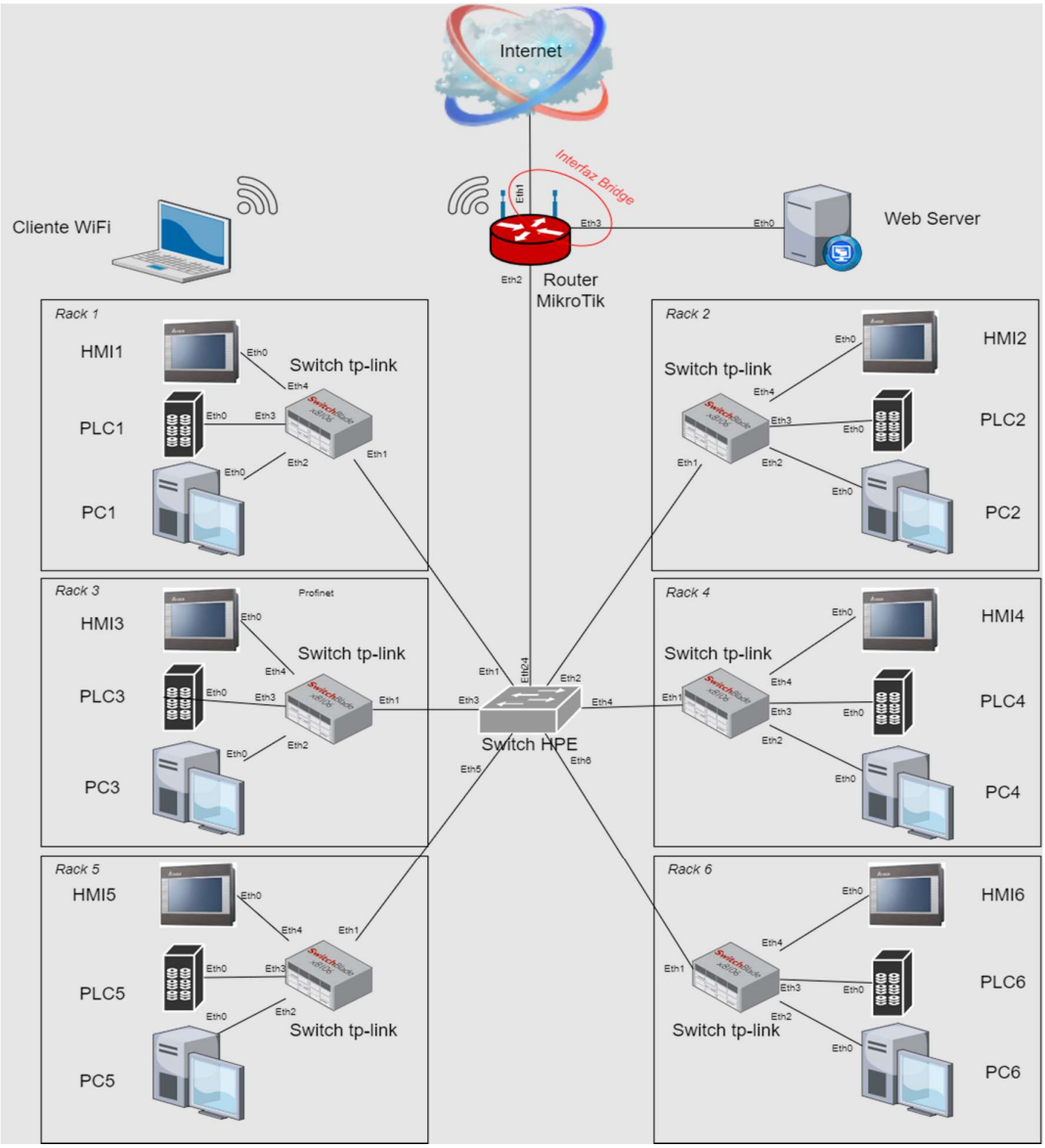


Fig. 35. Topología física de la red interna del laboratorio.

Como se puede apreciar en la Figura 35, la conexión de los elementos perteneciente a cada Rack se lo realiza mediante un switch no administrable de la marca TP-Link, y éste se conecta con el switch HPE que distribuye la red a todo el laboratorio, permitiendo que cada elemento se comunique con el Router MikroTik. Por tanto, es necesario resaltar que el servidor Web está conectado a través de una interfaz bridge hacia la red exterior del laboratorio, lo cual significa que tanto el router como el servidor se encuentran en el mismo segmento de red, dando como resultado que se pueda acceder al aplicativo web y

al router MikroTik a través de cualquier IP publica asignada por el departamento de TICs de la UPSE.

En las Figuras 36 y 37 se muestra la configuración de para la interfaz Bridge realizada dentro del MikroTik.

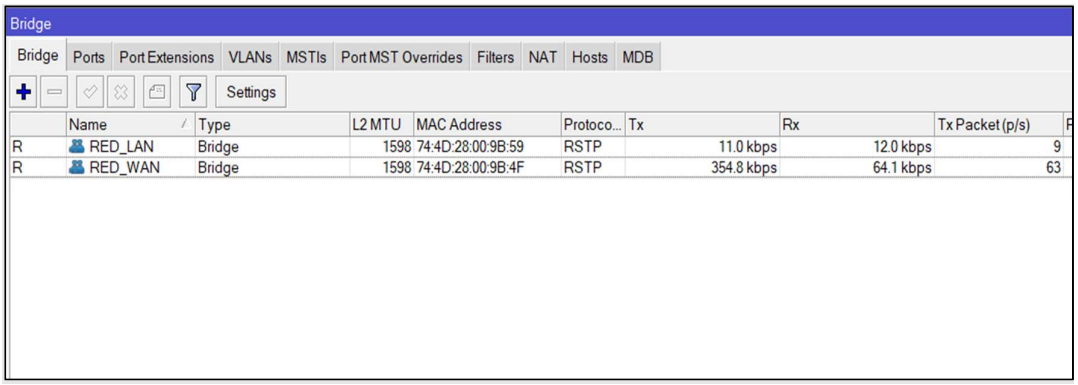


Fig. 36. Interfaces Bridge creadas dentro del MikroTik

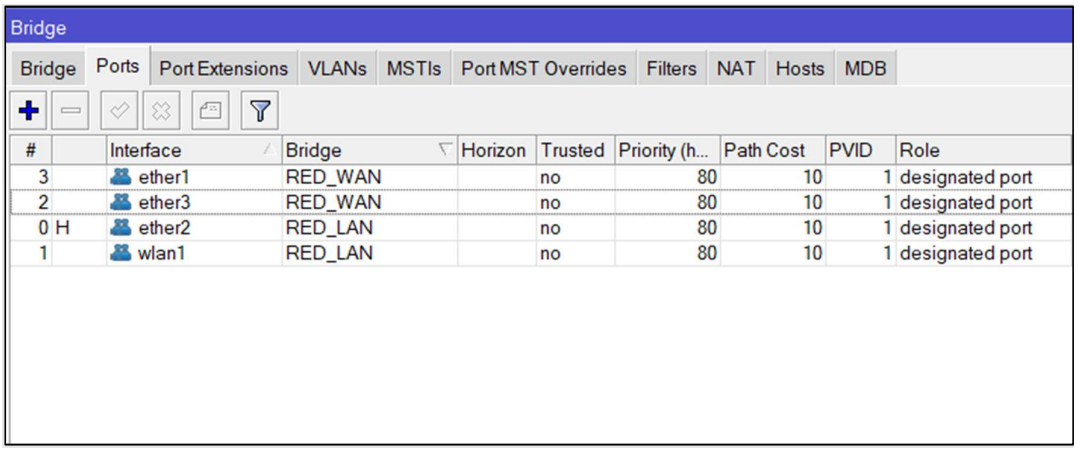


Fig. 37 Puertos pertenecientes a cada Bridge

En la Figura 37, se muestra que también existe otro Bridge entre la interfaz ether2 y la interfaz wlan1, esta configuración sirve para que cualquier estudiante o docente que se encuentre de forma física en el laboratorio, pueda acceder a la red interna desde cualquier dispositivo compatible con Wi-Fi, como una laptop o Smartphone, además, permite futuras aplicaciones de Internet de las cosas (IoT).

3.2.1.2 Topología lógica de la red

Una vez realizadas todas las conexiones físicas de la red, se debe de proceder con el diseño lógico, en donde se configura los diferentes dispositivos de la red con una dirección lógica (IP), de tal forma que no se repitan entre sí, además, todas ellas pertenezcan a un mismo segmento de red dando como resultado la comunicación entre los elementos. En la tabla XVI se indica las direcciones IP que serán asignadas a cada dispositivo, teniendo en cuenta que la red elegida para usarse dentro del laboratorio será la 192.168.0.0/24, y que el Default Gateway para dicha red será la dirección 192.168.0.254 que se encuentra asignada a la interfaz Bridge RED_LAN del Router MikroTik.

TABLA XVI. DIRECCIONES LÓGICAS DE LOS DISPOSITIVOS DEL LABORATORIO

Elemento	Dirección IP
PLC1	192.168.0.1/24
PLC2	192.168.0.2/24
PLC3	192.168.0.3/24
PLC4	192.168.0.4/24
PLC5	192.168.0.5/24
PLC6	192.168.0.6/24
HMI1	192.168.0.21/24
HMI2	192.168.0.22/24
HMI3	192.168.0.23/24
HMI4	192.168.0.24/24
HMI5	192.168.0.25/24
HMI6	192.168.0.26/24
PC1	192.168.0.31/24
PC2	192.168.0.32/24
PC3	192.168.0.33/24
PC4	192.168.0.34/24
PC5	192.168.0.35/24
PC6	192.168.0.36/24
SWITCH HPE	192.168.0.200/24
Web Server	192.168.23.11/24

El servidor web es el único dispositivo que no pertenece al mismo segmento de red que los demás elementos, esto se debe a que el servidor está conectado a la red externa al laboratorio a través de la interfaz bridge RED_WAN, y en dicha red se trabaja con el segmento 192.168.23.0/24, cabe recalcar que el servidor obligatoriamente debe contar con la IP 192.168.23.11 debido a que es a esta dirección a la que apunta el enrutamiento de la UPSE cuando se ingresa desde el exterior por medio de la IP publica asignada al proyecto.

En la Figura 45 se muestra las direcciones asignadas a las interfaces bridge del Router Mikrotik tanto para la RED_LAN (Red interna del laboratorio) como para la RED_WAN (Red externa al laboratorio).

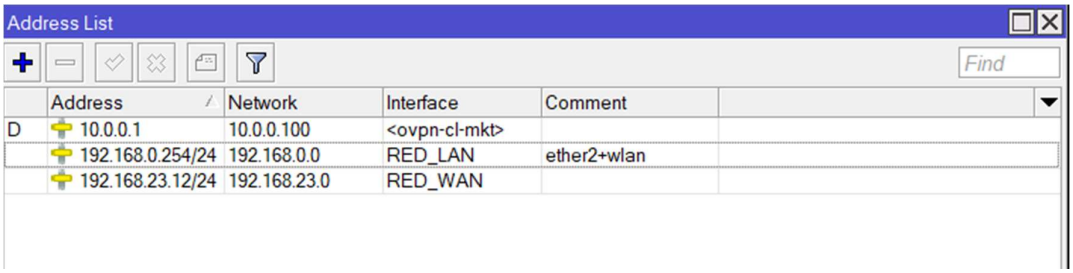


Fig. 38. Lista de direcciones de las interfaces Bridge del Router MikroTik.

3.2.1.3 Rack de comunicaciones

El rack de comunicaciones está conformado por dos elementos de red y un computador con sistema operativo Ubuntu Server que hará como servidor web y de base de datos. En los elementos de red contamos con un Router Mikrotik RB2011 UiAS-2HnD-IN y con un switch HPE OfficeConnect 1920 24G.

El rack de comunicaciones y sus elementos se muestra junto con su regleta eléctrica de protección en la Figura 39.

Fig. 39. Rack de comunicaciones del laboratorio de automatización.

3.2.2 ACCESO REMOTO POR VPN

Todo estudiante o docente que requiera acceder a algún equipo dentro del laboratorio de automatización de forma remota requiere un método de conexión segura para evitar que los datos sean interceptados por algún tercero con intenciones maliciosas, por ello, a continuación, se presenta las medidas implementadas en el proyecto para garantizar la seguridad de los datos del usuario.

3.2.2.1 Diseño de la VPN

Para que un estudiante pueda acceder de forma remota a los recursos fiscos del laboratorio, tendrán que hacer uso de la aplicación OpenVPN.

En primer lugar, se debe realizar un diseño global que permita entender el funcionamiento y modo de operación de la VPN, analizando desde el momento en el que un estudiante desea realizar una práctica desde su domicilio o cualquier otro lugar externo a la universidad hasta su conexión con el computador donde realizara dicha práctica con los elementos del laboratorio. El diagrama al que nos referimos se puede apreciar en la Figura 40.

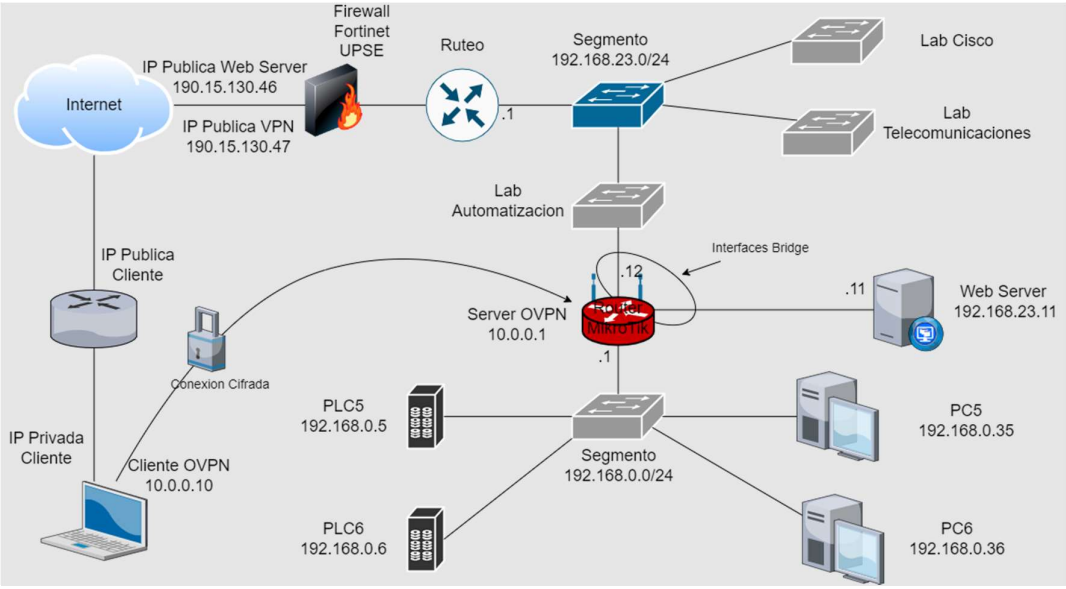


Fig. 40. Diseño topológico de la red VPN.

Como se puede observar en la Figura 40, un cliente remoto puede acceder a una red privada haciendo uso de una VPN. En el caso puntual del laboratorio de automatización de la UPSE el Router MikroTik es el servidor OpenVPN donde se encuentran los certificados que permiten el acceso de los estudiantes hasta el laboratorio, así mismo, se encarga de brindar una capa de seguridad cifrando los datos a través de un túnel VPN.

Para realizar la conexión con la VPN desde un lugar externo al laboratorio se requiere que previamente el estudiante cuente con un certificado firmado digitalmente por el servidor VPN y sus credenciales únicas de acceso. Por lo tanto, toda esta información debe de ingresarse al cliente OpenVPN instalado en su computador para que la conexión sea válida. En modo de conexión de un cliente remoto se detallará más adelante en la sección de anexos.

Una vez que la conexión con la VPN sea exitosa, si el cliente remoto cuenta con una reservación previa a través del aplicativo web para el agendamiento, entonces prosigue con la conexión mediante RDP hacia el computador que haya reservado.

3.2.2.2 Diseño e Implementación de OpenVPN en Router MIKROTIK

Para realizar las pruebas de funcionamiento del protocolo OpenVPN en un Router MikroTik se ha elaborado un ambiente de pruebas simulando las computadoras del laboratorio de automatización y, a un usuario remoto que contara con un dispositivo con

sistema operativo Windows para comprobar la conexión con los elementos internos del laboratorio.

El diseño de la red fue elaborado en GNS3 debido a la funcionalidad de emular imágenes de sistemas reales como RouterOS y Windows, el diagrama de la red se muestra en la Figura 41.

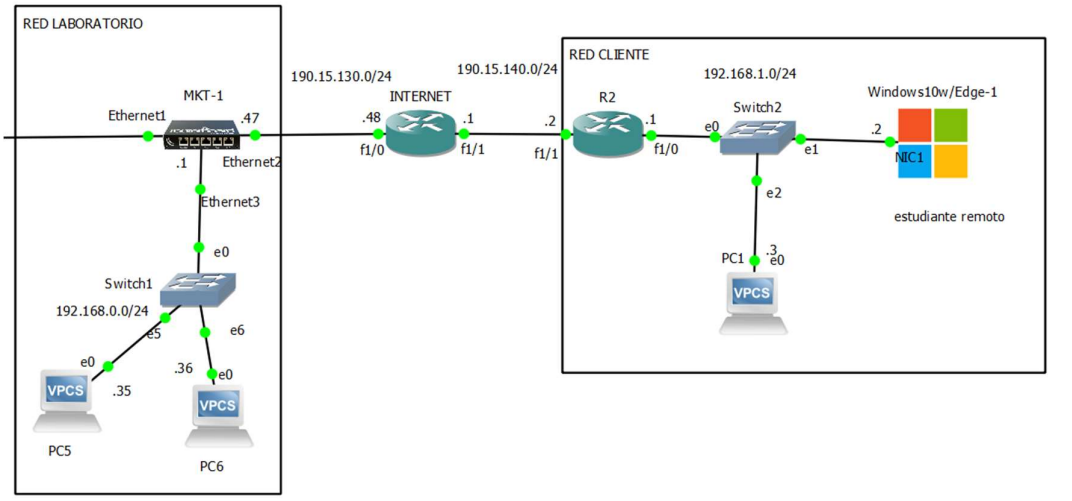


Fig. 41. Diseño de la red para pruebas.

En la Figura 41 contamos con 3 elementos que pueden identificarse a simple vista:

- El primer elemento es la red del laboratorio, en donde se empieza desde el Router MikroTik en la parte superior hasta los PCs clientes en la parte inferior que para esta prueba se realizara con solamente 2 computadoras, la PC5 y la PC6 respectivamente.
- Como segundo elemento tenemos al Router que lleva por nombre “INTERNET”, este equipo simulará a todo el enrutamiento desde el exterior a la universidad que conecta la IP pública del cliente remoto con la IP pública del laboratorio.
- El último elemento es la red del cliente, la cual consta de un Router y un switch, los cuales en un ambiente real serian reemplazados por un único elemento que cumpliría ambas funciones, y es el Router/Switch que utilizan los proveedores de internet o una ONU (*Optical Network User*) en caso de contar con servicio de fibra óptica residencial o FTTH (*Fiber To The Home*). Los otros dispositivos son 2 computadores, uno de ellos con sistema operativo Windows para posteriormente instalar el cliente OpenVPN y realizar la prueba de funcionamiento.

Con todo el enrutamiento habilitado solo podrán tener conectividad las IP públicas entre sí, más no las redes privadas, esto se debe a que las redes privadas no se enrutan a nivel de proveedores del internet y por otra parte a que las redes privadas se comunican con internet a través de un Router haciendo uso de un mecanismo de traducción de direcciones o NAT.

Los resultados que se obtienen si se realiza una prueba de conexión con el protocolo ICMP desde la computadora con Windows tanto a la IP pública del Router Mikrotik como a una PC dentro de la red del laboratorio se muestran en la Figura 42.

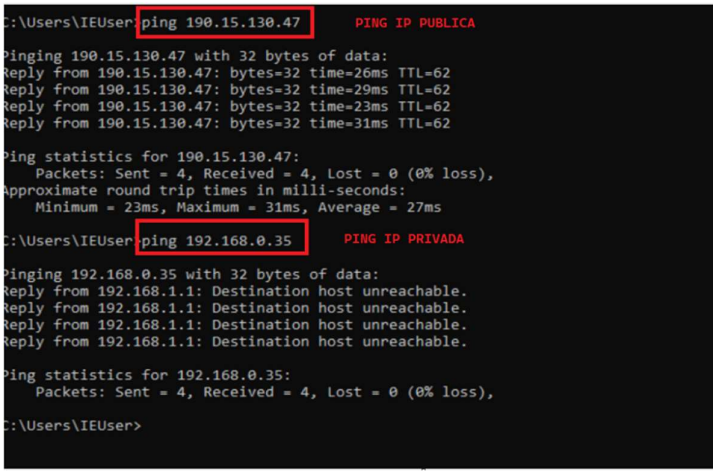


Fig. 42. Prueba ICMP a una IP publica y una IP privada.

Los resultados que se obtienen al realizar esta prueba son los esperados, la única respuesta exitosa es la que se hizo a la dirección IP pública, como la IP privada no se enruta hacia internet, el host remoto no tiene forma de llegar hacia ese destino.

Para lograr que un host tenga conectividad con una red privada remota debe de existir una VPN, por lo tanto, a continuación, se indican los pasos para el levantamiento de un servidor OpenVPN dentro de un Router Mikrotik.

Inicialmente, se realiza la conexión al Router Mikrotik por medio de la aplicación WinBox, y luego, como primer paso, se procede con la generación de los certificados para el servidor y para los clientes.

En la sección de certificados agregamos uno nuevo para la entidad certificadora, tal como se muestra en las Figuras 43 y 44.

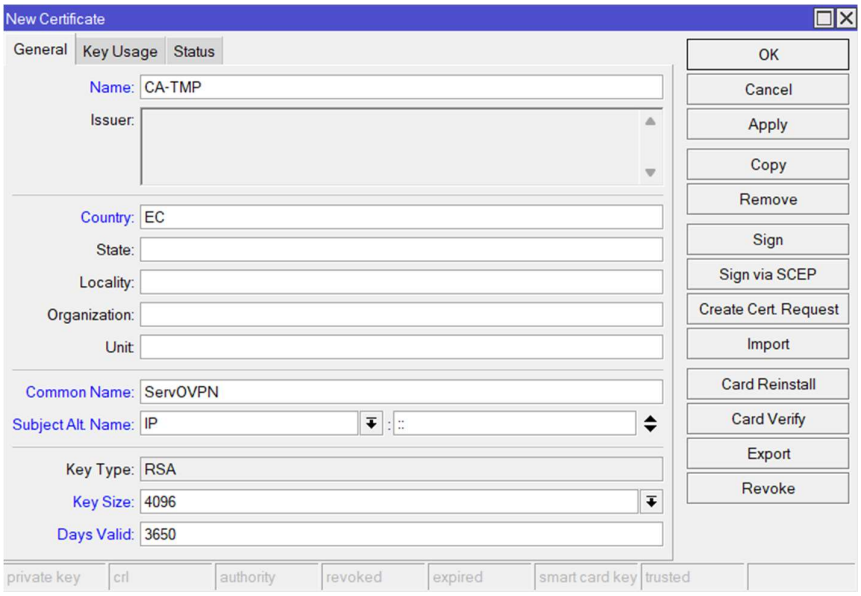


Fig. 43. Datos generales para certificado CA.

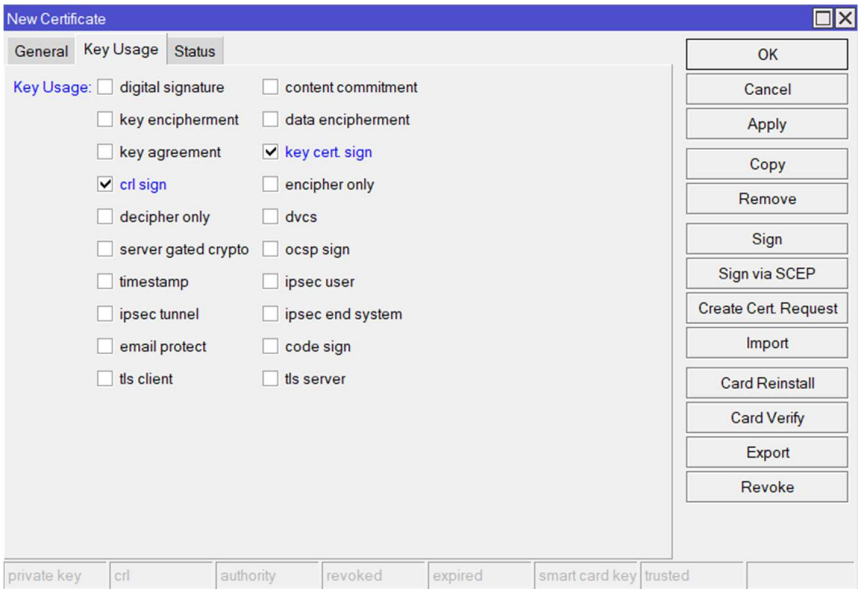


Fig. 44. Llaves habilitadas para el certificado CA.

Luego del certificado CA debemos crear el certificado para el servidor VPN con los valores mostrados en las Figuras 45 y 46.

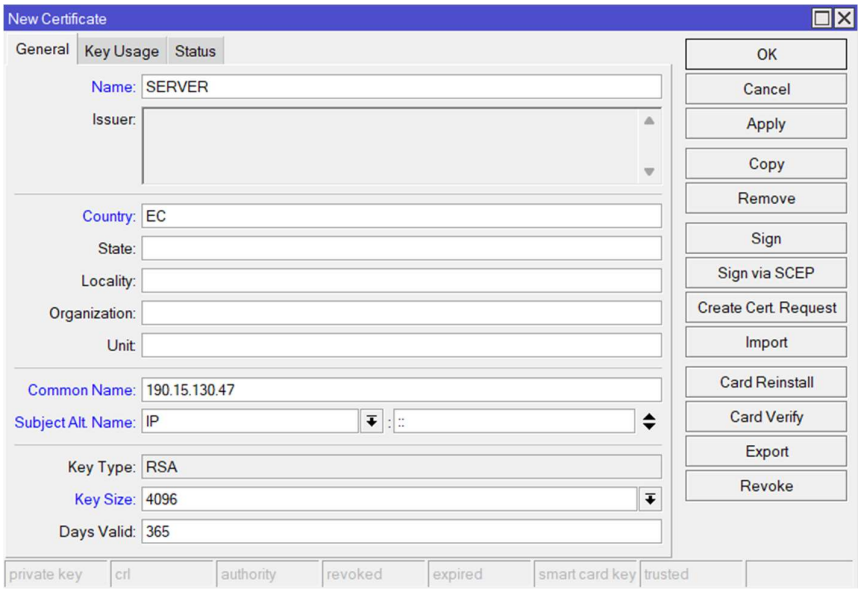


Fig. 45. Datos generales para certificado SERVER.

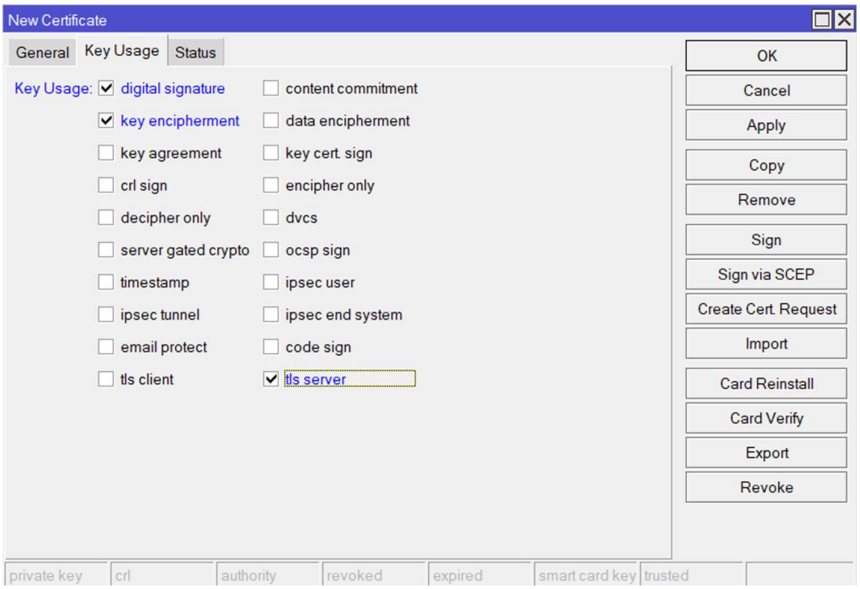


Fig. 46. Llaves habilitadas para el certificado SERVER.

Por último, se deben de crear los certificados de los clientes, por otra parte debido a que la prueba será realizada en un ambiente emulado, y con un Router Mikrotik virtualizado sin licencia, solo podremos tener conectado a un solo cliente VPN a la vez, en otras palabras, únicamente se generara un certificado de cliente, con los valores que de muestran en la Figura 47 y 48.

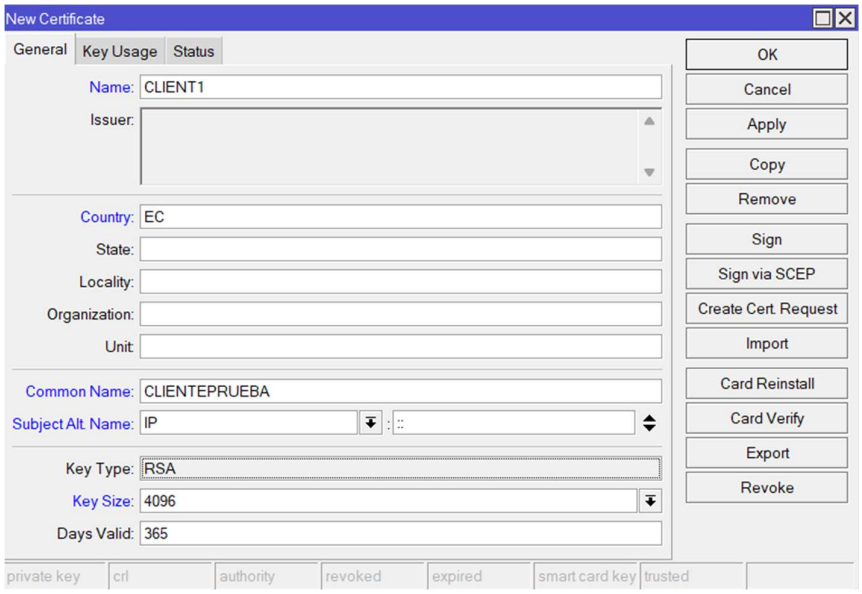


Fig. 47. Datos generales para certificado CLIENT1.

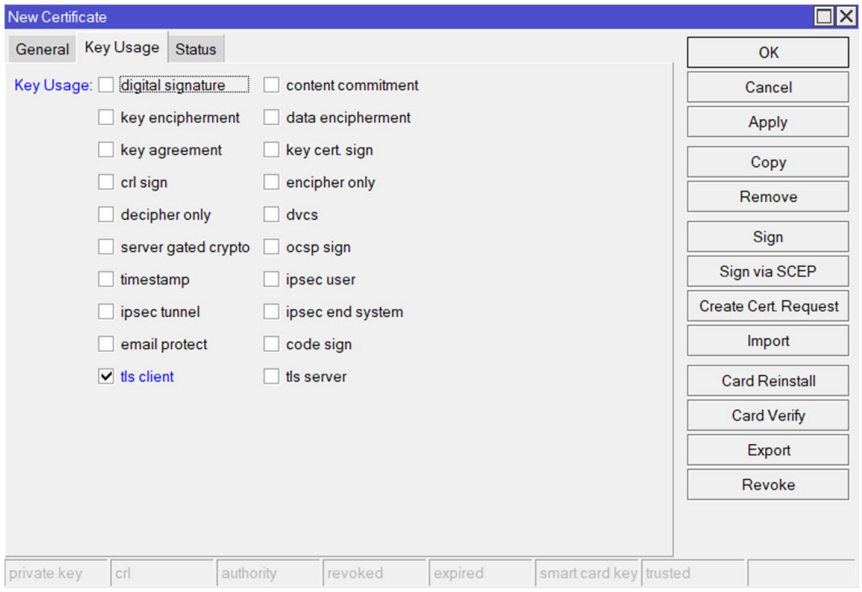


Fig. 48. Llaves habilitadas para el certificado CLIENT1.

Una vez creados estos certificados deben de aparecer los 3 certificados como se muestra en la Figura 49.

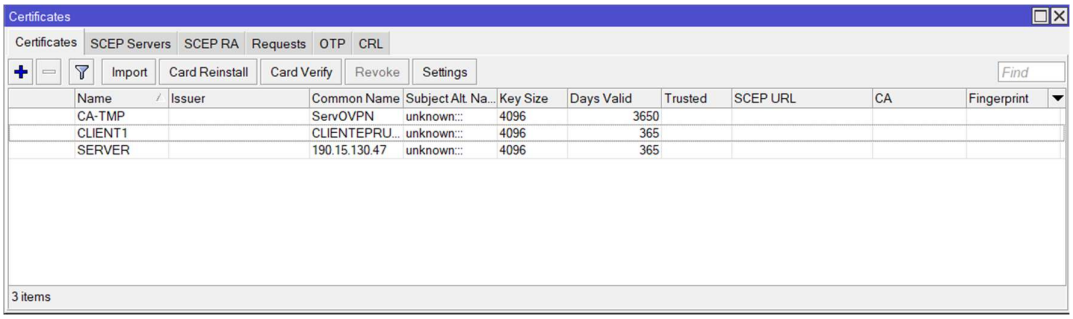


Fig. 49. Certificados VPN sin firmar.

Posteriormente procedemos a ejecutar la siguiente línea en la terminal del Router, esto firmara al certificado CA-TMP y le cambiara el nombre a CA.

```
/certificate sign CA-TMP name=CA
```

Ahora que contamos con la entidad certificadora respectivamente firmada, se procede a firmar el certificado del SERVER con dicha entidad a cargo.

```
/certificate sign SERVER ca=CA ca-crl-host="190.15.130.47"
/certificate set SERVER trusted=yes
```

Y finalmente firmamos el certificado del cliente.

```
/certificate sign CLIENT1 ca=CA
/certificate set CLIENT1 trusted=yes
```

Una vez terminados estos pasos, debemos tener los certificados debidamente firmados como se observa en la Figura 50.

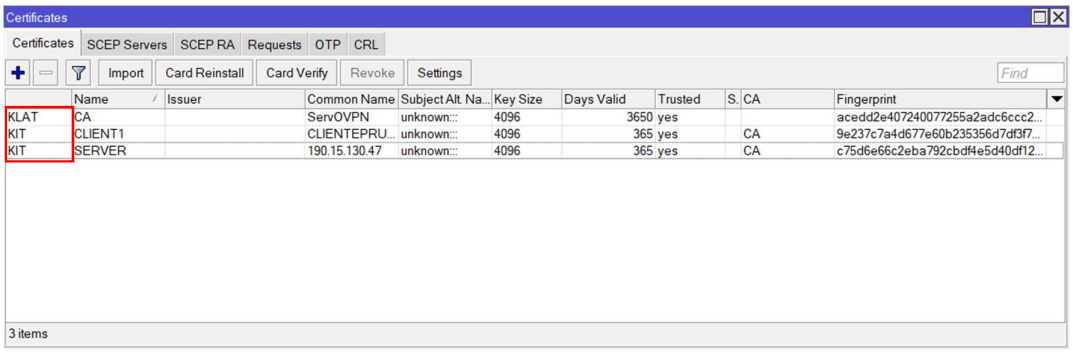


Fig. 50. Certificados VPN firmados.

Cuando los certificados estén correctamente firmados procedemos con la habilitación del servidor OpenVPN.

En la Figura 51 se muestran las configuraciones que se deben de realizar la interfaz PPP para el levantamiento del servidor OpenVPN. La mayoría de las configuraciones se dejan por defecto, exceptuando por el certificado en donde se debe seleccionar el certificado del SERVER previamente generado, verificando que está habilitada la opción de "Requerir certificado del cliente", y seleccionar el modo de autenticación sha1 y el cifrado aes 256.

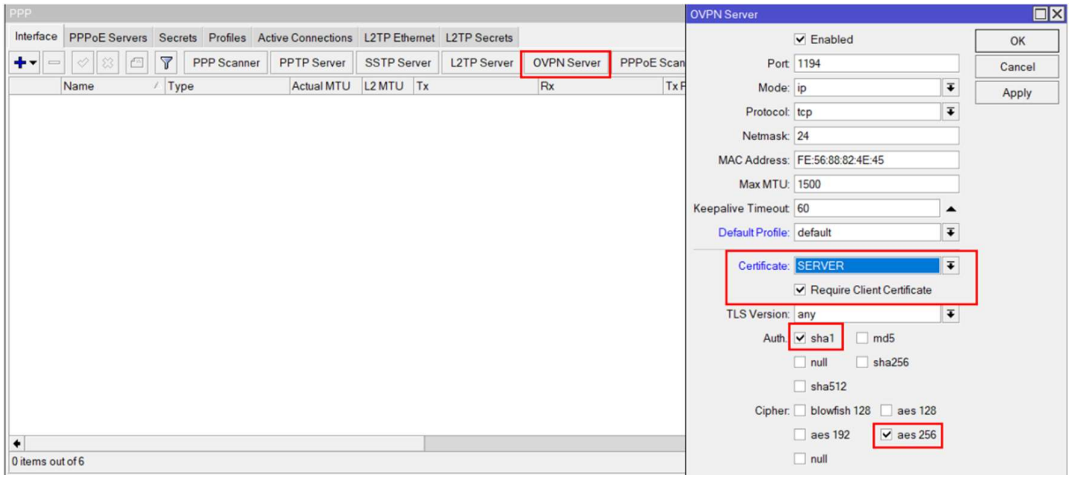


Fig. 51. Habilitación del OpenVPN Server.

Un requisito adicional para que un usuario pueda autenticarse es el uso de credenciales que deben ser creadas en la parte de *Secrets*, aquí es donde debe colocarse el nombre de usuario y la contraseña, además en la mima pestaña debe de seleccionarse el tipo de servicio del cliente, que en nuestro caso será OpenVPN, y el perfil de encriptación "*default-encryption*", por último, colocamos la IP virtual que tendrá por defecto el servidor VPN que será "*10.0.0.1*" y la IP de nuestro cliente remoto tendrá la IP "*10.0.0.11*". Estas configuraciones se detallan en la Figura 52.

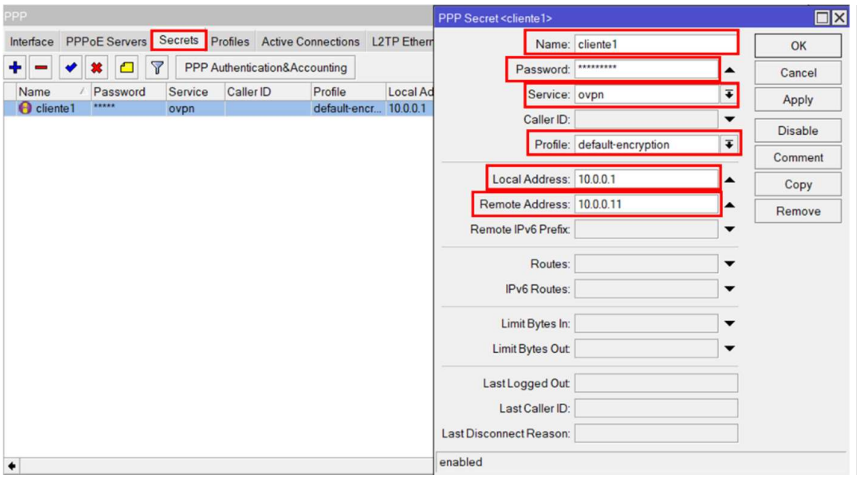


Fig. 52. Credenciales de acceso para cliente OpenVPN.

Por otra parte, se debe de realizar la exportación de los certificados, que servirán para que el cliente OpenVPN pueda realizar la conexión remota. Para realizar la exportación de los certificados, primero seleccionamos la entidad certificante "CA" y con clic derecho abrimos el menú de opciones para elegir la que dice "Export" como se muestra en la Figura 53.

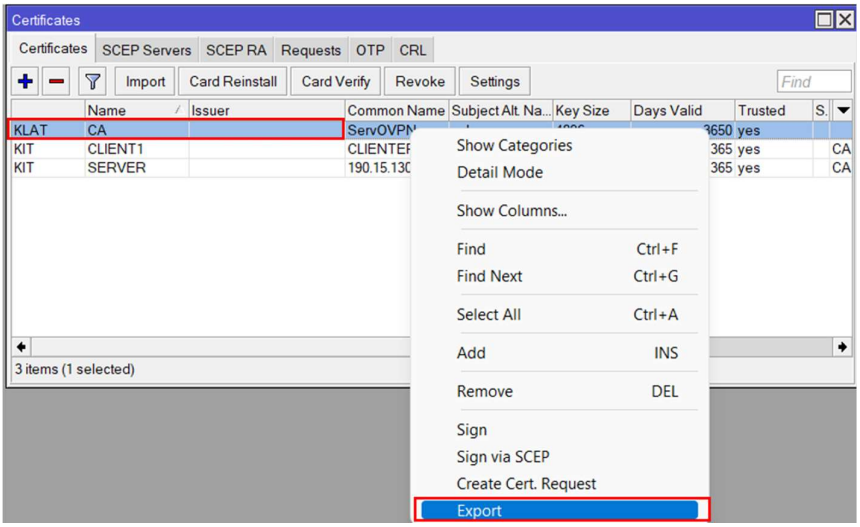


Fig. 53. Menú de opciones para certificados.

En la ventana que emerge verificamos que este seccionado el certificado que necesitamos exportar y damos clic en "Export" como indica la Figura 54.

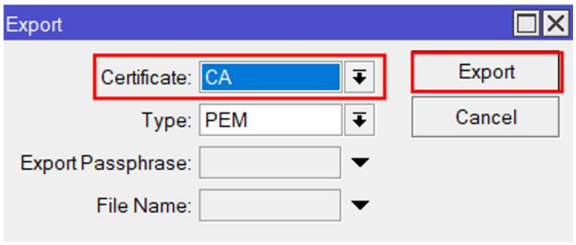


Fig. 54. Exportación de certificado CA.

Luego se realizan los mismos pasos para exportar el certificado del cliente, con la única diferencia de que se debe colocar una frase de paso con la finalidad de separar el certificado en 2 archivos, uno con extensión ".crt" y otro con extensión ".key", ambos archivos son necesarios para posteriormente conectarse con el servidor (Ver Figura 55).

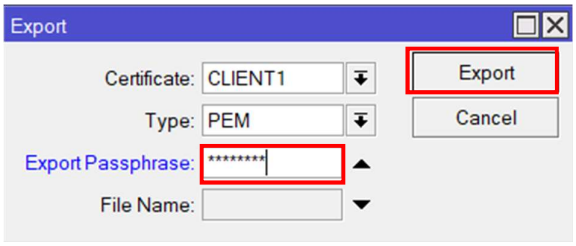


Fig. 55. Exportación de certificado CLIENT1.

Cuando se hayan exportados los certificados, estos estarán almacenados en la sección de "Files" del Router MikroTik, en la Figura 56 se puede observar los certificados respectivos a CA y a CLIENT1, además del archivo con extensión ".key" perteneciente al certificado CLIENT1 debido a la frase de paso colocada previo a su exportación.

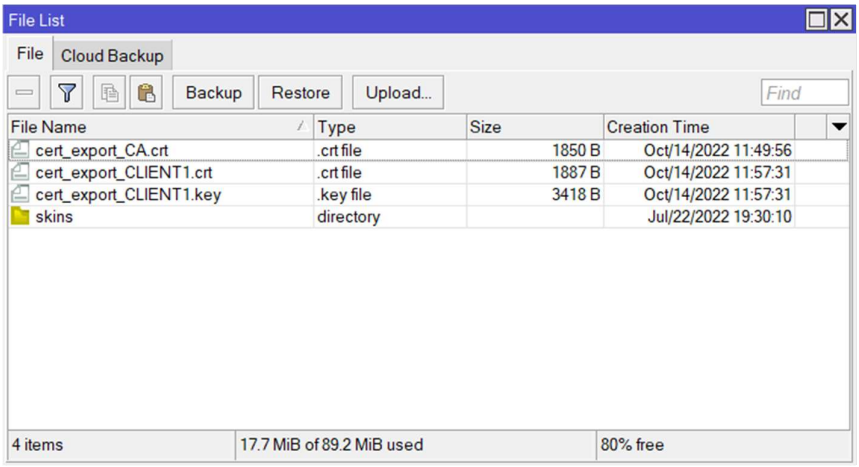


Fig. 56. Lista de archivos almacenados en el Router Mikrotik.

Hay que resaltar que la generación del certificado del cliente es individual para cada cliente remoto, es decir, en caso de requerir "n" cantidad de clientes remotos, se necesita generar "n" cantidad de certificados para clientes. En el caso de ejemplo previamente mostrado se trabaja solamente con un único cliente, no hay que olvidar que esa es la cantidad máxima permitida para un Router MikroTik sin licencia.

En la siguiente sección se mostrará como se usan las credenciales exportadas dentro del software cliente OpenVPN y la respectiva comprobación de conexión remota.

3.2.2.3 Control de acceso por medio del Firewall embebido en MIKROTIK

Con todos los pasos realizados hasta el momento, ya se cuenta con un servidor VPN activo y con credenciales de acceso para los clientes remotos, a continuación, se realizará un control de acceso haciendo uso del Firewall embebido que ofrece MikroTik con su sistema operativo RouterOS.

Para ofrecer un control de acceso que permita hacer uso del laboratorio de manera organizada, se pretende gestionar la hora y fecha de acceso de cada cliente remoto haciendo uso del Firewall de MikroTik, en la Figura 57 se muestra esta acción de forma gráfica.

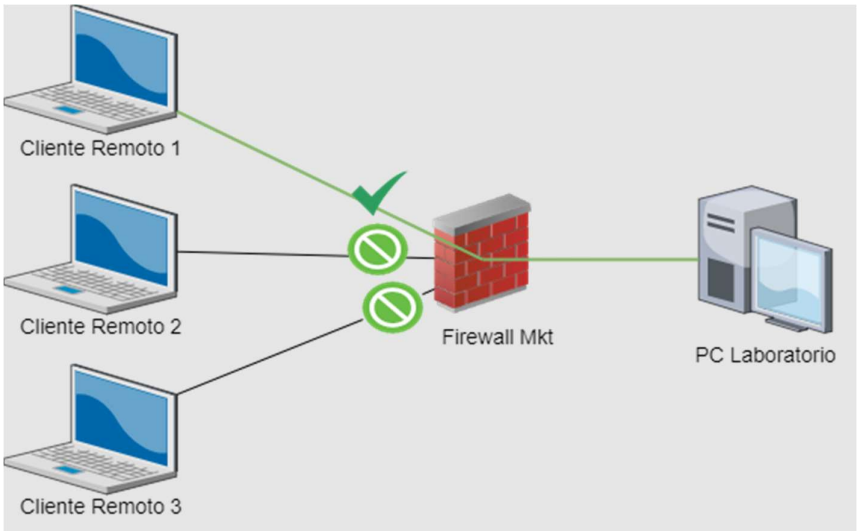


Fig. 57. Diagrama del Control de acceso mediante Firewall.

Para implementar esto con nuestro sistema, se debe de englobar a todos nuestros clientes remotos en una Lista de Acceso, esto se hará mediante la IP virtual que tendrán los

clientes, puesto que este dato lo conocemos de forma previa porque nosotros mismos somos quienes definimos el segmento de red con el que trabajarán los clientes remotos. Es necesario crear una regla de Firewall general que bloquee el acceso a todos los clientes del segmento, y posteriormente se permitirá el acceso únicamente al cliente remoto que haya agendado un turno previamente.

Primero se debe generar las listas de direcciones en el apartado de Firewall del Mikrotik, en la Figura 58 se muestran las dos listas que pertenecen a la red del laboratorio y a la red de los clientes VPN respectivamente.

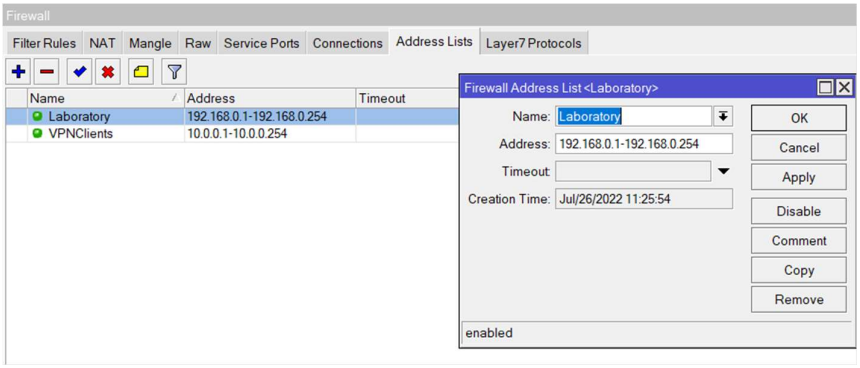


Fig. 58. Address List de las redes del sistema

Posteriormente, para crear la regla general del bloqueo de todos los clientes VPN a la red interna se crea una nueva regla de Firewall como se muestra en la Figura 59, seleccionando que todo el tráfico será rechazado (*drop*).

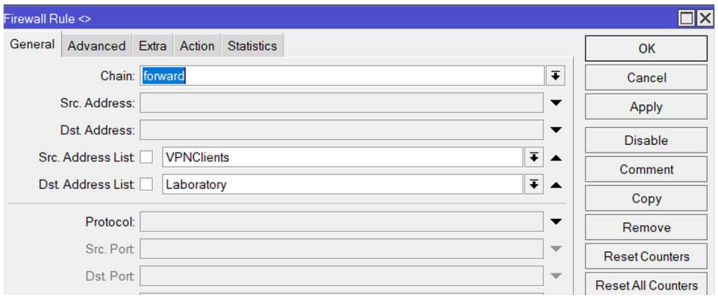


Fig. 59. Regla de Firewall de bloqueo de todos los clientes remotos.

Además, en la Figura 60 se indica las configuraciones para crear la regla que permita el acceso (*accept*) a un único cliente remoto y este a su vez tendrá acceso únicamente a un solo host dentro del laboratorio.

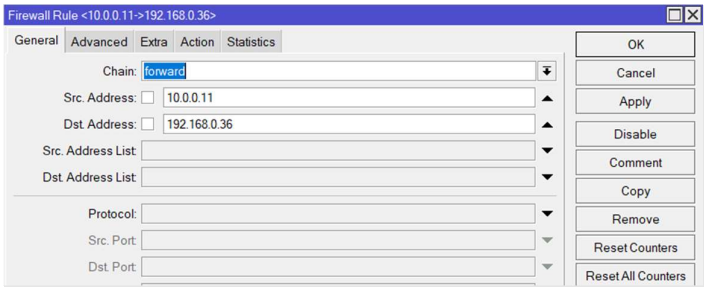


Fig. 60. Regla de Firewall de acceso de un único cliente remoto.

Un aspecto clave es que las reglas de firewall tienen un nivel de prioridad según la ubicación que tengan dentro de la lista, dicho de otro modo, si primero colocamos la regla de bloqueo general y debajo de ésta permitimos el acceso de un cliente en específico, el cliente remoto no podría acceder a los recursos internos del laboratorio, por ello, se debe de tener precaución al momento de crear las reglas de Firewall. Unas de las ventajas que ofrece la interfaz gráfica de Mikrotik es que para cambiar la posición de una regla basta solamente con arrastrarla hacia arriba o hacia abajo, e incluso se puede mover las reglas desde la terminal o conexión remota vía SSH o Telnet (*Telecomunication Network*) haciendo uso de la línea de comandos, cosa que no se puede hacer en marcas como CISCO.

En la Figura 61 se puede apreciar el orden que deben tener las reglas de Firewall para que el acceso se permita de forma correcta, esto servirá como base en el diseño de la interfaz de grafica para el agendamiento de forma automática que se detalla en secciones posteriores.

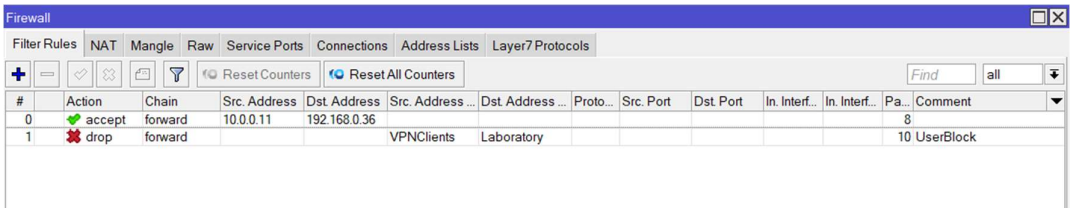


Fig. 61. Orden de las reglas de Firewall para permitir el acceso de un cliente.

3.2.3 DISEÑO DE LA INTERFAZ DE USUARIO

Para la puesta en marcha del servidor web, se realizó un análisis para seleccionar el sistema operativo donde se aloja la página web, concluyendo que usar Ubuntu Server como sistema operativo para el servidor web era una excelente opción, además de ser gratuito.

Un software distribución de GNU/Linux que ofrece un sistema operativo para servidores lo cual implica no tener instaladas utilidades innecesarias, por ejemplo, la interfaz gráfica de usuario, con el único propósito de ahorrar la mayor cantidad de recursos posibles en CPU y RAM.

Comenzaremos por dirigirnos a la página oficial de Ubuntu Server y se procede con la descarga y posterior instalación del sistema operativo, siguiendo los pasos respectivos. Una vez instalado el sistema operativo, ingresamos una línea de comando en el CLI para visualizar la versión de Ubuntu que tenemos (ver Figura 62):

```
lsb_release -a
```

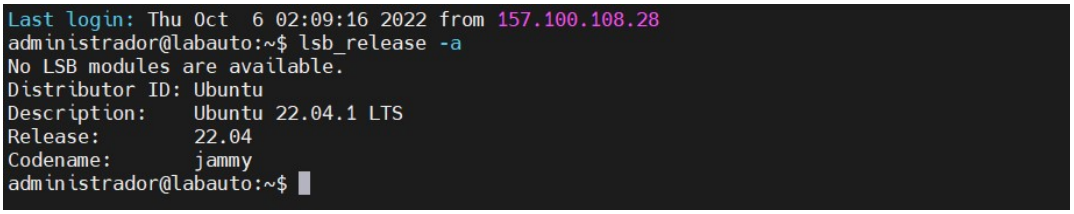


Fig. 62. Versión de Ubuntu Server.

El siguiente paso fue encontrar el servidor web que se iba a utilizar, en el mercado existen una gran variedad y popularidad entre los cuales están:

- HTTP Apache
- Nginx
- LiteSpeed
- Microsoft-IIS *(Microsoft Internet Information Services)*
- OpenResty
- Lighttpd
- NodeJS
- GWS *(Google Web Server)*

Entre los cuales podemos destacar a Apache y Nginx.

HTTP Apache destaca por:

- Múltiples funcionalidades.
- Fácil configuración y personalización.

- Continua actualización de parches de seguridad.
- Open source.

Nginx destaca por:

- Open source.
- Alto rendimiento.
- Arquitectura asíncrona basada en eventos.
- Ideal para la gestión de páginas con alto tráfico.

Al final de esta investigación se decantó por utilizar Nginx por sus características y también al formar parte de un tándem perfecto junto con Linux, MySQL y PHP, en el denominado stack LNMP [69].

3.2.3.1 Instalación del servidor WEB

A continuación, se detalla en breves pasos el proceso que se llevó a cabo para la instalación correcta del servidor web con su respectiva verificación en caso de tener errores en el proceso.

Instalación de Nginx Server

En primera instancia se instala apache2 por la línea de comando:

```
apt-get install nginx
```

En la Figura 63 se observa la versión y por ende la correcta instalación de Apache2 con:

```
nginx -v
```

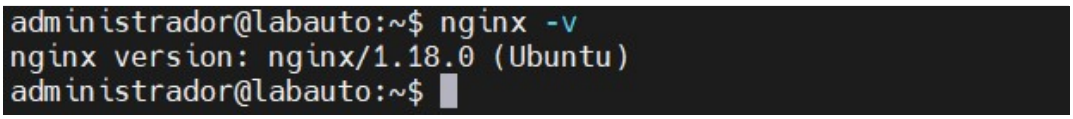


Fig. 63. Versión de Servidor Nginx.

Nginx por defecto crea un fichero en HTML en la carpeta de origen (*/var/www/html/index.html*) el cual se puede visualizar en http://localhost estando desde el propio servidor, o utilizando la IP local asignada al servidor en el proceso de instalación del sistema operativo.

Una parte fundamental en este proceso es la edición del archivo *ports.conf*, en la cual a más de definir la dirección IP también se define los puertos en los cuales Apache aceptará peticiones. En este archivo también se define el puerto para los certificados SSL, el cual permite a posterior tener más seguridad en la página web.

Instalación del gestor de Base de Datos MySQL

Este sistema MySQL trabaja como servidor en el cual se puede crear un sin número de bases de datos a las cuales el usuario por medio de solicitudes desde la página web podrá tener acceso.

Se instala por medio de la siguiente línea de comando:

```
sudo apt-get install mysql-server
```

Previo a la culminación de este servicio es posible que tenga que ingresar un usuario y contraseña para seguridad de los datos.

Instalación de servicio PHP

PHP es el lenguaje de programación de código abierto que nos ayuda a crear sitios webs dinámicos, ya que con HTML puro no se puede hacerlo como es el claro ejemplo de la consulta a una base de datos en el caso de la creación de la página web del laboratorio remoto.

Se ingresa el siguiente código como línea de comando y se procede a su instalación:

```
sudo apt-get install php5 php-pear
```

finalizado se debe también instalar el soporte de PHP5 para MySQL:

```
sudo apt-get install php5-mysql
```

Se verifica su correcta instalación y posterior versión (ver Figura 64):

```
php -v
```

```
administrador@labauto:~$ php -v
PHP 8.1.2 (cli) (built: Aug  8 2022 07:28:23) (NTS)
Copyright (c) The PHP Group
Zend Engine v4.1.2, Copyright (c) Zend Technologies
    with Zend OPcache v8.1.2, Copyright (c), by Zend Technologies
administrador@labauto:~$
```

Fig. 64. Versión de Servicio PHP.

Finalizado todas las instalaciones de los servicios de LNMP, se procede a verificar el funcionamiento del servidor antes de empezar con la programación de la página web (ver Figura 65).

```
sudo systemctl status nginx
```

```
administrador@labauto:~$ sudo systemctl status nginx
[sudo] password for administrador:
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2022-10-26 00:38:29 -05; 17h ago
       Docs: man:nginx(8)
   Main PID: 2621 (nginx)
      Tasks: 6 (limit: 9245)
     Memory: 67.0M
        CPU: 7min 5.464s
     CGroup: /system.slice/nginx.service
             ├─2621 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
             ├─2622 "nginx: worker process"
             ├─2623 "nginx: worker process"
             ├─2624 "nginx: worker process"
             ├─2625 "nginx: worker process"
             └─2626 "nginx: cache manager process"

oct 26 00:38:29 labauto systemd[1]: Starting A high performance web server and a reverse proxy server...
oct 26 00:38:29 labauto nginx[2618]: nginx: [warn] the "ssl" directive is deprecated, use the "listen ... ssl" directive instead in /etc/nginx/sites-enabled/
oct 26 00:38:29 labauto nginx[2618]: nginx: [warn] the "ssl" directive is deprecated, use the "listen ... ssl" directive instead in /etc/nginx/sites-enabled/
oct 26 00:38:29 labauto nginx[2619]: nginx: [warn] the "ssl" directive is deprecated, use the "listen ... ssl" directive instead in /etc/nginx/sites-enabled/
oct 26 00:38:29 labauto nginx[2619]: nginx: [warn] the "ssl" directive is deprecated, use the "listen ... ssl" directive instead in /etc/nginx/sites-enabled/
oct 26 00:38:29 labauto systemd[1]: Started A high performance web server and a reverse proxy server.
lines 1-22/22 (END)
```

Fig. 65. Servicio Nginx.

3.2.3.2 Diseño del sistema de agendamiento

El agendamiento como parte esencial del desarrollo de la propuesta tuvo varios puntos en los que trabajar, reglas definidas a lo largo de la investigación, así como corrección de errores a medida que se iba desarrollando, se detalla entonces el proceso a continuación.

Diseño de la Base de Datos

Previo a la creación de la página web se tuvo que realizar la respectiva base de datos, que solventará algunos requerimientos de seguridad al momento del registro del estudiante y su correcto agendamiento a los laboratorios designados.

Entre esos puntos podemos destacar:

- Que exista una tabla exclusiva para datos personales y otra tabla la cual se encargará del acceso a la página web.

- Tablas que definan el rol que tendrá cada uno de los usuarios que en este caso serán:
    - Administradores
    - Docentes
    - Estudiantes
- Una tabla exclusiva del agendamiento en donde constará con:
    - Fecha de agendamiento
    - Un ID único de usuario
    - Un ID único por laboratorio
- Una tabla que defina el horario inicial y final por cada agendamiento.
- Una tabla para que cada estudiante o docente este organizado por curso y/o grupo, entendiendo por grupo la carrera y grupo al semestre actual que estén cursando.

El resultado final luego del análisis y puesta en marcha la base de datos resultó con las tablas y conexiones que se indican en la Figura 66.

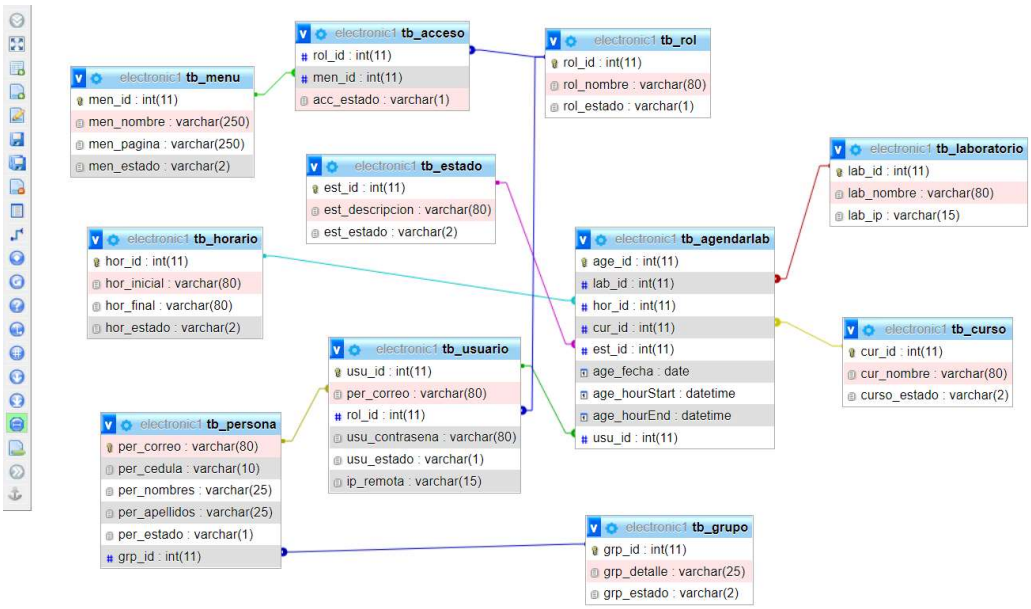


Fig. 66. Base de Datos actual del Laboratorio Remoto.

Diseño de la interfaz de usuario

Para esta sección se hizo uso de elementos Bootstrap que facilitaron el diseño, tanto en la página de inicio (login) y posterior Dashboard (Interfaz gráfica para la visualización de

datos), en la Figura 67 se muestra el diseño previo de un Dashboard administrativo en el cual se realizó las pruebas respectivas en conexión con la base de datos existente.

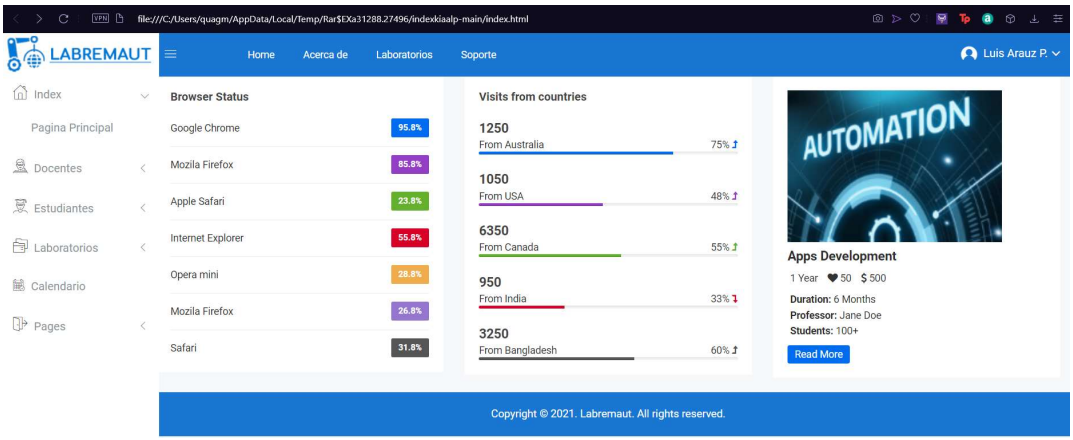


Fig. 67. Dashboard previo del Laboratorio Remoto.

Una vez finalizado toda la etapa de programación web haciendo uso de lenguajes de programación como HTML, PHP, java, CSS, y tras pruebas tanto en la página de inicio como en el Dashboard principal se presenta el resultado final de la aplicación web en las Figuras 68 y 69.

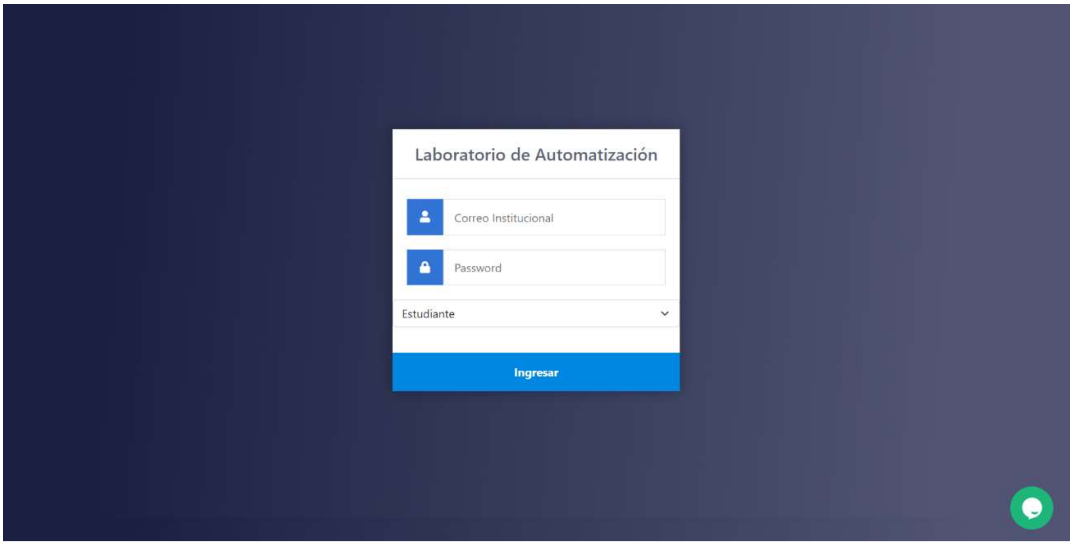


Fig. 68. Página de inicio de sesión (Login)

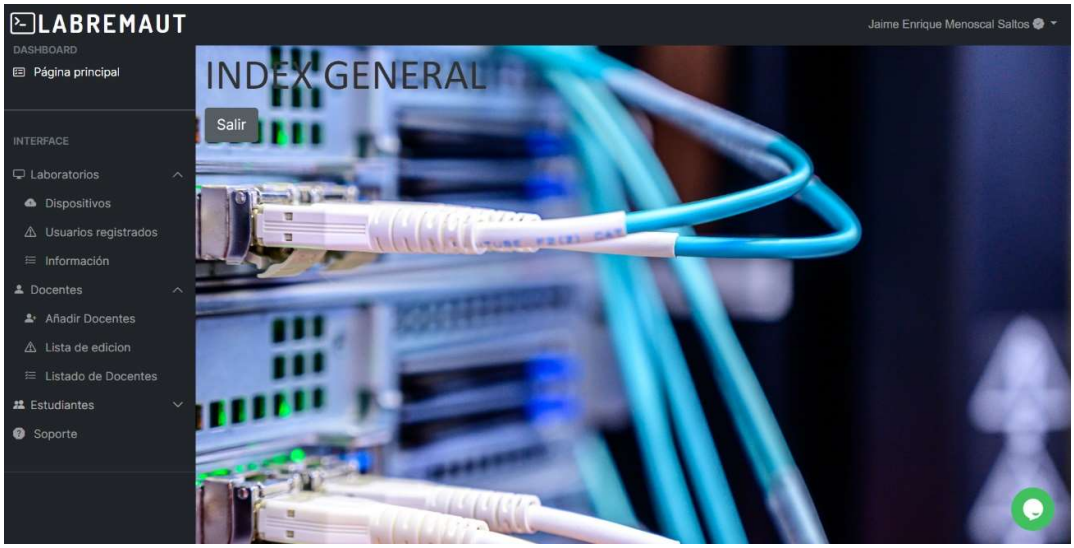


Fig. 69. Dashboard principal del Aplicativo Web.

Dashboard de visualización de Dispositivos disponibles

En el apartado de Dispositivos dentro de Laboratorios, tenemos la interfaz que ayuda tanto al administrador como al docente a la hora de visualizar que equipos en este caso PLCs y PCs de cada una de las estaciones de trabajo están encendidas y por ende siendo usadas dentro del laboratorio, teniendo la posibilidad de encender cada uno de los ordenadores por medio de un botón haciendo uso del protocolo Wake on LAN.

También se visualiza las direcciones IP estáticas que fueron asignadas a cada uno de estos dispositivos (ver Figura 70).

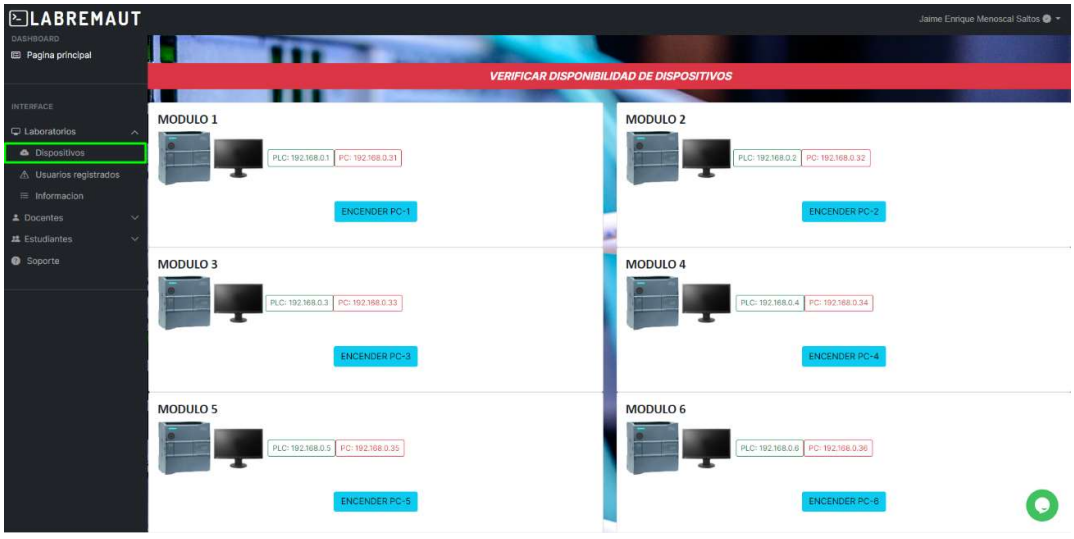


Fig. 70. Dashboard de encendido de ordenadores del Laboratorio.

A continuación, se explicará las líneas de código que nos permiten visualizar si los ordenadores están encendidos o apagados.

En primera instancia al ingresar a la pestaña “Dispositivos” se carga un script que previo a la conexión de la página web con el router Mikrotik, éste recibe comandos como el siguiente:

```
#PC1
$API->write('/ping',false);
$API->write('=address=ip fija PC1',false);
$API->write('=count=1',false);
$API->write('=interval=1');
$_SESSION['variable1'] = $API->read();
```

Las cuatro primeras líneas son comandos ya preestablecidos en la documentación de la API en la cual nos dice que se va a hacer un ping a determinada dirección IP en este caso es la IP fija previamente asignada a la PC1, luego envía un paquete ICMP con un intervalo de 1 segundo y este resultado se guardara en una variable de sesión llamada en este caso variable1.

Luego se extrae el vector principal del array en variables locales `$mystr11.`

```
$mystr11=$_SESSION['variable1'][0];
```

Con la siguiente línea se extrae el valor de interés dentro del vector, en este caso, necesitamos saber si hubo perdida de paquetes.

```
$packloss11=$mystr11['packet-loss'];
```

Seguido de esto preguntamos por sentencia “if” si hubo o no perdida de paquetes, si las hubo entonces se presentará en pantalla imágenes de los dispositivos apagados o encendidos si no hubo perdidas.

```
<?php
     if ( $packloss11  == '0'){
        echo '<img src="'.$plce.'">';
     }else{
        echo '<img src="'.$plca.'">';
     }
?>
```

Dashboard de encendido de computadores

El administrador o docente tendrá la facilidad de poder encender los ordenadores dentro del laboratorio haciendo uso del protocolo de redes ethernet Wake on LAN, a continuación, se detalla el script usado para este propósito.

Dentro del archivo *wolpcs.php* se tiene parte del siguiente código:

```
if($_SERVER["REQUEST_METHOD"]=="POST"){
            if($_POST['valor']=='PC1'){
                if ($API-
>connect('IP.router', 'usuario', 'password')) {
                    $API->write('/system/script/run',false);
                    $API->write("=.id=*6");
                    $READ = $API->read(false);
                    $API->disconnect();
                }
```

Declarada las librerías de la API y establecida la conexión con el Router, tenemos que por medio del método post enviamos una variable `valor` para activar esta parte del código, dicho valor variará dependiendo de la PC que se quiera encender, en la cuarta línea se ingresa un script:

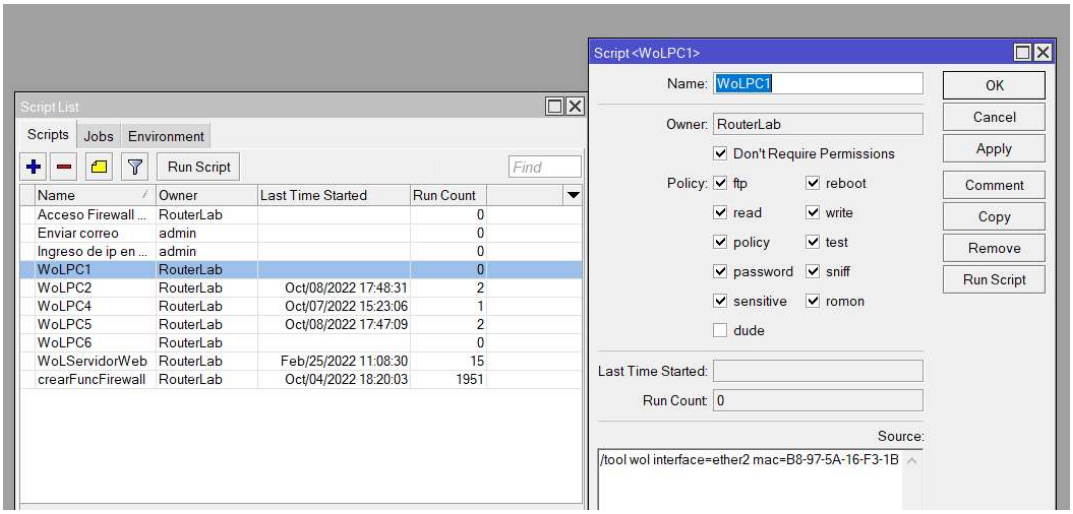


Fig. 71. Scripts para WOL.

En la Figura 71 se detalla la lista de scripts dentro del router (izquierda) y el script en donde se especifica la dirección MAC de la PC que se quiere encender (derecha).

Una vez este código es ejecutado el ordenador se encenderá siempre y cuando esté conectado la red interna del laboratorio y obviamente que cuente con alimentación

energética. Al pasar de unos cuantos segundos se podrá visualizar el encendido del ordenador en la página web.

Dashboard de registro de docentes y estudiantes

Esta sección es enteramente programación en HTML, PHP y MySQL por lo que no se extenderá en la explicación, pero si en las reglas que componen cada uno de estos Dashboard (ver Figuras 72 y 73):

- Los nombres de Docentes y Estudiantes son obligatorios.
- El correo institucional para Docentes y Estudiantes es obligatorio
- La cedula de identidad para los dos casos es obligatorio
- Por defecto la contraseña del estudiante será su cedula de identidad.
- Un Docente no podrá registrar a otro docente.
- Un estudiante no tendrá acceso a estos registros
- El administrador es el único que podrá registrar tanto docentes como estudiantes.
- El Docente podrá registrar estudiantes de ser el caso.

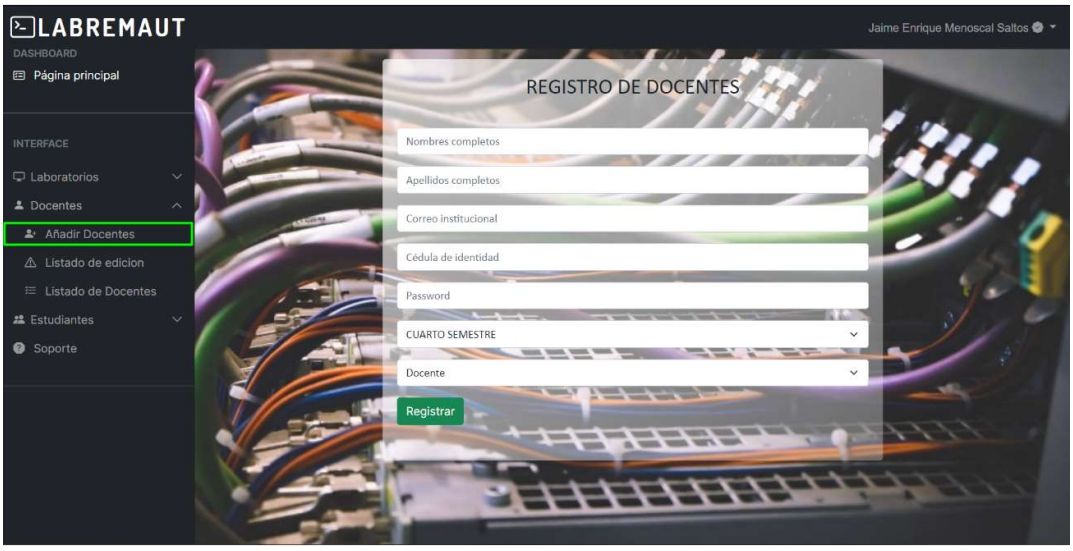


Fig. 72. Dashboard registro de Docentes.

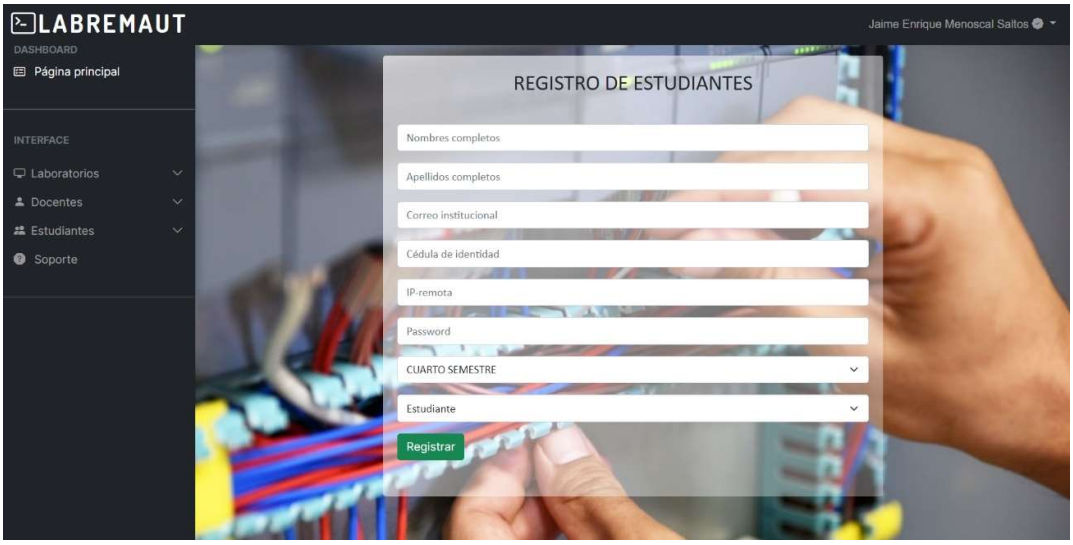


Fig. 73. Dashboard registro de Estudiantes.

Dashboard edición de datos de docentes y estudiantes

En esta sección tenemos la posibilidad de la actualización de datos tanto de Docentes como de estudiantes (ver Figura 74 y 75).

- El Docente podrá actualizar los datos de estudiantes.
- El Docente no podrá editar datos de otro docente o administrador.
- El Estudiante no tendrá acceso a este Dashboard.
- El Administrador es el único que podrá actualizar datos tanto de Docentes como de Estudiantes.

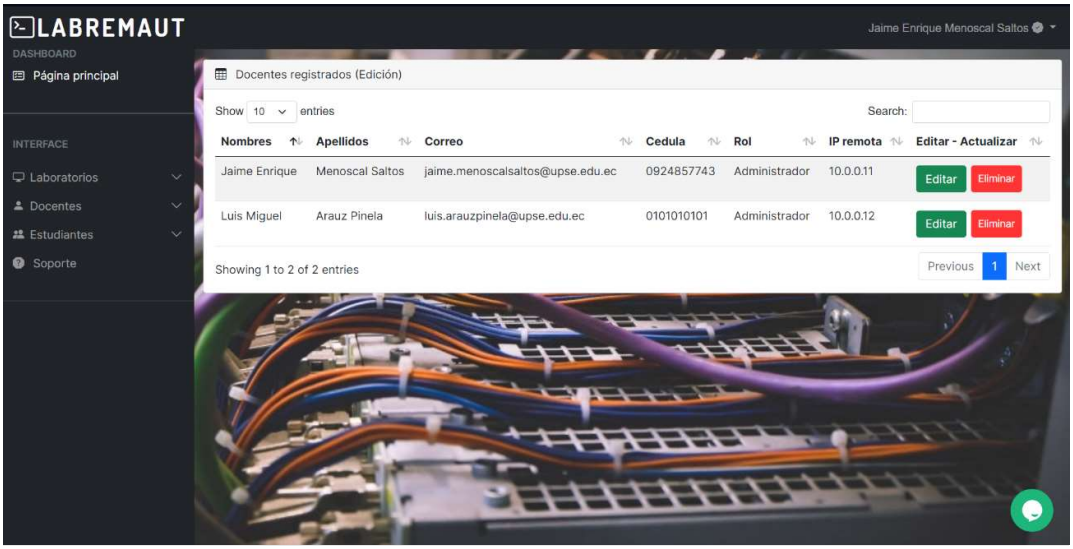


Fig. 74. Dashboard edición de datos de Administradores y Docentes.

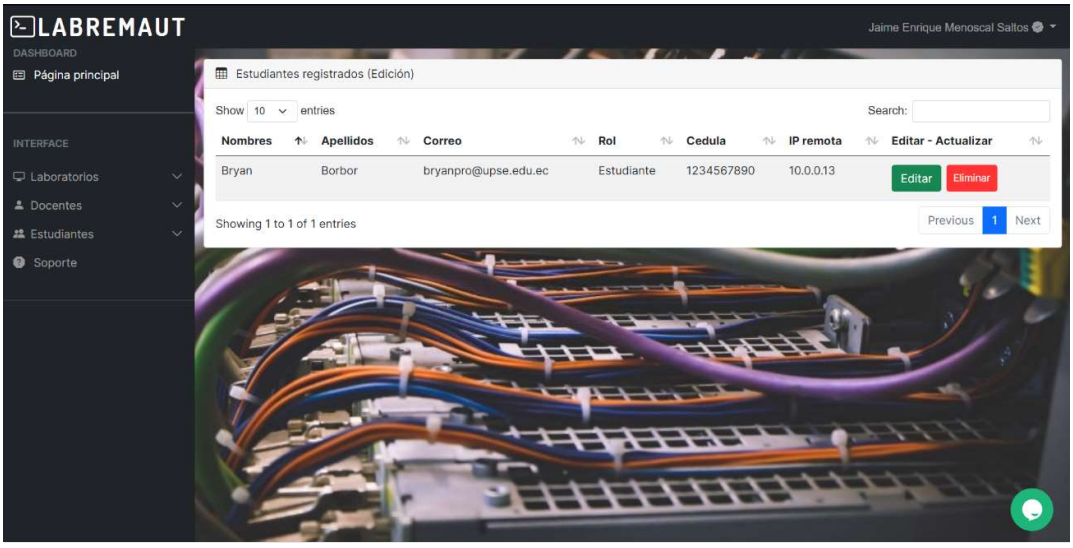


Fig. 75. Dashboard edición de datos de Estudiantes.

Dashboard de Agendamiento a los Laboratorios

En primera instancia tenemos una interfaz en la que podemos visualizar los módulos disponibles dentro del laboratorio como se muestra en la Figura 76.

Fig. 76. Dashboard de módulos disponibles.

Una vez ingresado al módulo correspondiente, tendremos un Dashboard en donde se elegirá la fecha y horario en la que se quiere realizar la práctica, se cuenta también con un calendario en el costado derecho en donde tendremos de manera grafica la visualización de turnos ya agendados dependiendo del día y la hora (ver Figura 77).

Se debe tomar en cuenta que el agendamiento luego de seleccionar día y hora, no se puede eliminar ni posponer, por lo que el estudiante deberá estar completamente seguro de tomar su turno.

Estas son algunas de las reglas que tenemos a la hora de tomar el turno.

- Un estudiante tendrá la opción de tomar 2 turnos por semana, uno para el Laboratorio 1 y otro para el Laboratorio 2
- En caso de que el estudiante quiera agendar un turno a día seguido el sistema generará un error.
- En caso de que el estudiante quiera tomar un turno ya agendado por otro estudiante, el sistema generará un error.
- Las credenciales y el manual para acceso a la práctica de laboratorio serán enviado a cada estudiante mediante su correo electrónico institucional.

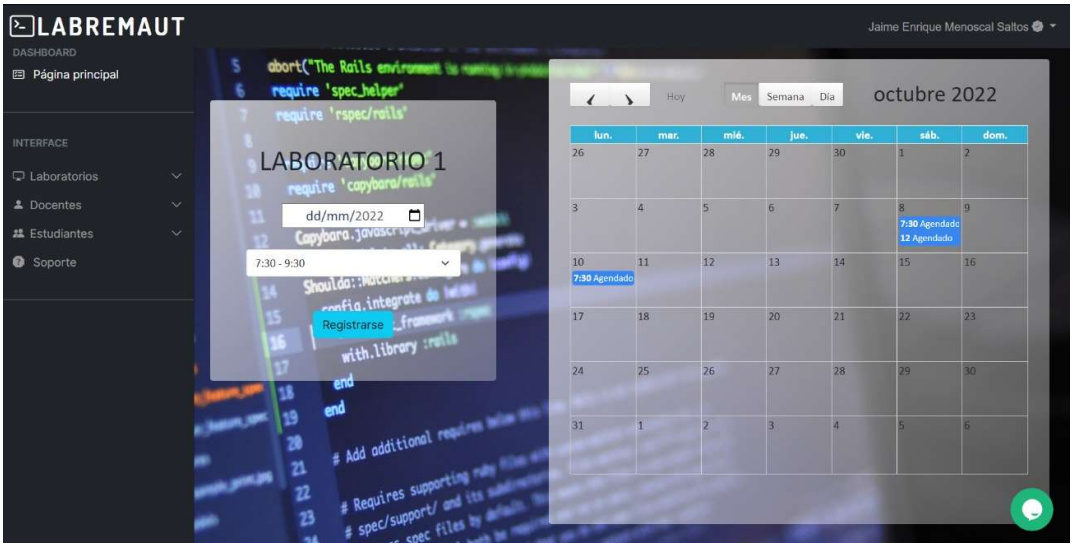


Fig. 77. Dashboard de Agendamiento de turnos.

3.2.3.3 Diagrama de flujo del proceso de agendamiento

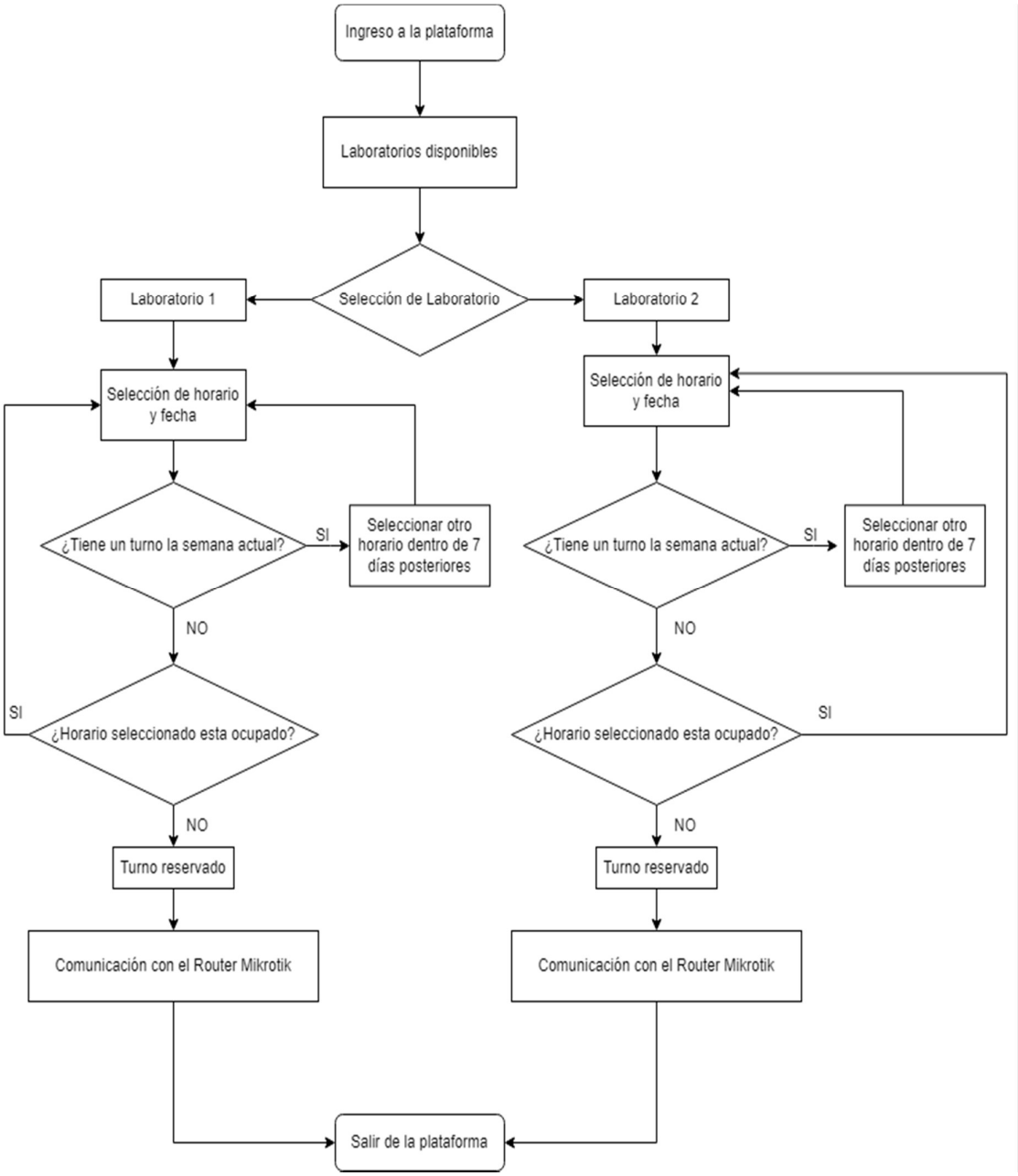


Fig. 78. Diagrama de flujo del proceso de Agendamiento.

3.2.3.4 Diagrama de roles de usuario de la Plataforma Web

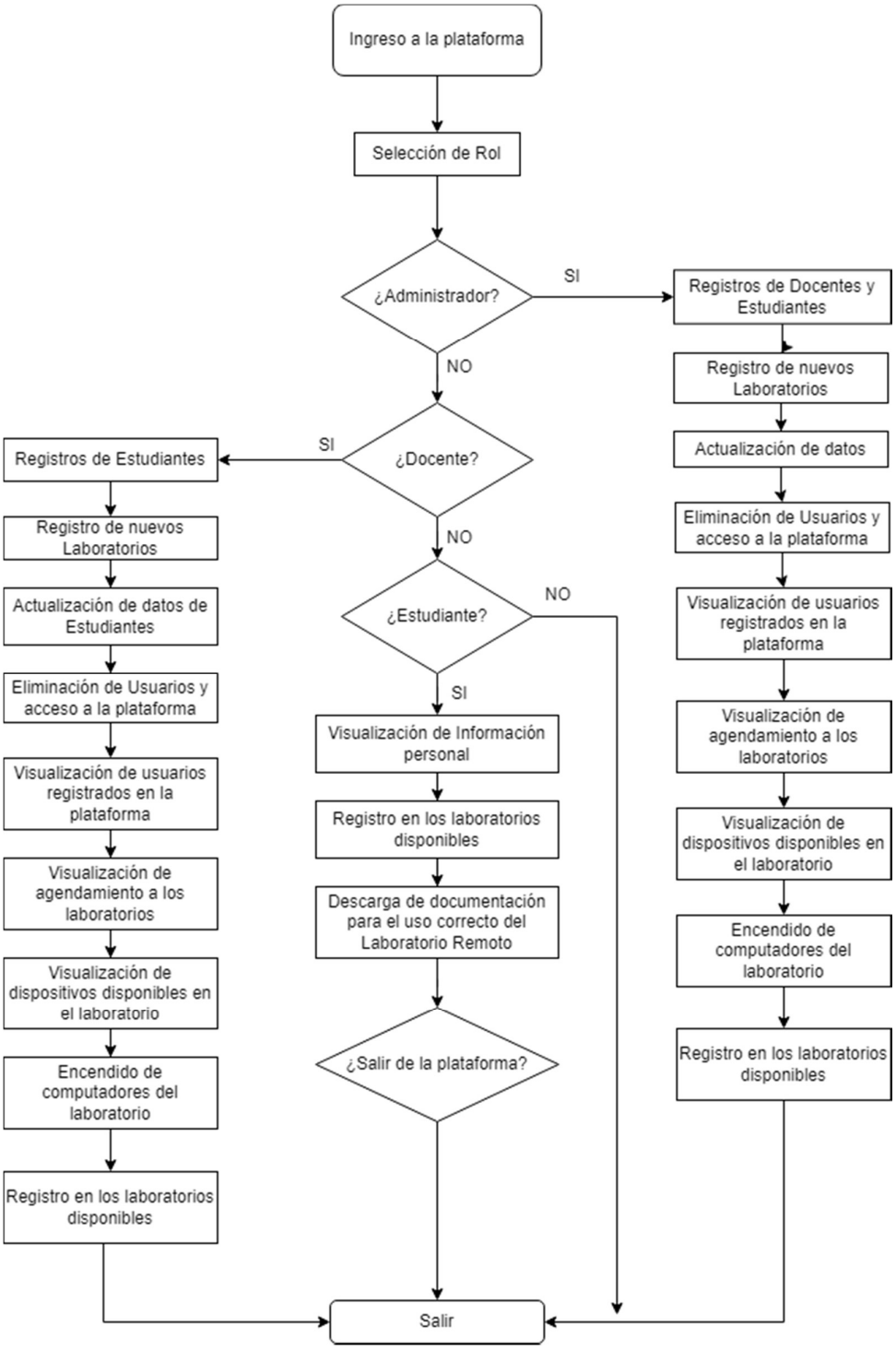


Fig. 79. Diagrama de flujo del rol de usuarios.

3.2.3.5 Monitoreo en tiempo real del funcionamiento

Para realizar el monitoreo del tablero de prácticas en tiempo real, se requiere de la instalación de un módulo adicional del servidor web Nginx que permita la retransmisión de video a través del protocolo RTMP *(Real Time Messaging Protocol)*, así mismo debe permitir que el video sea insertado en una página web bajo el protocolo HTTPS (*Hypertext Transfer Protocol Secure*).

Para comenzar, se procede con la instalación del módulo RTMP del servidor Nginx en la computadora que aloja la aplicación web previamente desarrollada, para ello se ejecuta la siguiente instrucción por la línea de comandos.

```
apt-get install libnginx-mod-rtmp
```

Sin embargo, es necesario resaltar que la transmisión no se iniciara de forma automática solo con la instalación del módulo, antes se debe de abrir el archivo de configuración Nginx y agregar el bloque de código que se muestra a continuación.

```
. . . .
rtmp {
        server {
                listen 1935;
                chunk_size 4096;
                allow publish 127.0.0.1;
                deny publish all;

                application live {
                        live on;
                        record off;
                        hls on;
                        hls_path /var/www/stream/hls;
                        hls_fragment 3;
                        hls_playlist_length 60;

                        dash on;
                        dash_path /var/www/stream/dash;
                }
        }
}
```

Con las modificaciones realizadas en el archivo se pretende configurar el puerto de escucha con el que trabajará Nginx, además de donde se publicará la retransmisión. Por otra parte, también se habilita el protocolo para retransmisión de video sobre HTTP denominado HLS y se indica el directorio donde se almacenarán los archivos temporales de la retransmisión.

Para que el archivo de configuración se cargue correctamente al servidor Nginx procedemos a reiniciar el servicio con el siguiente comando.

```
sudo systemctl reload nginx.service
```

Para realizar la captura de video de la cámara IP a utilizar, se debe de instalar el framework ffmpeg desde la consola.

```
sudo apt install ffmpeg
```

Para habilitar la retransmisión de video en el servidor y que este se encuentre disponible desde el exterior se debe de crear un nuevo sitio disponible dentro de las configuraciones del servidor Nginx, para ello creamos un nuevo archivo en el siguiente directorio.

```
sudo nano /etc/nginx/sites-available/rtmp
```

En el archivo se deben de colocar las configuraciones que se muestran a continuación.

```
. . .
server {
    listen 8088;
    location / {
        add_header Access-Control-Allow-Origin *;
        root /var/www/html/stream;
    }
}

types {
    application/dash+xml mpd;
}
```

En el archivo anterior se puede apreciar que la configuración es similar a la del aplicativo web, con la diferencia del cambio en el directorio de los archivos además del cambio de numero en el puerto de escucha.

Finalmente, para realizar la retransmisión del video de la cámara IP en el servidor basta con ejecutar una instrucción por la línea de comandos, donde se hará uso de framework instalado previamente, enviando la ubicación de la fuente de video y otras configuraciones como códecs de audio y video a utilizar y la salida por donde se encontrará disponible la retransmisión.

```
ffmpeg -i
"rtsp://user:password@ip_camera:port/cam/realmonitor?channel=1&s
ubtype=1" -vcodec libx264 -b:v 10M -acodec aac -b:a 256k -vsync
1 -async 1 -f flv rtmp://localhost/live/stream
```

Con todos estos pasos ya tendremos la retransmisión del video en tiempo real, y para insertarlo en la página web se debe de insertar un reproductor de video en HTML5 compatible con HLS, en el caso puntual de proyecto se usará Video.js [70]. El segmento de código a agregar en la página web se muestra a continuación.

```
<video-js id="my_video_1" class="vjs-default-skin" controls
preload="auto" width="700" height="500">

     <source src="https://ip_server:port/hls/stream.m3u8"
type="application/x-mpegURL">

</video-js>
```

Como resultado se obtiene la trasmisión en tiempo real del tablero de prácticas en una página web con la posibilidad de minimizar el reproductor de video y extraerlo del navegador, lo cual significa que el estudiante podrá realizar los ejercicios propuestos de forma remota mientras observa lo que pasa en el tablero en simultaneo (ver Figura 80).

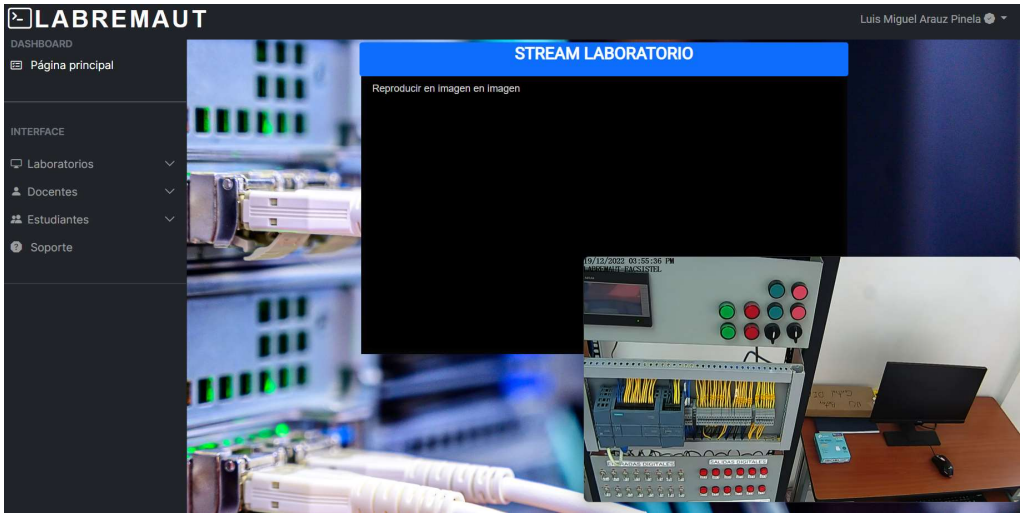


Fig. 80. Streaming del tablero de prácticas en página web.

3.2.4 INTEGRACIÓN DE LA API DE MIKROTIK CON INTERFAZ WEB

Con todas las configuraciones previas dentro del Router MikroTik y el levantamiento de la aplicación web para el agendamiento solo nos resta automatizar el sistema para permitir el acceso de los clientes remotos únicamente en el horario previamente agendado, caso contrario se debe de bloquear el acceso a la red interna del laboratorio independientemente de si está o no conectado a la red VPN.

3.2.4.1 Conexión entre el Servidor Web y el Router MikroTik mediante la API

Para realizar la conexión entre el Router MikroTik y el servidor se requiere que previamente se haya colocado el archivo PHP correspondiente a la API de RouterOS en algún directorio cercano al que se encuentran los archivos correspondientes a la aplicación web, esto es para que sea más sencillo acceder a dicho archivo cuando se requiera la comunicación con el Router.

Se debe de incluir en primer lugar el fichero de la API para que posteriormente se ejecuten las instrucciones de conexión y envío de las instrucciones requeridas para que se ejecuten por el Router. Un ejemplo de conexión se presenta a continuación.

```
if ($API->connect('172.16.12.70', 'user', 'password')) {
  $API->write('/execute',false);
  $scriptmkt='=script={$FcrearRegla ipRemota='.$iprem.'
ipLocal='.$iplocal.' id='.$correov.$labid.$date.'
schName='.$correov.$labid.$date.' fecha='.$datem.'
hora='.$time.' hora2='.$time2.'}';

  $API->write($scriptmkt);
  $READ = $API->read(false);
  $API->disconnect();
}
```

En el código anterior, en la línea 1 se evalúa si la conexión fue exitosa y si es así ejecuta las siguientes líneas de código, con en la instrucción 'connect' se envía la dirección IP de Router, usuario y contraseña, luego usamos la instrucción '$API->write' que sirve para ejecutar comandos como si se estuviera escribiendo desde la consola del Router usando WinBox por ejemplo, la respuesta recibida se almacena con la instrucción '$READ=$API->read(false)' y se finaliza la conexión con la instrucción '$API->disconnect()'. Las instrucciones enviadas en el código se utilizan para realizar el agendamiento dentro del Router, ya que lo que hace es ejecutar funciones con parámetros previamente almacenadas en el MikroTik, se hace el llamado a dichas funciones y se envía los valores para que cada función cumpla con su algoritmo y programe el acceso del cliente en la fecha y hora elegida.

En la Figura 81 se muestra el esquema para la conexión entre el servidor web y el Router Mikrotik.

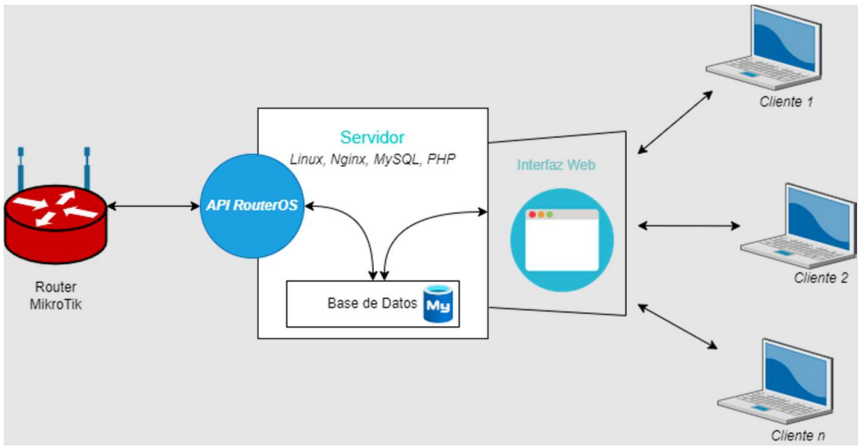


Fig. 81. Esquema de conexión con API de RouterOS.

3.2.4.2 Script para automatización del agendamiento

Para automatizar el proceso de admisión de los clientes remotos hacia la red interna, usaremos dos de las herramientas que ofrece RouterOS como son: Scripts y Scheduler.

Scripts

En secciones anteriores se describió la instrucción que envía el servidor al Router para encender un equipo dentro del laboratorio haciendo uso del estándar WOL (Wake on LAN), esta instrucción daba la orden de ejecutar un script que ya se encontraba previamente en el Router listo para su ejecución. Para ilustrar de mejor manera lo que hace el Router para encender la PC, en la Figura 82 se describe la instrucción que se haya dentro del script que realizaba esta tarea.

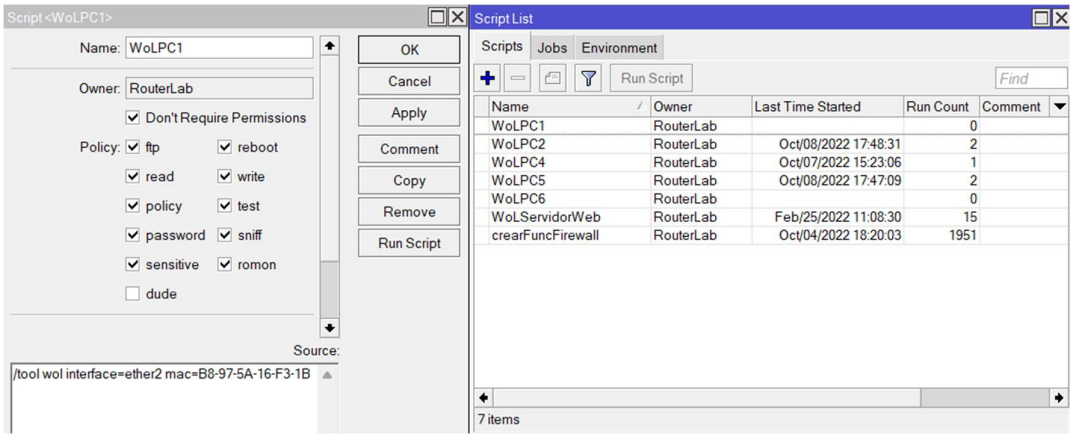
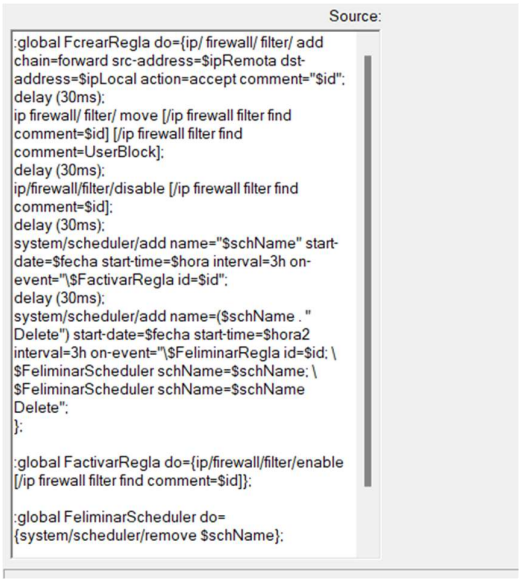


Fig. 82. Script para el encendido de una PC con WOL.

El script más importante que se implementó en el proyecto es aquel que genera todas las funciones necesarias para el agendamiento automático de turnos para el acceso mediante el Firewall propio del Router, al mismo tiempo se programó que se ejecute cada cierto lapso con la finalidad de crear las funciones en caso de que se produzca la ausencia de energía eléctrica por un tiempo mayor al que suministra el UPS de respaldo.

La generación de las funciones se puede apreciar en la Figura 83, mediante un solo script se crean todas ellas de forma global, para que puedan ser accedidas desde la API cuando se requiera ejecutar alguna acción.


Source:

```
:global FcrearRegla do={ip/ firewall/ filter/ add
chain=forward src-address=$ipRemota dst-
address=$ipLocal action=accept comment="$id";
delay (30ms);
ip firewall/ filter/ move [/ip firewall filter find
comment=$id] [/ip firewall filter find
comment=UserBlock];
delay (30ms);
ip/firewall/filter/disable [/ip firewall filter find
comment=$id];
delay (30ms);
system/scheduler/add name="$schName" start-
date=$fecha start-time=$hora interval=3h on-
event="\$FactivarRegla id=$id";
delay (30ms);
system/scheduler/add name=($schName . "
Delete") start-date=$fecha start-time=$hora2
interval=3h on-event="\$FeliminarRegla id=$id; \
$FeliminarScheduler schName=$schName; \
$FeliminarScheduler schName=$schName
Delete";
};

:global FactivarRegla do={ip/firewall/filter/enable
[/ip firewall filter find comment=$id]};

:global FeliminarScheduler do=
{system/scheduler/remove $schName};
```

Fig. 83. Script para generar las funciones requeridas para el agendamiento.

Scheduler

El Schedule sirve para programar la ejecución de scripts y funciones en una fecha y hora determinada, y esta funcionalidad es la que se aprovechará para programar el permiso y posteriormente el bloqueo del acceso a cada cliente remoto que haga un registro.

Para ejecutar el script que genera las funciones necesarias para el proyecto se creó un Schedule que ejecuta dicho script cada 10 minutos, y además de crear las funciones también ejecuta el script para el encendido del servidor mediante el estándar WOL en caso de que se encuentre apagado por cualquier causa externa, esto se observa en la Figura 84.

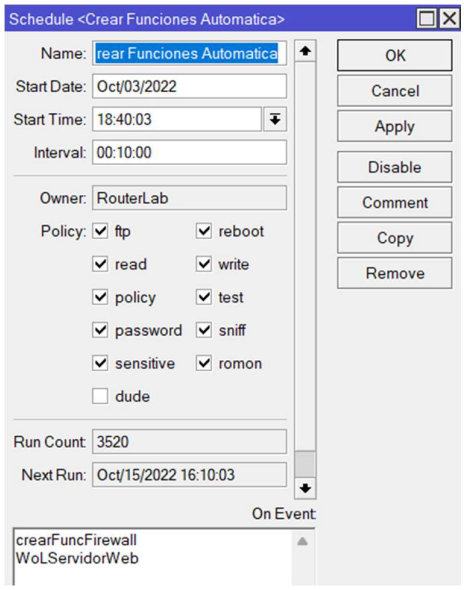


Fig. 84. Programación para ejecución de Script de forma automática.

3.2.4.3 Control de acceso mediante automatización de RouterOS y reglas de Firewall

Teniendo automatizada la parte de generar las funciones mediante la ejecución de un script, solo queda tomar la información necesaria de la base de datos y de aplicación web para agendar el acceso de la IP virtual del estudiante en la fecha y hora elegido por el cliente remoto.

Cuando un usuario registra un turno, se genera una regla de firewall para permitir el acceso, pero se deshabilita inmediatamente hasta que le corresponda habilitar según el agendamiento. Esto puede ser confuso de entender mediante la observación de las funciones en texto plano, por ello se detallará el proceso de agendamiento de turno en el Mikrotik mediante un diagrama de flujo, este se puede apreciar en la Figura 85.

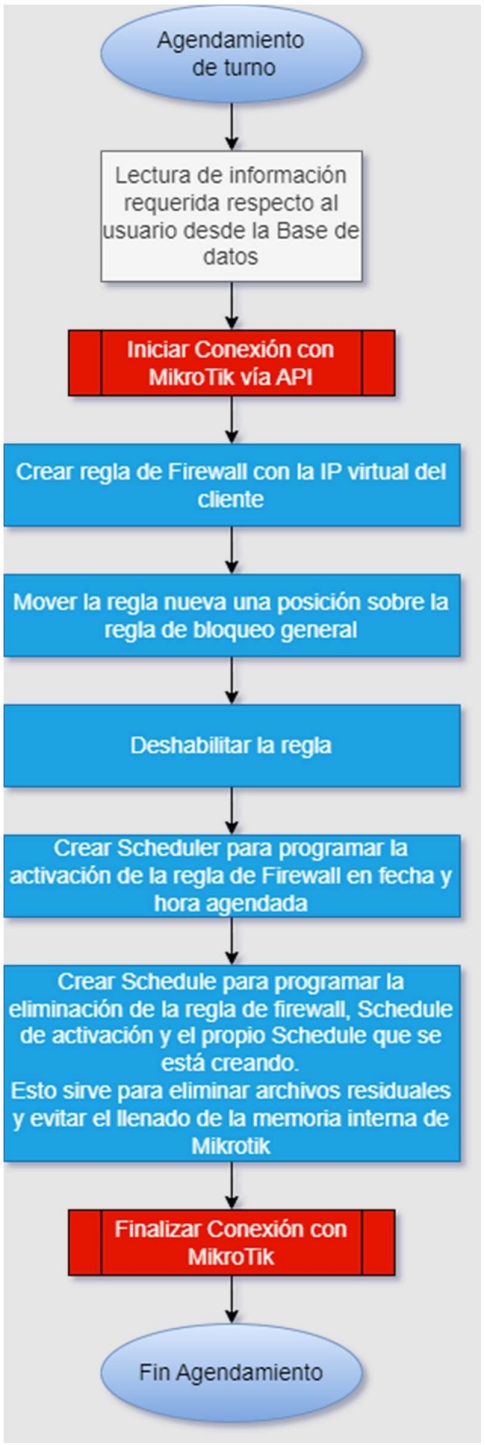


Fig. 85. Diagrama de flujo del proceso de agendamiento en router MikroTik.

3.2.5 DISEÑO DEL TABLERO PARA PRÁCTICAS

Finalizado todos los aspectos de telecomunicaciones dentro de la propuesta tecnológica, así como la parte del agendamiento dentro del servidor web y todos los procesos que este conlleva, ahora se continúa con la parte eléctrica y electrónica en donde se detallará las conexiones en los racks o módulos de trabajo que están dentro del laboratorio y de los cuales se hará uso más adelante.

3.2.5.1 Diseño de la electrónica de potencia

El reacondicionamiento del Laboratorio se efectuó en el primer semestre del año 2022, ya que se contaba con una distribución obsoleta y no apta para el desarrollo de prácticas en las diferentes asignaturas que hacían uso de este laboratorio.

Se realizo un esquema general de los elementos que contaría cada una de las estaciones de trabajo (ver Figura 86).

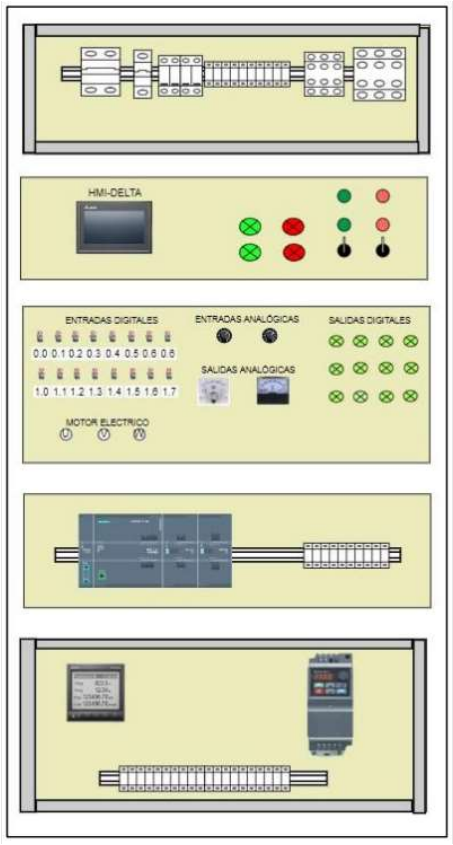


Fig. 86. Diagrama de Estación de trabajo.

Como primer punto se tiene a la protección eléctrica de todos los elementos dentro de la estación de trabajo, el que está compuesto por (ver Figura 87):

- 2 borneras de alimentación (Línea A y B)
- 1 neutro del sistema
- 2 disyuntores de 2 polos
- 1 disyuntor de 1 polo
- 4 fusibles
- 1 relé
- 1 contactor.

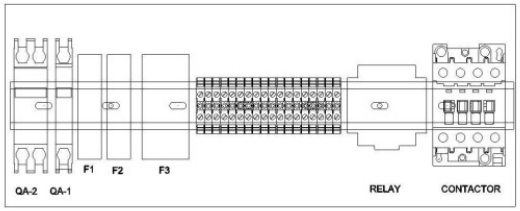


Fig. 87.Protección eléctrica de la estación de trabajo.

En la Figura 87 se observa un esquema de la distribución de los elementos, en donde se tiene un disyuntor empleado para la protección del variador y el medidor de parámetros. Fusibles que son las protecciones para los elementos conectados directamente como el PLC, pantalla HMI.

El segundo disyuntor es empleado para la protección del bloque donde se sitúa la pantalla HMI, donde se realizan prácticas de forma presencial usando un sistema ya establecido de marcha y paro, que en esta sección no se ahondará ya que en las prácticas detalladas a posterior no se hará uso de ello.

El tercer disyuntor es el encargado de la protección del bloque donde está ubicado el PLC, y por consiguiente las luces piloto, switch que representan las entradas, salidas digitales y dos potenciómetros que representan las entradas analógicas.

3.2.5.2 Diseño de la electrónica de control

En la parte de control tenemos el diseño eléctrico de conexiones de alimentación y control del PLC S7 1200, como se observa en la figura 96, se realizó una adecuación entera, con peinado de cables y también su conexión a la red del laboratorio por medio de protocolo ethernet (ver Figura 88).

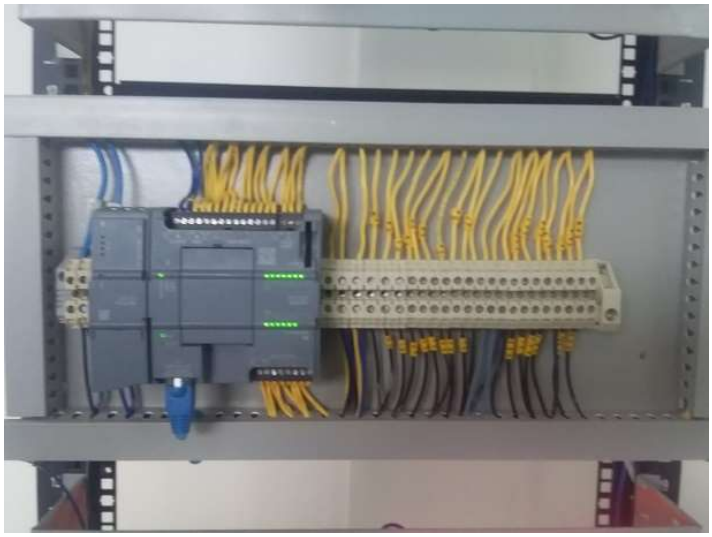


Fig. 88. Sección de control de la estación de trabajo.

En la Figura 89 se observa el diagrama eléctrico de las conexiones del PLC hacia el tablero con luces piloto, switch, y potenciómetros, que ayudan en el desarrollo de prácticas al ser más visual las entradas y salidas que tiene el autómata.

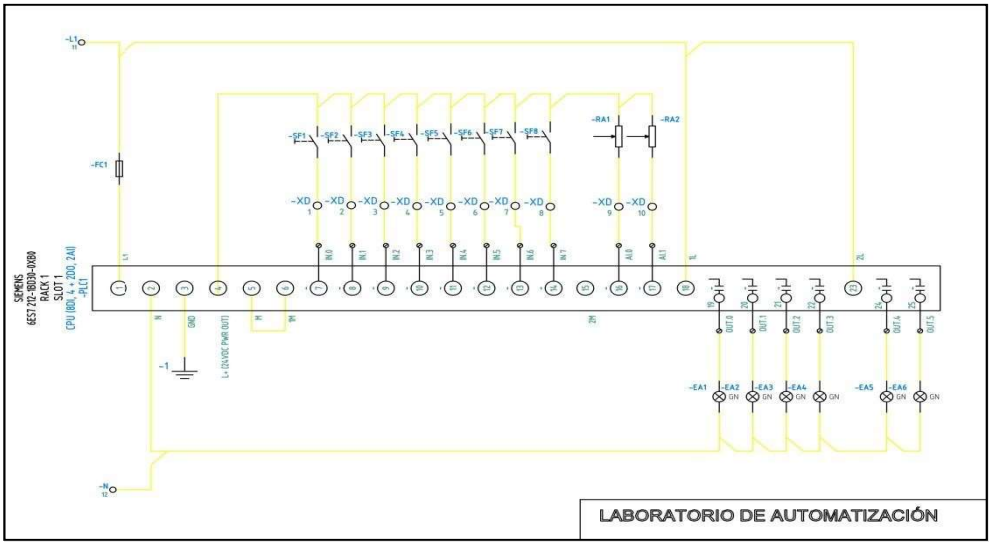


Fig. 89. Diagrama eléctrico de la estación de trabajo.

3.2.5.3 Indicadores

En el proceso de la creación de prácticas para el uso de la plataforma de Laboratorio remoto, se tomó en cuenta el uso de las luces pilotos que se encuentran en las estaciones de trabajo, las que nos ayudaran en la visualización se si una salida de relé del PLC ha sido activada (ver Figura 90).

Fig. 90. Sección de luces pilotos de la estación de trabajo.

3.2.5.4 Sensores

El sensor utilizado para una de las prácticas es el sensor de temperatura PT100 del cual se obtiene los datos a través del controlador de temperatura DTB4848 mediante la comunicación serial MODBUS RTU RS485, a continuación, en la Figura 91 se observa el tipo de conexión que se realizó para su correcto funcionamiento.

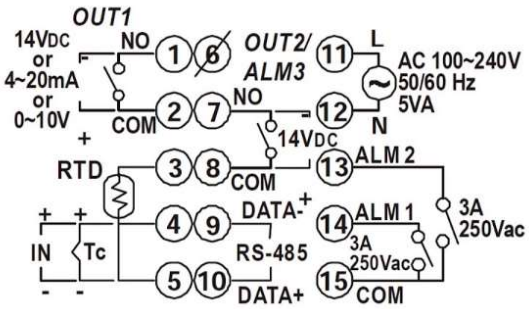


Fig. 91 Diagrama de conexión del controlador DTB4848 [71].

Para la lectura de temperatura del sensor PT100 se hace la respectiva conexión al controlador de temperatura en los pines 3, 4 y 5, que a su vez se conecta hacia el módulo SM 1241 de comunicación del PLC con los pines 9 y 10 (DATA + y DATA -), encargados del envío y recepción de datos (ver Figura 92).

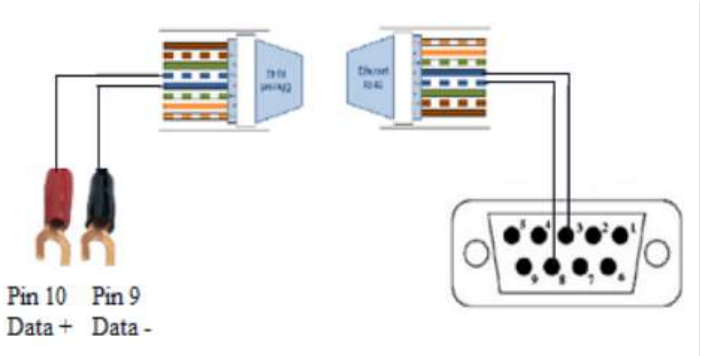


Fig. 92 Conexión de pines en el cable par trenzado.

3.2.6 DISEÑO DE PRÁCTICAS DE LABORATORIO

3.2.6.1 Práctica 1. Declaración, lectura y escritura de variables booleanas para un control de marcha y paro de un motor monofásico.

<table>
<tr><td colspan="2">UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
UPSE</td><td colspan="2">GUÍA DE PRÁCTICAS LABREMAUT</td></tr>
<tr><td colspan="2">Carrera: Electrónica y Telecomunicaciones</td><td colspan="2">Asignatura: Sensores e instrumentación</td></tr>
<tr><td>Práctica Nro.</td><td>1</td><td colspan="2">Título de Práctica: Declaración, lectura y escritura de variables booleanas para un control de marcha y paro de un motor monofásico.</td></tr>
<tr><td colspan="4">Objetivos:
• Activar y desactivar salidas digitales mediante la lectura del estado de variables.
• Realizar la programación mediante el lenguaje LADDER en el software TIA Portal
• Conexión del PLC Siemens 1200 con el software de simulación Factory ÍO.</td></tr>
<tr><td colspan="4">Descripción de la Práctica:
Se procederá con la implementación de un tablero de control en Factory IO, con el cual se manipulará una botonera, y dependiendo del estado de los botones activar las salidas digitales del PLC, lo cual será visible a través de las luces piloto en tablero de prácticas dentro del laboratorio las cuales simularan el arranque directo de un motor monofásico.</td></tr>
<tr><td colspan="2" rowspan="3">Instrucciones:</td><td colspan="2">1. Verificar que el PC remoto en el que va a trabajar se encuentre encendido, caso contrario informar al docente o administrador.</td></tr>
<tr><td colspan="2">2. Revisar el anexo 2 sobre las configuraciones en Tia Portal para la conexión con Factory IO.</td></tr>
<tr><td colspan="2">3. Desarrollar la Práctica teniendo como guía el detalle de la Práctica 1 en el presente documento</td></tr>
<tr><td colspan="4">Actividades por desarrollar:
1. Desarrollar la programación para el control de marcha y paro de 3 elementos en Tia Portal con sus respectivas variables de entrada y salida.
2. Realizar la conexión del PLC con Factory IO para las pruebas respectivas.</td></tr>
<tr><td colspan="4">Resultados:
Control de marcha y paro de tres elementos.
Visualización del funcionamiento el tiempo real en Factory IO y en tablero de control.</td></tr>
<tr><td colspan="4">Conclusiones:
Se realizo el control de marcha y paro a través de variables mediante con conexión con Factory IO.
Se realizo la programación en lenguaje Ladder con enclavamiento de la variable de salida.</td></tr>
<tr><td colspan="4">Recomendaciones:
Revisión de los anexos respectivos para conexión remota mediante OpenVPN y detalle de Práctica 1.
Verificación de que los equipos a utilizar dentro del laboratorio estén encendidos.</td></tr>
</table>

Tabla de variables de entrada

En esta primera practica se procede con el arranque directo de tres motores monofásicos, por lo cual se requiere realizar un enclavamiento de tres variables de salida, y para el control de cada salida, se requiere de un par de entradas digitas, una para el "arranque" y otra para el "paro". En total se requieren de seis variables de entradas, dos por cada motor, y estas pueden observarse en la Figura 93.

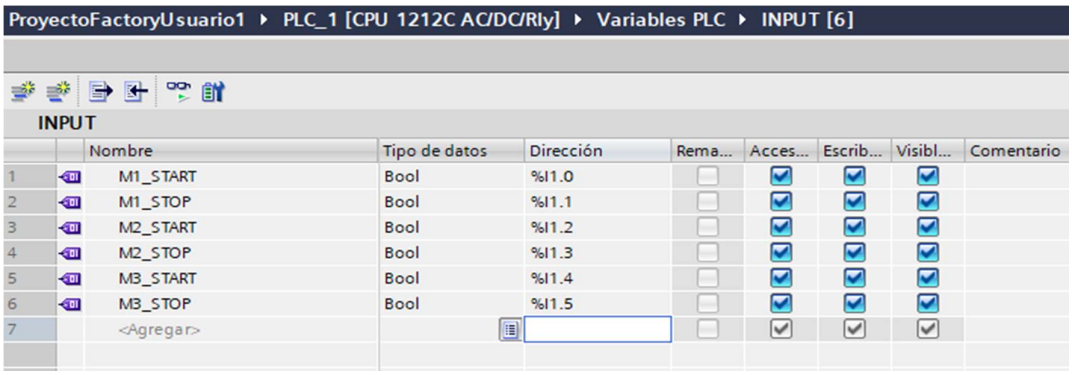


Fig. 93. Tabla de variables de entrada de la Práctica 1.

Tabla de variables de salida

Para controlar el encendido de cada motor se necesita de una salida digital, por lo que en total se requieren 3 salidas, y estas se pueden apreciar en la Figura 94.

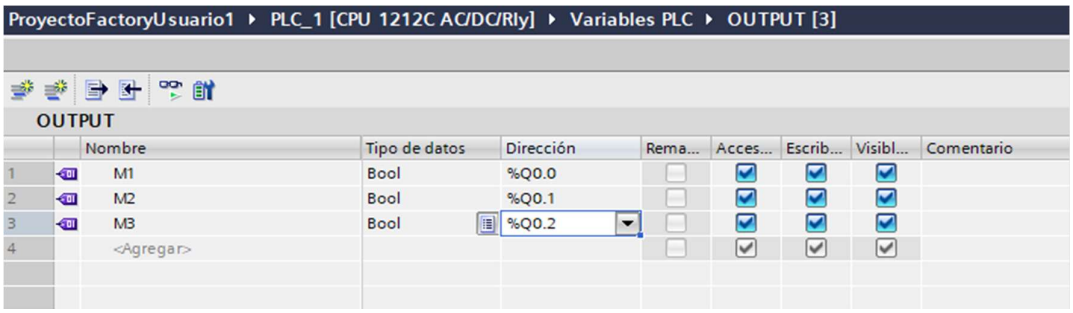


Fig. 94. Tabla de variables de salida de la Práctica 1.

Programación en lenguaje LADDER para enclavamiento de motor.

A continuación, se muestra la codificación en lenguaje LADDER que sirven par lograr enclavar una salida digital luego de presionar el botón M1_START (en caso del motor M1), y esta salida se mantendrá activa hasta que se presione el botón M1_STOP, la misma programación se repite para los motores M2 y M3 (ver Figura 95).

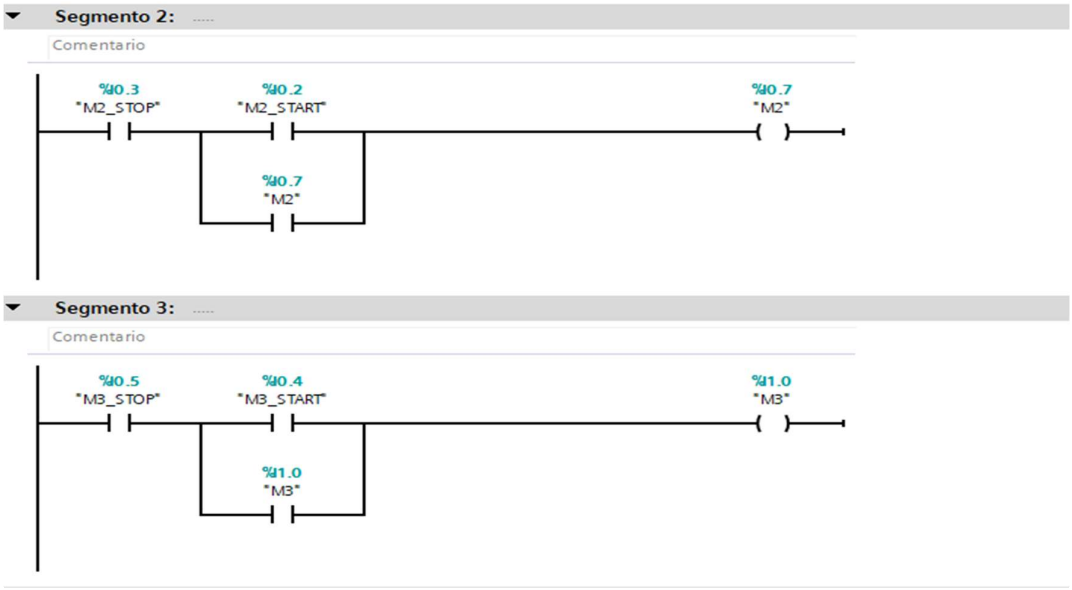


Fig. 95. Programación en lenguaje Ladder de la Práctica 1.

Tablero de control de marcha y paro de motores realizado en Factory IO

En Factory IO se realizó un tablero eléctrico en 3D, con los botones necesarios para poder cumplir con el objetivo de la práctica, además se cuenta con leds indicadores conectados a las salidas digitales del PLC con la finalidad de visualizar el momento en que el motor este encendido, activando el indicador de color verde (ver Figura 96).

Fig. 96. Tablero de control en Factory IO de la Práctica 1.

3.2.6.2 Práctica 2. Salidas físicas digitales para control de un semáforo

<table>
<tr><td colspan="2">  </td><td colspan="2">GUÍA DE PRÁCTICAS LABREMAUT</td></tr>
<tr><td colspan="3">Carrera: Electrónica y Telecomunicaciones</td><td>Asignatura: Sensores e instrumentación</td></tr>
<tr><td>Práctica Nro.</td><td>2</td><td colspan="2">Título de Práctica: Salidas físicas digitales para control de un semáforo</td></tr>
<tr><td colspan="4">Objetivos:
Realizar la programación Ladder mediante TIA Portal v16 para el control del semáforo.
Utilizar el módulo de salidas digitales SM 1222 del PLC S7-1200.
Cargar el programa al PLC S7-1200 para realizar las pruebas necesarias.
Comprender la lógica de un temporizador dentro de la programación Ladder.</td></tr>
<tr><td colspan="4">Descripción de la práctica:
Esta práctica tiene como objetivo la comprensión de los temporizadores en un proceso básico del control automático de luces de tráfico.</td></tr>
<tr><td colspan="2" rowspan="2">Instrucciones:</td><td colspan="2">1. Verificar que el PC remoto en el que va a trabajar se encuentre encendido, caso contrario informar al docente o administrador.</td></tr>
<tr><td colspan="2">2. Desarrollar la práctica teniendo como guía el detalle de la Práctica 2 en el presente documento</td></tr>
<tr><td colspan="4">Actividades por desarrollar:
Realizar la programación en Ladder para el control de luces de tráfico.
Utilizar los temporizadores necesarios para su correcto funcionamiento.
Establecer la conexión con el PLC y observar por medio de la cámara su accionar.</td></tr>
<tr><td colspan="4">Resultados:
Control de luces de tráfico, mediante el uso de temporizadores.
Declaración de diferentes tipos de variables para la correcta programación en Ladder.</td></tr>
<tr><td colspan="4">Conclusiones:
La práctica tiene la finalidad de familiarizar al estudiante con el uso de diferentes tipos de variables dentro de la programación Ladder.
El conocimiento de la lógica tras el uso del bloque temporizador resulta de principal objetivo para el fin de la práctica.</td></tr>
<tr><td colspan="4">Recomendaciones:
Revisión de los anexos respectivos para conexión remota mediante OpenVPN y detalle de práctica 2.
Verificar que los dispositivos a usar en la práctica se encuentren encendidos y disponibles.
La práctica puede tener diferentes maneras de resolución.</td></tr>
</table>

Tabla de variables

En la Figura 97 se muestra las diferentes variables que se utilizó para el desarrollo de la programación en LADDER, la variable de entrada booleana INICIO (contacto normalmente cerrado) se utiliza para dar comienzo al ciclo de programación, MARCHA es una variable de tipo memoria que ayuda a hacer el enclavamiento y por ende su constante ejecución en cada uno de los segmentos del programa.

Otra variable de memoria es REINICIO (contacto normalmente cerrado), es la que permite que el sistema vuelva a empezar, las variables booleanas L_ROJO, L_AMARILLO, L_VERDE, en este caso representadas como salidas, son los leds que representan el semáforo.

Variables de memoria TIEMPO_0, TIEMPO_1, TIEMPO_2 son salidas asignadas a los bloques de temporizador que se han utilizado en esta programación (ver Figura 98).

	Nombre	Tipo de datos	Dirección	Rema...	Acces...	Escrib...	Visibl...
1	INICIO	Bool	%I0.0	☐	☑	☑	☑
2	MARCHA	Bool	%M0.1	☐	☑	☑	☑
3	REINICIO	Bool	%M0.2	☐	☑	☑	☑
4	L_ROJO	Bool	%Q0.1	☐	☑	☑	☑
5	L_AMARILLO	Bool	%Q0.2	☐	☑	☑	☑
6	L_VERDE	Bool	%Q0.3	☐	☑	☑	☑
7	TIEMPO_1	Time	%MD2	☐	☑	☑	☑
8	TIEMPO_2	Time	%MD10	☐	☑	☑	☑
9	TIEMPO_0	Time	%MD6	☐	☑	☑	☑
10	BUCLE	Bool	%M0.3	☐	☑	☑	☑

Fig. 97. Tabla de variables de E/S de la Práctica 2.

Programación en Ladder

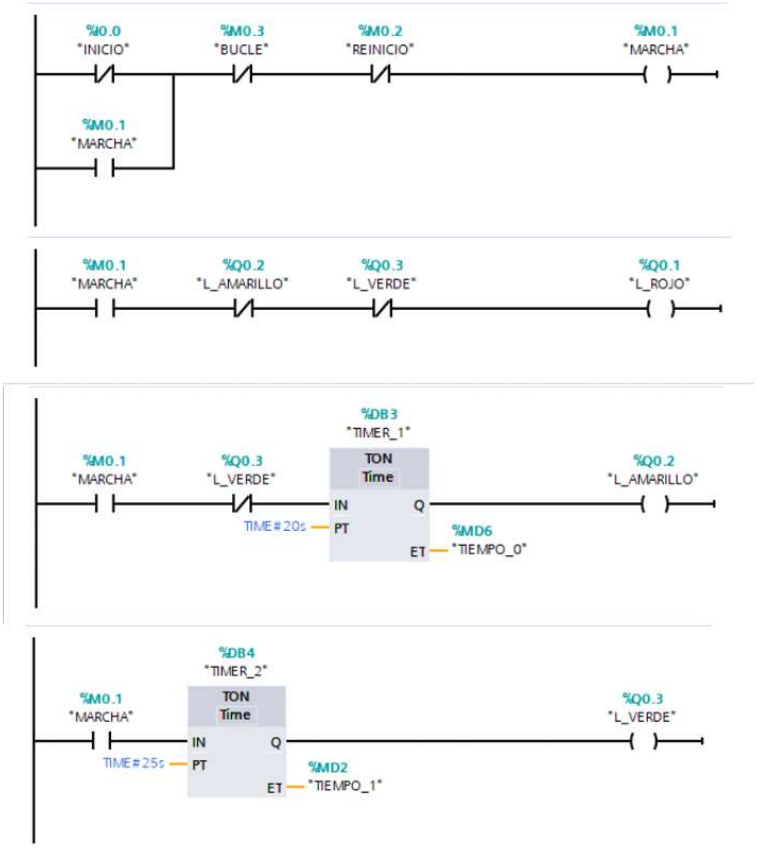


Fig. 98. Programación en lenguaje Ladder de la Práctica 2.

3.2.6.3 Práctica 3. Control de temperatura ON/OFF con termocupla PT100

<table>
<tr><td colspan="2">  </td><td colspan="2">GUÍA DE PRÁCTICAS LABREMAUT</td></tr>
<tr><td colspan="3">Carrera: Electrónica y Telecomunicaciones</td><td>Asignatura: Sensores e instrumentación</td></tr>
<tr><td>Práctica Nro.</td><td>3</td><td colspan="2">Título de Práctica: Control de temperatura ON/OFF con termocupla PT100</td></tr>
<tr><td colspan="4">Objetivos:
Realizar la programación Ladder mediante TIA Portal v16
Utilizar el módulo de comunicación SM 1241 del PLC S7-1200.
Utilizar el controlador de temperatura DTB4848.
Utilizar termocupla PT100.
Cargar el programa al PLC S7-1200 para realizar las pruebas necesarias.
Comprender la lógica de un temporizador dentro de la programación Ladder.</td></tr>
<tr><td colspan="4">Descripción de la práctica:
En esta práctica se realizará la toma de datos de una termocupla por medio de un controlador de temperatura, el cual establece una comunicación MODBUS RTU con el PLC. Para ello se harán uso de los bloques de comunicación dentro de la programación en LADDER.</td></tr>
<tr><td colspan="2" rowspan="2">Instrucciones:</td><td colspan="2">1. Verificar que el PC remoto en el que va a trabajar se encuentre encendido, caso contrario informar al docente o administrador.</td></tr>
<tr><td colspan="2">2. Desarrollar la práctica teniendo como guía el detalle de la Práctica 2 en el presente documento</td></tr>
<tr><td colspan="4">Actividades por desarrollar:
Realizar la programación en Ladder para la comunicación entre el PLC y el controlador de temperatura DTB4848.
Desarrollar la programación den Ladder para la recepción de los datos de la termocupla PT100.
Establecer la conexión con el PLC y observar por medio de la cámara su accionar.</td></tr>
<tr><td colspan="4">Resultados:
Sistema de recepción de datos desde un PT100 mediante el uso de un controlador de temperatura.</td></tr>
<tr><td colspan="4">Conclusiones:
Sistema que familiariza al estudiante en el uso de otro tipo de comunicación al ya utilizado hasta el momento (MODBUS RTU).
La correcta programación y ejecución de bloques de programación Ladder para la lectura y escritura de datos analógicos, en este caso datos de temperatura, es objetivo principal de esta práctica.</td></tr>
</table>

Recomendaciones:
Se recomienda la verificación del estado actual de la termocupla a utilizar.
Se recomienda saber el tipo de termocupla a utilizar por medio de su hoja de datos.
Se recomienda la investigación profunda del controlador de temperatura a utilizar.
Se recomienda verificar que los dispositivos a usar en la práctica se encuentren encendidos y disponibles.
Se recomienda la revisión de los anexos respectivos para la conexión remota mediante OpenVPN y detalle de práctica 3.

Tabla de variables

Las variables System_Byte, FirstScan, DiagStatusUpdate, AlwaysTRUE, AlwaysFALSE, se crean automáticamente al realizar la programación del bloque de comunicación MB_COMM (ver Figura 102) previamente habilitadas en propiedades del bloque, "Marcas de sistema y de ciclo", "Activar la utilización del byte de marcas de ciclo".

	Nombre	Tipo de datos	Dirección	Rema...	Acces...	Escrib...	Visibl...
1	System_Byte	Byte	%MB1	☐	☑	☑	☑
2	FirstScan	Bool	%M1.0	☐	☑	☑	☑
3	DiagStatusUpdate	Bool	%M1.1	☐	☑	☑	☑
4	AlwaysTRUE	Bool	%M1.2	☐	☑	☑	☑
5	AlwaysFALSE	Bool	%M1.3	☐	☑	☑	☑
6	Set_point	Word	%MW2	☐	☑	☑	☑
7	run	Bool	%M10.0	☐	☑	☑	☑
8	run_read	Bool	%M10.1	☐	☑	☑	☑
9	C_read	Word	%MW10	☐	☑	☑	☑
10	<Agregar>			☐	☑	☑	☑

Fig. 99 Tabla de variables de bloques de Práctica 3.

Bloque para la lectura de datos.

Fig. 100 Bloque para la lectura de datos de Práctica 3.

Programación en leguaje LADDER

En la Figura 101 se encuentra la programación del bloque maestro de comunicación, en REQ se coloca "FirstScan" que da inicio a la ejecución del bloque, en MB_ADDR se añade la dirección del esclavo, el parámetro MODE se configura de forma individual (ver Figura 99) variable de tipo Word ya que puede tomar en este caso dos valores, 0 o 1, dependiendo si se quiere leer o escribir los datos respectivamente.

C_read, permite cargar los valores del registro (4096, 4097) de lectura o escritura. DATA_LEN tiene un valor de 2, el cual es el tamaño del registro, DATA_PIR se crea un bloque de datos (ver Figura 100).

En el segmento 2 se configura al registro como un Set_point mediante el bloque MOVE.

En el segmento 3 se configura al registro como un Set_point mediante el bloque MOVE pero para realizar la lectura de temperatura.

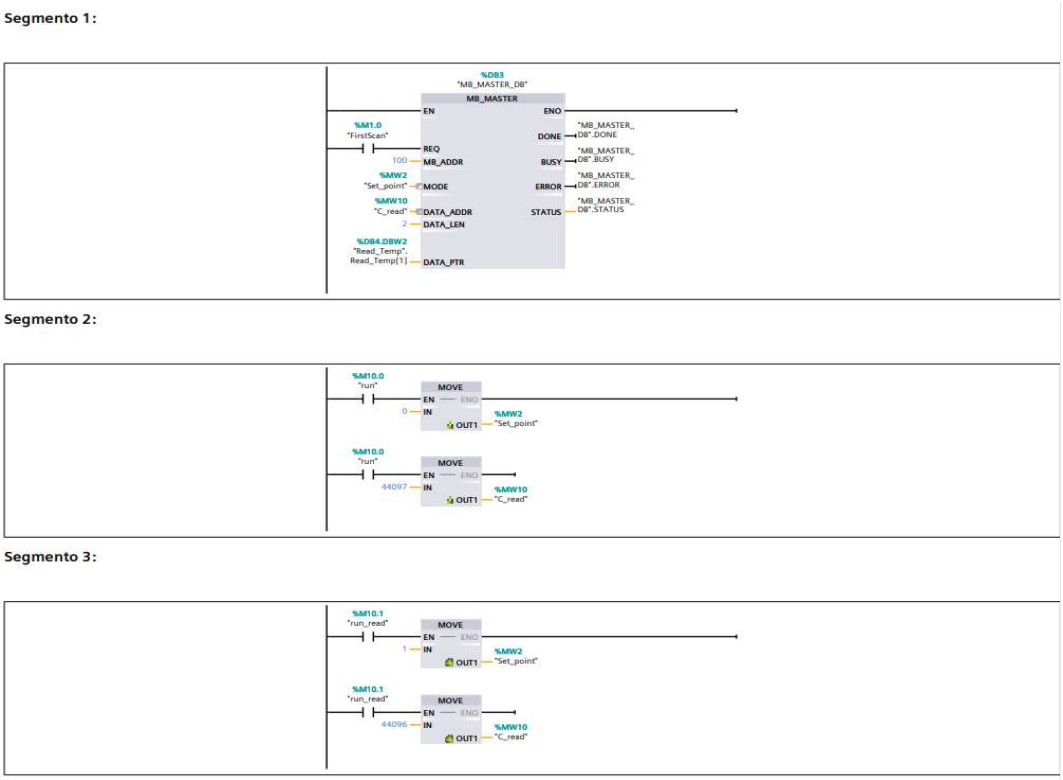


Fig. 101 Programación del bloque principal en lenguaje Ladder de la Práctica 3.

En REQ (Ejecución de instrucción) se coloca la variable "FirstScan" que ayuda en la consulta inicial de si hay o no una conexión. En PORT se verifica el puerto por el cual se va a comunicar, BAUD la velocidad de comunicación, y PARITY selección de paridad

es 0, en DONE, ERROR, STATUS, se configuran por defecto en los cuales se observará los posibles errores o instructivos de ejecución del bloque.

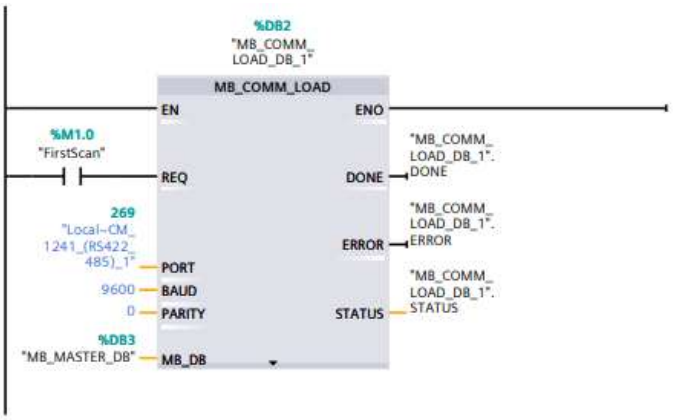


Fig. 102 Programación del bloque de comunicación en lenguaje Ladder de la Práctica 3.

En las Figuras 103. 104 se puede observar la lectura del sensor PT100 y como varia el mismo al inducirle calor, en la Figura 105 se observa la conexión del controlador DTB4848, hacia la alimentación, termocupla y puertos de comunicación hacial el módulo del PLC.

Fig. 103 Lectura inicial de temperatura del sensor PT100.

Fig. 104 Lectura de variación de temperatura de sensor PT100.

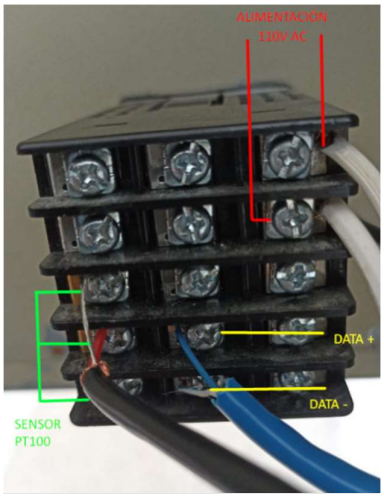


Fig. 105 Conexión del controlador de temperatura DBT4848.

3.2.6.4 Práctica 4. Clasificación de cajas por tamaño en FactoryIO y dashboard en Node-RED

<table>
<tr><td colspan="2">  </td><td colspan="2">GUÍA DE PRÁCTICAS LABREMAUT</td></tr>
<tr><td colspan="3">Carrera: Electrónica y Telecomunicaciones</td><td>Asignatura: Sensores e instrumentación</td></tr>
<tr><td>Práctica Nro.</td><td>4</td><td colspan="2">Título de Práctica: Clasificación de cajas por tamaño en FactoryIO y dashboard en Node-RED</td></tr>
<tr><td colspan="4">Objetivos:
• Controlar actuadores digitales en el software Factory IO dependiendo de los valores leídos por los sensores virtuales.
• Utilizar bloques temporizadores para el control de actuadores.
• Desarrollar un Dashboard con Node-RED para presentar datos y controlar la planta de forma remota.</td></tr>
<tr><td colspan="4">Descripción de la práctica:
Con esta práctica se pretende realizar la clasificación de cajas según su tamaño, para ello se utilizarán elementos de Factory IO que simulen una cinta transportadora por donde circulen cajas de dos tamaños diferentes, las cuales deberán tomar una u otra dirección, primero identificando su tamaño mediante la lectura de sensores infrarrojos y segundo utilizando lógica de programación en lenguaje LADDER.</td></tr>
<tr><td colspan="2" rowspan="3">Instrucciones:</td><td colspan="2">1. Verificar que el PC remoto en el que va a trabajar se encuentre encendido, caso contrario informar al docente o administrador.</td></tr>
<tr><td colspan="2">2. Revisar el anexo 2 sobre las configuraciones en TIA Portal para la conexión con Factory IO.</td></tr>
<tr><td colspan="2">3. Desarrollar la Práctica teniendo como guía el detalle de la Práctica 3 en el presente documento</td></tr>
<tr><td colspan="4">Actividades por desarrollar:
1. Desarrollar la programación para la clasificación de cajas con TIA Portal.
2. Desarrollar el Dashboard con Node-RED y configurar las variables a leer del PLC.
3. Realizar la conexión del PLC con Factory IO para las pruebas respectivas.</td></tr>
<tr><td colspan="4">Resultados:
Planta clasificadora de cajas según su tamaño con Factory IO.
Dashboard capaz de presentar el estado actual de la planta y con un control de paro de emergencia.</td></tr>
<tr><td colspan="4">Conclusiones:
Se obtiene un sistema capaz de clasificar objetos según su tamaño, además de tener la capacidad de aumentar el número de sensores y poder clasificar otros tamaños adicionales o basándose en otro tipo de característica, como su peso, forma, etc.
Con el Dashboard de Node-RED se puede tener bajo vigilancia el estado actual de la planta facilitando su estudio o análisis para personas con pocos conocimientos técnicos y con la facilidad de realizar el control de forma remota.</td></tr>
<tr><td colspan="4">Recomendaciones:
Revisión de los anexos respectivos para conexión remota mediante OpenVPN y detalle de Práctica 3.</td></tr>
</table>

Verificación de que los equipos a utilizar dentro del laboratorio estén encendidos.
En caso de presentarse algún error durante la conexión de Factory IO con el PLC, primero se debe de restablecer al PLC de fabrica conservando su dirección IP.

Tabla de variables de entrada

Para realizar la practica 4, vamos a necesitar de tres variables de entrada para el control de arranque y paro del sistema (START, STOP y RESET), además se requieres dos entradas adicionales para el uso de dos sensores infrarrojos que servirán para determinar el tamaño de las cajas a clasificar (SENSOR_SUP y SENSOR_INF), y una entrada extra para detectar cuando el pistón que empuja las cajas grandes esté en su punto máximo de empuje (LIMIT_PUSHER). Todas estas variables de entradas se pueden observar en la Figura 106.

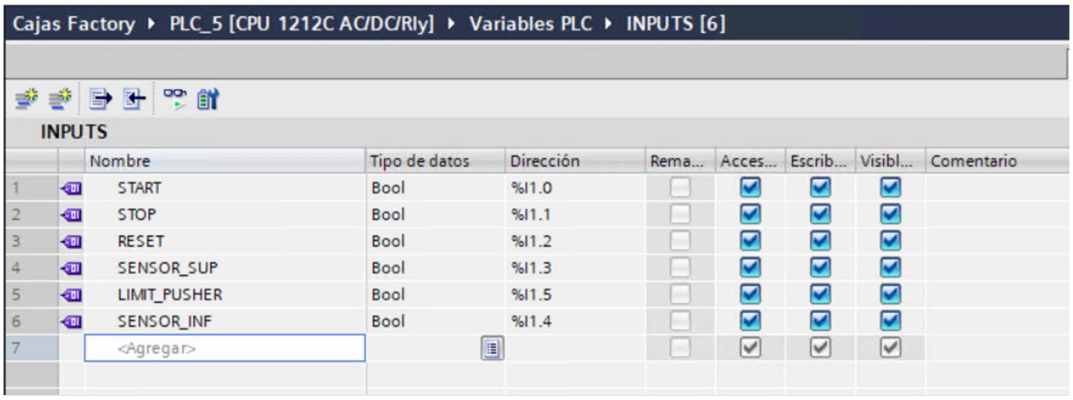


Fig. 106. Tabla de variables de entrada de la Práctica 4.

Tabla de variables de salida

Para indicar si el sistema se encuentra en funcionamiento o en parada se usarán dos variables de salida que se conectaras a dos indicadores led (L_START y L_STOP). La banda transportadora y el pistón tendrán sus propias salidas digitales (CONVEYOR y PUSHER). Para almacenar la cantidad de cajas grandes y pequeñas se requieren de otras dos variables adicionales (CJGR y CJCH). Y la última variable que podría ser opcional es la que servirá para reiniciar la simulación en Factory IO (ver Figura 107).

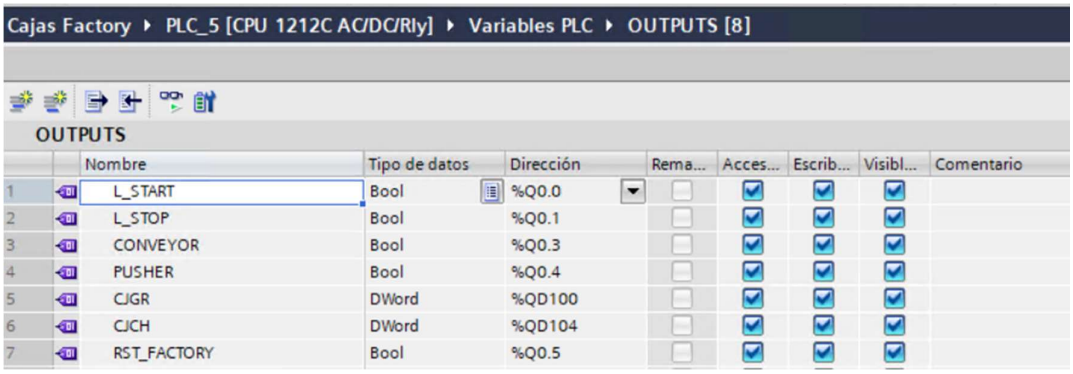


Fig. 107. Tabla de variables de salida de la Práctica 4.

Bloque de datos para comunicación con Node-RED

Para lograr que el PLC se logre comunicar de forma correcta con Node-RED, se requiere de un bloque de datos, por ello en este nuevo bloque se deben de crear variables semejantes a las ya utilizadas hasta el momento, con la finalidad de que los mismos valores puedan ser compartidos en tiempo real entre el PLC y Node-RED (ver Figura 108).

Fig. 108. Bloque de datos para la comunicación con Node-RED.

Programación en leguaje LADDER

En la primera sección del código se desarrolla el control del encendido de la cinta transportadora y los respectivos indicadores leds. En el segundo segmento se programa el accionamiento del pistón, dando un pequeño delay con la finalidad de que la caja se posicione en un lugar adecuado para ser empujada. En el tercer segmento se procede con la contabilización de las cajas según su tamaño. En la quinta sección se combinan los diferentes orígenes para las variables de entrada (Factory IO o Node-RED) en una sola variable, para ser utilizada en el resto del código. Y en la última sección se hace la sumatoria total de las cajas que han sido trasladadas y clasificadas por la cinta transportadora (ver Figura 109).

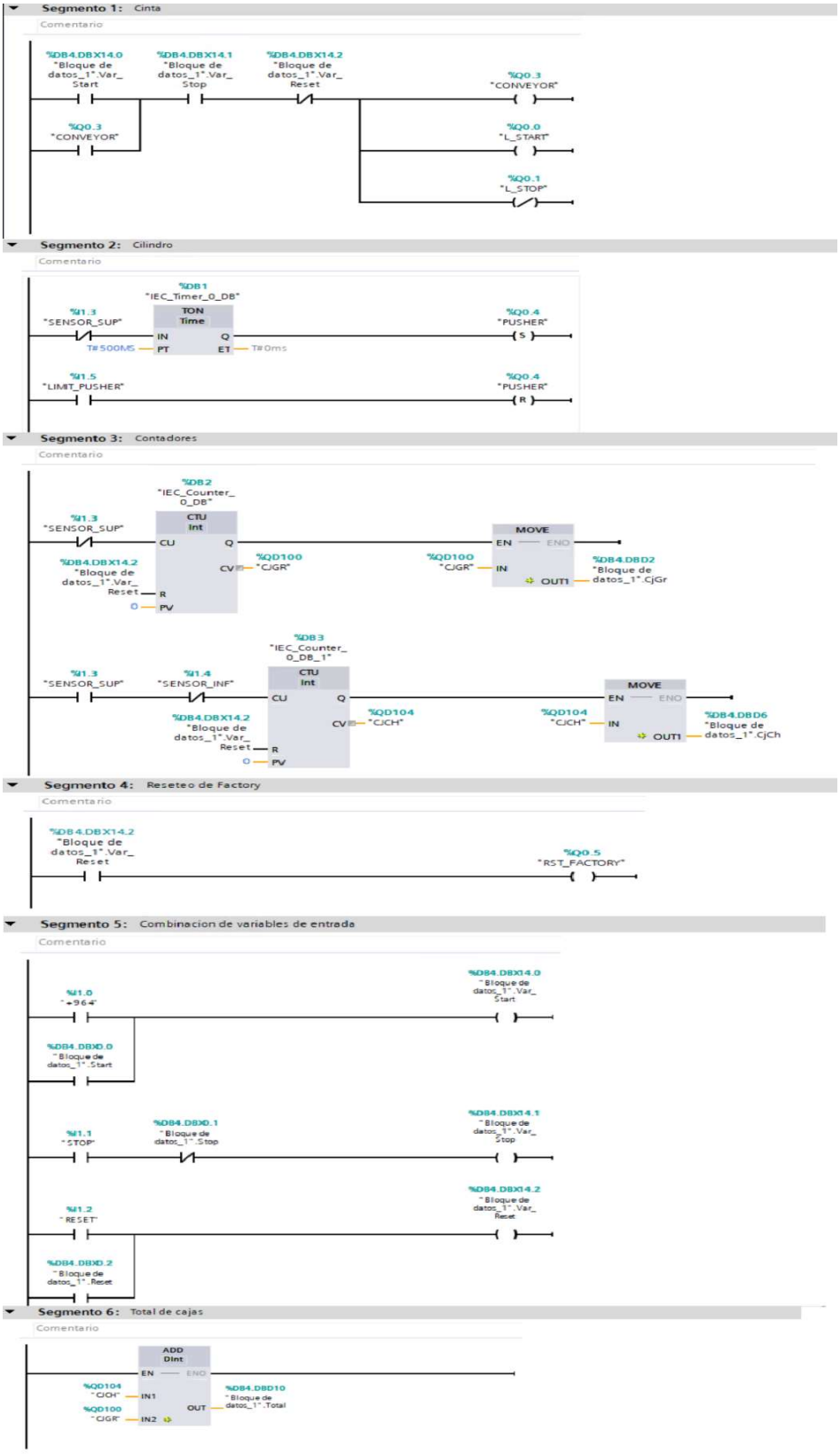


Fig. 109. Programación en LADDER de la Práctica 4.

Planta de clasificación de cajas y tablero de control elaborados en Factory IO

En la Figura 110 se observa la planta en 3D para realizar la practica 4. Incluye la cinta transportadora, con sus sensores reflectivos y el pistón, además se puede apreciar en la parte izquierda al tablero de control que servirá para iniciar o detener el proceso además cuenta con dos display que indican la cantidad de cajas grandes y pequeñas que ha logrado clasificar.

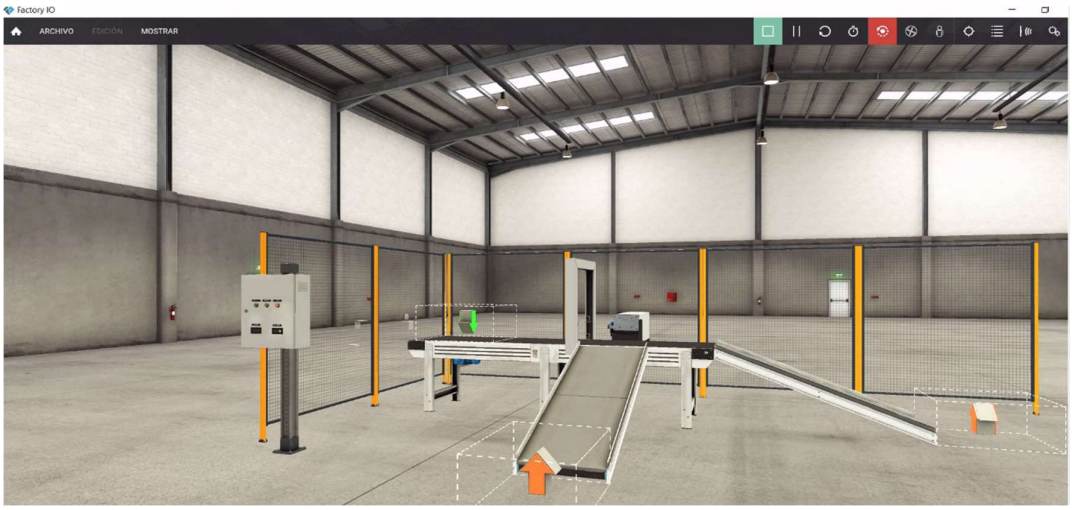


Fig. 110. Planta de clasificación de cajas.

Conexión de los elementos de la planta al PLC

Para lograr un correcto funcionamiento del sistema, en la Figura 111 se indican las variables de Factory IO y su respectiva conexión con el PLC Siemens S7-1200, cada elemento debe coincidir con las variables creadas durante la programación, tanto en variables de entrada como de salida.

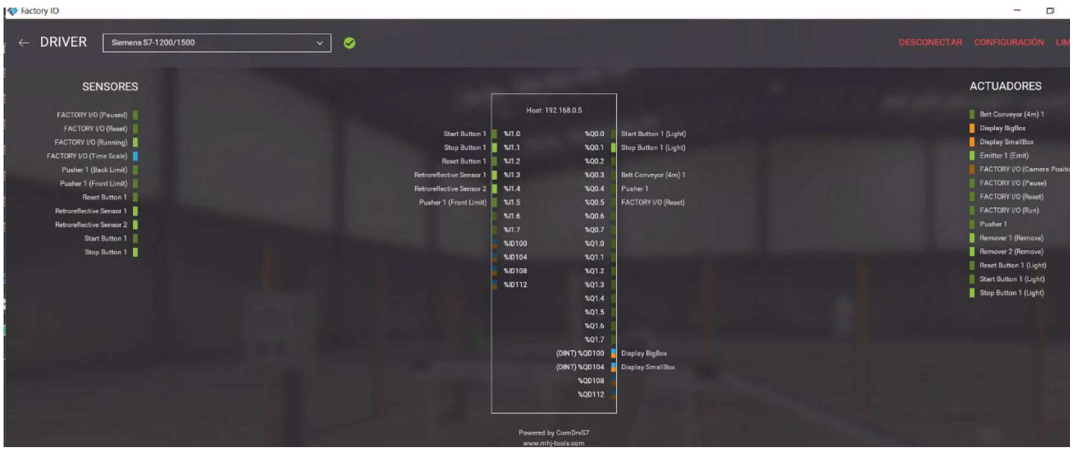


Fig. 111. Conexión de elementos de la planta al PLC.

Instrucción de arranque de Node-RED de forma local en la PC

Para inicializar el servidor de Node-RED de forma local en la computadora del laboratorio, como primer punto se procede con la ejecución de la instrucción “node-red” a través de la línea de comando (ver Figura 112).

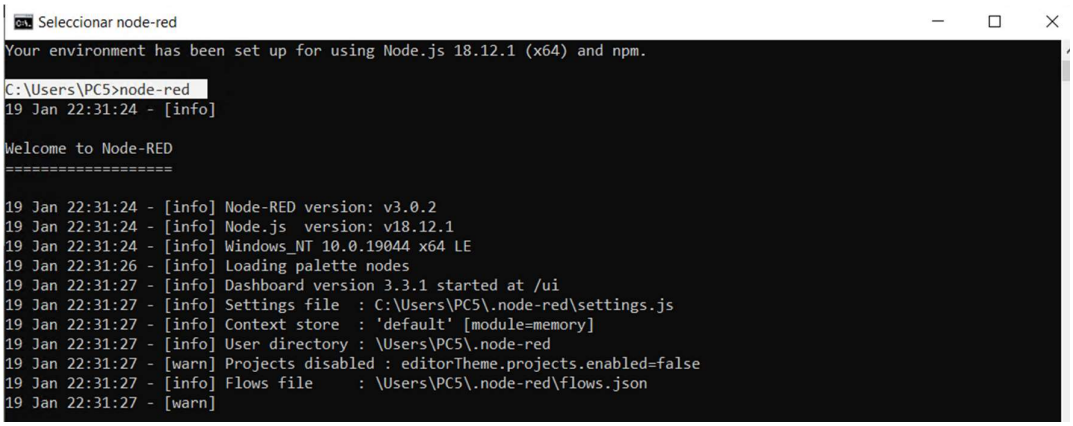


Fig. 112. Inicialización de Node-RED en PC local

Estructura de bloques de Node-RED para conexión con el PLC

En la programación de bloques de Node-RED, primero se ubicaron los 3 botones para el funcionamiento del sistema, y en la parte inferior se procede con la lectura de las variables que contienen la cantidad de cajas clasificadas para ser mostradas en el Dashboard creado con Node-RED (ver Figura 113).

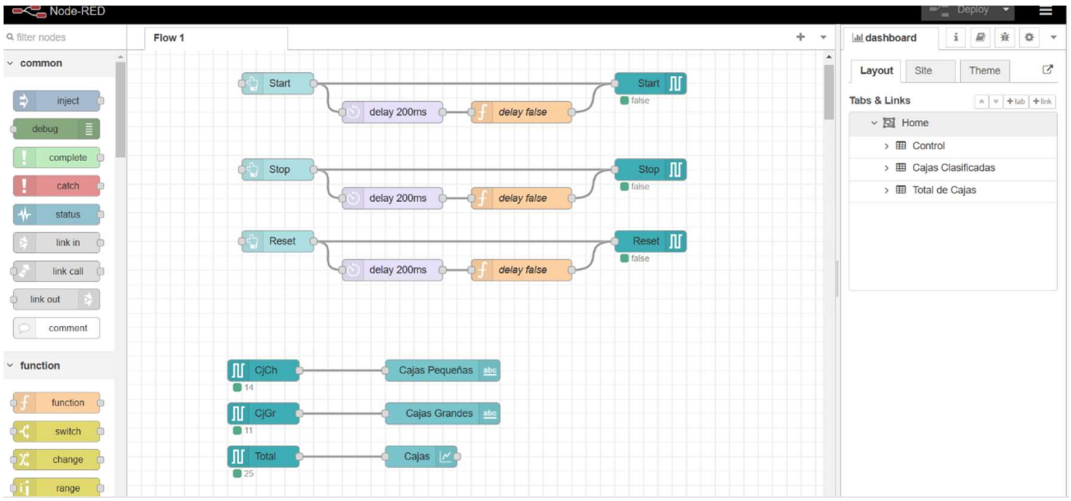


Fig. 113. Estructura de bloques de Node-RED para conexión con PLC

Dashboard de control y monitoreo remoto realizado en Node-RED

En la Figura 114 se muestra el Dashboard resultante realizado en Node-RED, desde aquí se puede iniciar o parar el sistema de forma remota, además de contar con la capacidad de visualizar la cantidad de cajas clasificadas en tiempo real.

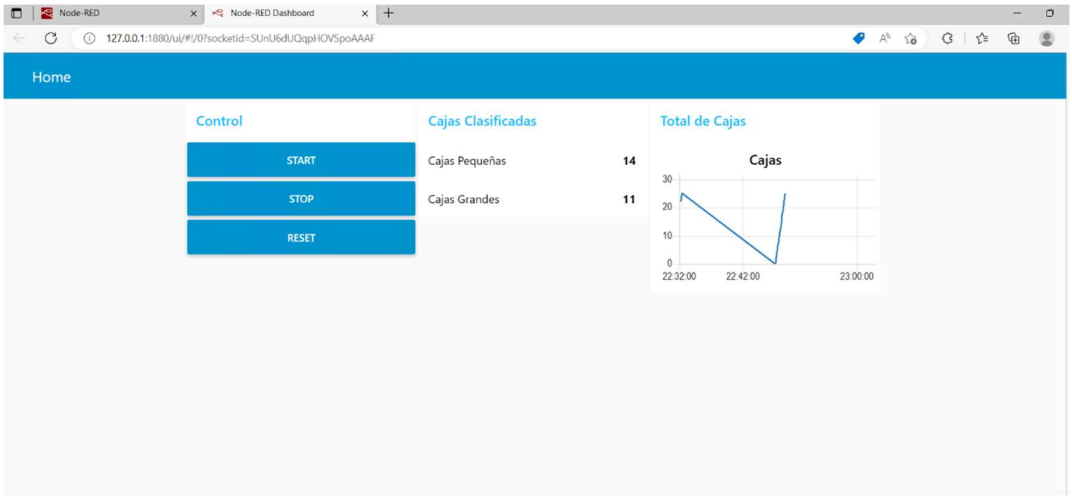


Fig. 114. Dashboard de control y monitoreo para la Práctica 4.

3.3 ESTUDIO DE FACTIBILIDAD

3.3.1 Factibilidad técnica

En la actualidad la facultad de sistemas y telecomunicaciones no cuenta con un sistema que les permita a los estudiantes tener acceso al laboratorio de automatización de manera remota, haciendo uso de todos los equipos que éste ofrece únicamente de forma presencial para el desarrollo integral de los estudiantes, motivo por el cual se propone como solución, el diseño y la implementación de un laboratorio remoto para la facultad.

Para el diseño de esta propuesta, se realizó un estudio de las tecnologías ya existentes, teniendo como resultado el uso de diferentes herramientas en conjunto con protocolos de comunicación que ayudaran a el correcto funcionamiento de este sistema.

El diseño del laboratorio remoto propone la utilización tecnologías VPN gracias a un router Mikrotik, programación avanzada haciendo uso de la API de RouterOS, redes de comunicación Ethernet, MODBUS RTU RS485, en consecuencia, se tomó en cuenta varios elementos que conforman parte fundamental del proyecto y que están detalladas en la sección de componentes de la propuesta en el presente documento.

Adicional a la implementación de este sistema de laboratorio remoto, se realizó Prácticas básicas para el uso de los elementos que están dentro del laboratorio de automatización, siendo los estudiantes los mayores beneficiados en esta propuesta tecnológica.

3.3.2 Factibilidad económica

TABLA XVII. COSTO DE EQUIPOS PARA LA IMPLEMENTACIÓN DEL LABORATORIO REMOTO

NOMBRE	CANTIDAD	PRECIO U.	TOTAL
PLC S7-1200 CPU 1212C AC/DC/RELE	1	$ 473,00	$ 473,00
MODULO SM 1222	1	$ 200,00	$ 200,00
MODULO SM 1241	1	$ 257,00	$ 257,00
CONTROLADOR DE TEMPERATURA DTB4848	1	$ 104.52	$ 104,52
SENSOR DE TEMPERATURA PT100	1	$ 15,00	$ 15,00
ROUTER MIKROTIK RB2011UiAS-2HnD-IN	1	$ 178,00	$ 178,00
CABLES (UTP-PROFINET-MODBUS)	1	$ 50,00	$ 50,00
SIEMENS BREAKER RIEL-DIN 1 POLO 50 A 230/400v	2	$ 23,00	$ 46,00
SWITCH TP-LINK	1	$ 15,00	$ 15,00
INDICADOR LED 16MM	12	$ 1,35	$ 16,20
CAMARA IP NEXXT	1	$ 50,00	$ 50,00
PONCHADORA CRIMPADORA RJ45	1	$ 12,00	$ 12,00
TOTAL			**$ 1416,72**

3.4 PRUEBAS Y RESULTADOS

3.4.1 Pruebas del Sistema

Como primer punto a evaluar, se procedió con la verificación de que el docente o el administrador del sistema tenga la disponibilidad de verificar los PLC que se encuentren encendidos desde la aplicación web, además de encender las computadoras de forma remota. En la Figura 115 se muestran los dispositivos encendidos al momento de realizar la prueba, y se puede notar que hay solamente dos PLC encendidos mediante un indicador de color verde y que ninguna computadora esta encendida.

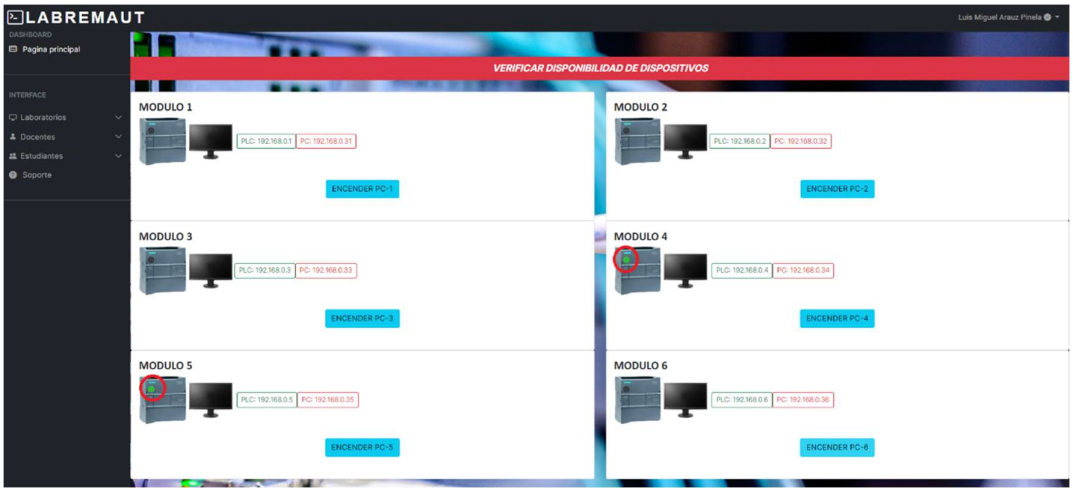


Fig. 115. Test de verificación de dispositivos activos

Luego de dar clic en el botón para encender la PC-6 y volver a escanear los dispositivos encendidos se muestra la siguiente (ver Figura 116).

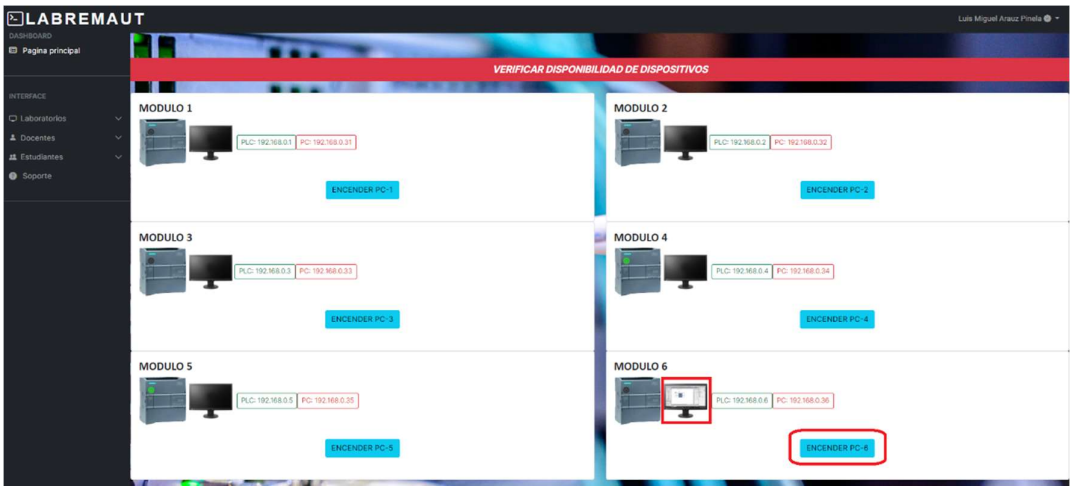


Fig. 116. Test de verificación de encendido remoto de PC

El monitor de la PC-6 muestra una imagen característica de TIA Portal, indicando con esto que la PC se encuentra encendida y demostrando a su vez que en encendido remoto esta correctamente operativo.

Para continuar con las pruebas del sistema, se pidió la colaboración de dos estudiantes para que utilicen el sistema y que procedan a agendar un turno en la misma fecha y hora, pero cada uno en una PC (laboratorio) diferente, esto con la finalidad de evaluar posibles inconvenientes por latencia o por consumo excesivo de recursos del sistema.

Luego de que los estudiantes agendaron su turno en el aplicativo web, su agendamiento queda almacenado en la base de datos, esto se muestra en la Figura 117.

Fig. 117. Almacenamiento del agendamiento de turno en la base de datos

En simultaneo el servidor web se comunica mediante la API de RouterOS para programar el acceso de los estudiantes hacia los hosts internos del laboratorio, para ello crea dos Scheduler para cada agendamiento, el primero para permitir el acceso, y el segundo para quitárselo (ver Figura 118).

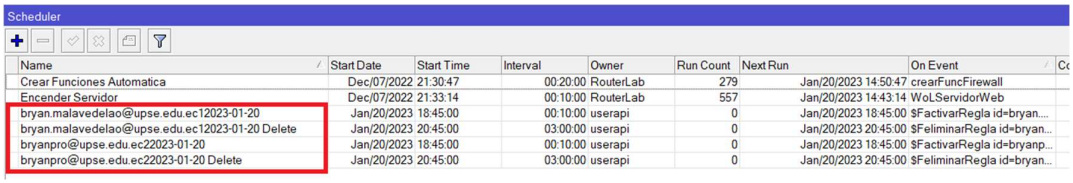


Fig. 118. Scheduler para automatizar el acceso de los estudiantes.

En total son 5 instrucciones que se deben ejecutar en el MikroTik para programar el agendamiento correctamente, primero se debe de crear una regla de firewall para permitir el acceso desde la IP de la VPN remota hacia la IP local de la PC a la que se va a conectar, luego esta regla debe de posicionarse sobre otra regla que bloquea el acceso a todas las demás IP remotas, al crear una regla de firewall en MikroTik viene habilitada por defecto, por ello el siguiente paso es deshabilitar la regla para que posteriormente sea habilitada y eliminada por los dos Scheduler creados al final. Todo esto se puede apreciar desde el Log en RouterOS mediante WinBox (ver Figura 119).

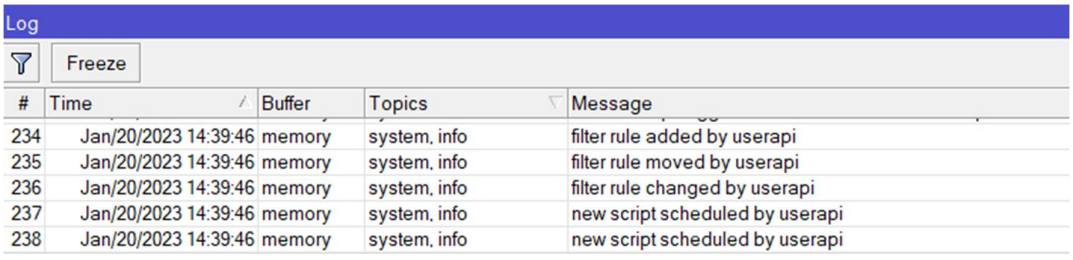


Fig. 119. Procesos internos de RouterOS para el agendamiento.

Si nos trasladamos a las reglas de Firewall en WinBox se puede apreciar las dos reglas generadas que se encuentran temporalmente deshabilitadas y ubicadas sobre la regla

general para el bloqueo de todas las IP asignadas a los estudiantes remotos (ver Figura 120).

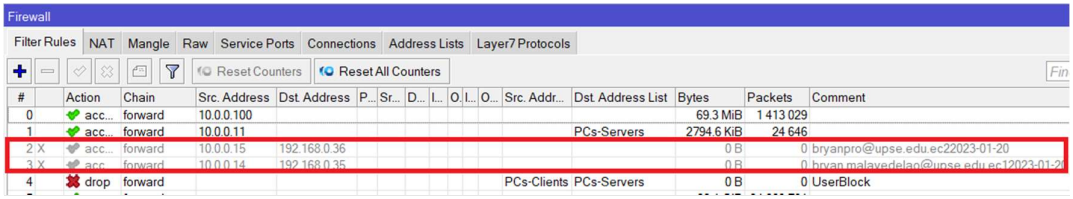


Fig. 120. Reglas de Firewall resultantes del agendamiento.

Verificando en conjunto la ventana del Log con la del Firewall se puede notar que a la hora indicada para el agendamiento se habilitaron ambas reglas, permitiendo el acceso de los estudiantes remotos (ver Figura 121).

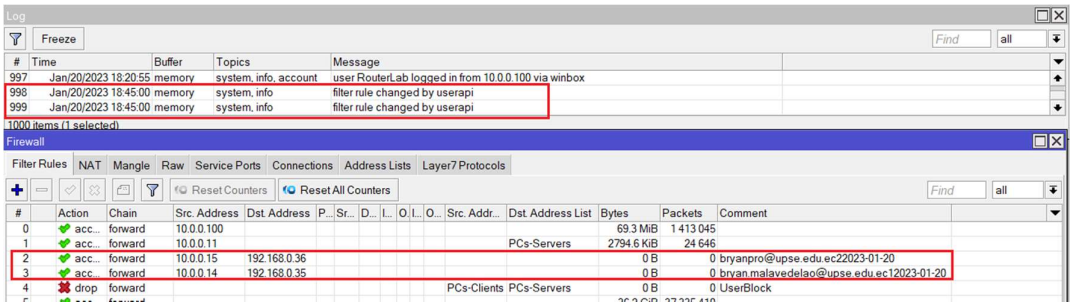


Fig. 121. Habilitación automática de regla de Firewall.

Finalmente, luego de que la sesión concluya, el Scheduler para la eliminación de residuos cumple su cometido, y éste elimina la regla de Firewall bloqueando el acceso para el estudiante en cuestión, además de eliminar también los Scheduler creados durante el proceso de agendamiento, por consiguiente, se evita que archivos residuales congestionen la memoria del Router (ver Figura 122).

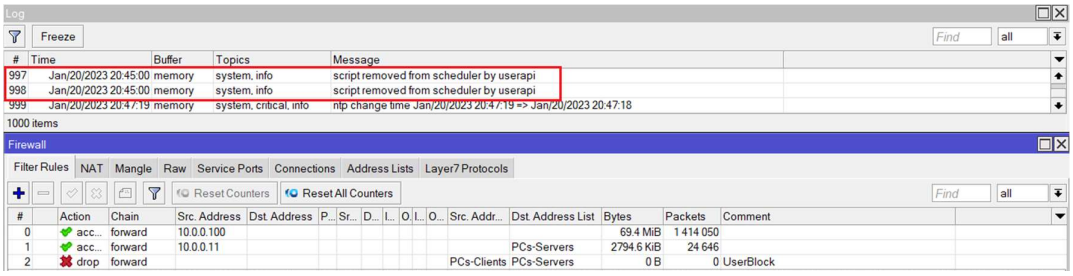


Fig. 122. Eliminación automática de reglas de Firewall.

Durante el tiempo que la regla de Firewall que permite el acceso esté activa, el estudiante puede conectarse a la VPN y tendrá acceso a la red interna del laboratorio, posteriormente puede conectarse mediante el protocolo RDP a la PC que le corresponda dentro del

laboratorio para realizar la práctica que le haya asignado el docente. En la Figura 123 se muestran los pasos que realiza el MikroTik para autenticar que la conexión remota sea válida, también indica la IP que se la ha asignado mediante la VPN por medio de la cual se realiza el acceso controlado al laboratorio.

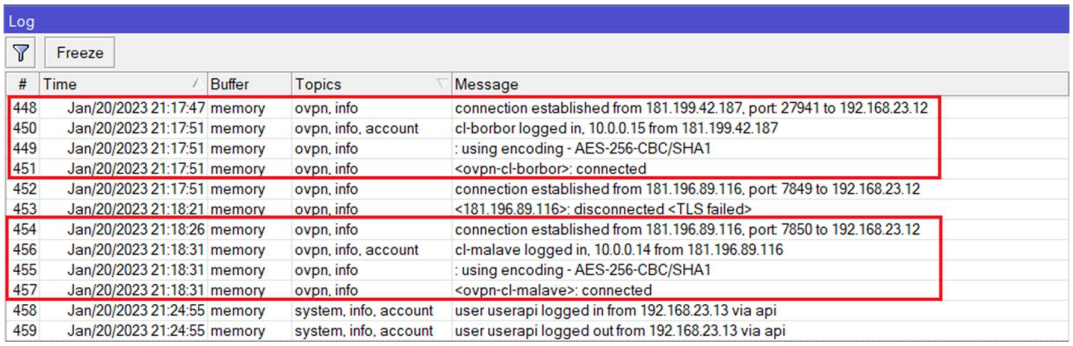


Fig. 123. Log de la conexión remota mediante OpenVPN.

Desde la vista de interfaces del Router MikroTik se crea una interfaz virtual por cada cliente remoto conectado, además si se está haciendo uso de los equipos internos del laboratorio también se puede observar el tráfico de entrada y salida (ver Figura 124).

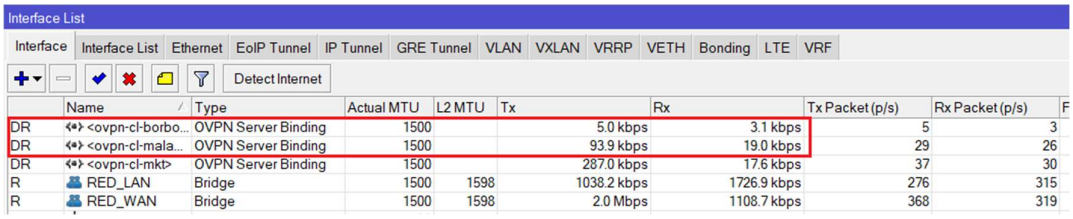


Fig. 124. Clientes remotos conectados por VPN.

En la Figura 125 se está analizando el tráfico de datos que ocupan ambos clientes remotos en simultaneo, mientras hacen uso de la PC asignada dentro del laboratorio mediante el protocolo RDP.

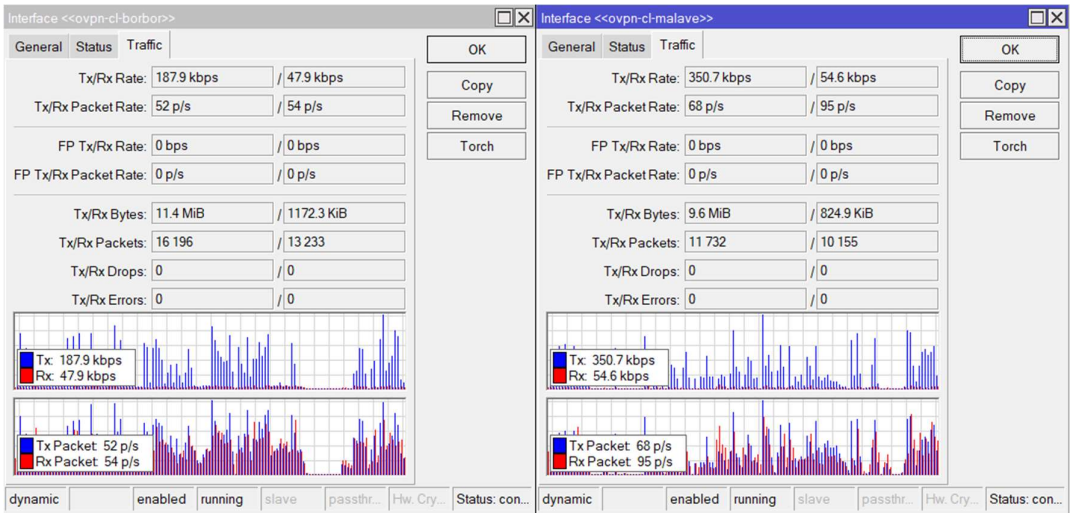


Fig. 125. Análisis del tráfico de datos de los clientes remotos.

Como se observa en la imagen anterior el tráfico generado por los clientes no superan los 500 kbps, además la carga del CPU está muy por debajo del 50% (ver Figura 126), por lo que se concluye que el sistema está trabajando de forma óptima y garantiza que no se va a saturar durante su operación.

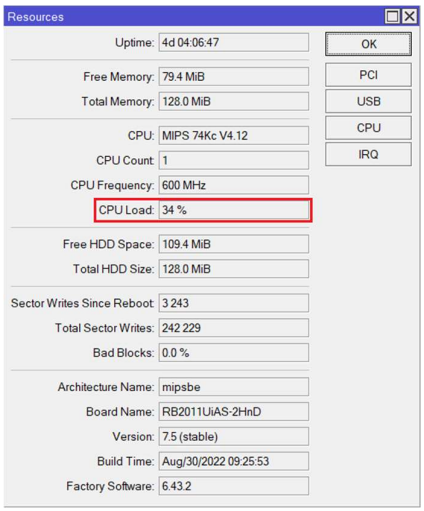


Fig. 126. Estado de los recursos del Router MikroTik.

Para finalizar con las pruebas del sistema, a continuación, se presentan capturas de pantalla realizadas por los estudiantes voluntarios que participaron haciendo uso del laboratorio (ver Figuras 127 y 128).

Fig. 127. Comparativa de IP remota del estudiante 1.

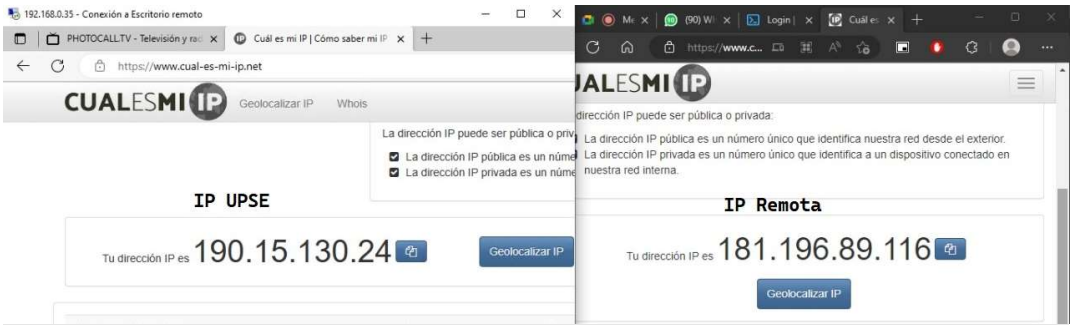


Fig. 128. Comparativa de IP remota del estudiante 2.

3.4.2 Resultados

Los resultados que se obtuvieron con el presente proyecto se indican a continuación.

- Se obtuvo un rack para Prácticas industriales equipados con elementos de control, sensores, actuadores, entre otros módulos de comunicación, todo ello con las debidas protecciones eléctricas, como fusibles, relé térmico, etc.
- Se implemento un rack de comunicación que centralizo la administración de la red del laboratorio, permitiendo la interconexión entre todos los módulos de prácticas y cada uno de los elementos que cuenten con el protocolo de comunicación ethernet.
- Se implementó un servidor de OpenVPN en un router MikroTik, con la finalidad de brindar acceso remoto al laboratorio, garantizando la confidencialidad e integridad de los datos que viajen a través de la red VPN.
- Se logro la interconexión de todos los PLC Siemens ubicados dentro del laboratorio, además de otros elementos como HMI y variadores de frecuencia que fueron compatibles con el protocolo industrial PROFINET basado en el estándar abierto TCP/IP,

permitiendo configurar y/o monitorear a los elementos desde cualquier puerto de red del laboratorio o mediante Wifi.

- Se desarrollo un aplicativo web que permite el acceso controlado a la red interna del laboratorio de forma remota, además de contar con otras características exclusivas para el docente o el administrador del sistema.

CAPITULO IV

4. CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

Según las diferentes pruebas realizadas al sistema del laboratorio remoto con la finalidad de comprobar el funcionamiento y la estabilidad de éste, se ha llegado a las siguientes conclusiones:

- Se obtuvo tableros de control equipados con elementos de entrada y salida que cumplan con las normativas y estándares internacionales, basándose en la norma IEC 1082-1 para el diseño del esquema eléctrico y en la norma IEC 60947 para las protecciones eléctricas en baja tensión, que en nuestro caso no superan los 220 V.
- Se incorporó un rack de comunicaciones con soporte para un PC de escritorio tipo torre que cumplirá la función de servidor web, además, se reacondiciono el switch de distribución para la incorporación de los elementos electrónicos que cuenten con capacidad ethernet, cumpliendo con el estándar ANSI/EIA/TIA-568-A para el cableado estructurado.
- Se obtuvo un sistema de red robusto con capacidad para permitir el acceso remoto de los usuarios de forma segura mediante el uso de Redes Privadas Virtuales (VPN) haciendo uso de una llave criptográfica RSA (*Rivest, Shamir y Adleman*) de 4096 bits con método de autenticación SHA1 (*Secure Hash Algorithm-1*) y cifrado AES-256 (*Advanced Encryption Standard* - 256).
- Se incorporó un sensor industrial para monitorear una variable en tiempo real haciendo uso del controlador de temperatura DTB4848 mediante comunicación serial MODBUS RTU RS485 debido a que las entradas analógicas del PLC se encuentran en uso y dependiendo del resultado deseado realizar el control del actuador correspondiente.
- Se planteó la implementación de un sistema de control de encendido de los PLC de forma remota haciendo uso de un microprocesador de bajo consumo energético.
- Se implementó una red de datos capaz de permitir la interconexión de todos los PLC y demás elementos eléctricos compatibles con PROFINET, además, se habilito la programación de los Autómatas programables de forma inalámbrica mediante el estándar Wifi.

- Se desarrollaron cuatro prácticas de laboratorios con TIA Portal y Factory IO para la adquisición de conocimientos solidos relacionados con la programación a nivel industrial de Controladores Autómatas Programables, además de hacer uso de tecnologías de vanguardia con IoT utilizando Node-RED.
- Se implementó un sistema de agendamiento para el control de acceso al laboratorio de forma remota, haciendo uso de software libre como Linux, Nginx, PHP y MySQL, y se desarrolló el control de acceso haciendo uso del protocolo abierto OpenVPN.

4.2 RECOMENDACIONES

- Se recomienda el mantenimiento cada cierto periodo de tiempo de los módulos usados en las Prácticas, para garantizar su buen funcionamiento ante posibles errores.
- El docente o administrador encargado de la página web debería borrar las fechas vencidas en el listado de personas agendadas en los diferentes módulos, así como eliminar el acceso a usuarios inactivos, lo recomendable es hacer una actualización de datos cada inicio de periodo lectivo.
- Se recomienda hacer uso del sistema de encendido y apagado de los dispositivos por medio de un microcontrolador o microprocesador como Rasberry Pi, sean estos sensores, actuadores, etc.
- Se recomienda una actualización del hardware de cada estación de trabajo con el fin de brindarle al estudiante una mayor experiencia al momento de realizar las prácticas de laboratorio.
- Se recomienda el uso de un servidor netamente en el uso de la cámara IP, para disminuir considerablemente la latencia entre la visualización en la página y lo que esté pasando en el laboratorio.

REFERENCIAS

[1] Naciones-Unidas, «Informe de políticas: La educación durante la COVID-19 y después de ella,» 1 Agosto 2020. [En línea]. Available: https://www.un.org/sites/un2.un.org/files/policy_brief_-_education_during_covid-19_and_beyond_spanish.pdf.

[2] J. Vargas, J. Cuero y C. Torres, *ESPACIOS,* vol. 41, 2020.

[3] C. A. Matarrita y S. B. Concari, «Hacia un estado del arte de los laboratorios remotos en la enseñanza de la física,» *Enseñanza de la Fisica,* vol. 27, 2015.

[4] D. Pontaza, «Tecnologico de Monterrey,» 1 Marzo 2018. [En línea]. Available: https://tec.mx/es/noticias/nacional/educacion/laboratorios-remotos-una-opcion-para-la-educacion-distancia. [Último acceso: 27 Enero 2022].

[5] LabsLand, «LabsLand,» 2022. [En línea]. Available: https://labsland.com/es/about. [Último acceso: 27 Enero 2022].

[6] G. Bonilla, «Laboratorio Remoto Arduino para la realizacion de practicas de electronica en la escuela de sistemas de la Pontificia Universidad Catolica del Ecuador Sede Santo Domingo,» Santo Domingo, 2017.

[7] N. Electritelecom, «Nodo,» 2022. [En línea]. Available: https://www.nodo.com.ec/quienes-somos/. [Último acceso: 27 Enero 2022].

[8] Nodo, «Academia Nodo,» 2022. [En línea]. Available: https://academia.nodo.com.ec/robotica. [Último acceso: 27 Enero 2022].

[9] R. Zamora, Análsis de requerimiento para la implementación de Laboratorios Remotos, Barranquilla: Universidad de la Costa, 2021.

[10] P. W. H. Esneider, «Arquitectura de un Laboratorio Remoto Desde el Enfoque de la Formación de Ingenieros en EaD,» 22 Junio 2014. [En línea]. Available: https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1440/1759.

[11] O. A. J. B. Juan Montero-Vilela, Automatización, Digitalización y Robotización: Definición y protagonismo en la RSC del IBEX 35., Sevilla: Universidad Rovira, 2019.

[12] M. P. G. Juan Carlos Martín, Automatismos Industriales, Madrid: Editex S.A, 2012.

[13] C. Mathas, «Digi-Key Electronics,» 27 10 2011. [En línea]. Available: https://www.digikey.com/es/articles/temperature-sensors-the-basics. [Último acceso: 27 01 2022].

[14] Alpha, «Europe Heaters S.L.,» 16 Mayo 2014. [En línea]. Available: http://santiescoin.com/definiciones/resistencia-electrica-calefactora/. [Último acceso: 27 Enero 2022].

[15] Chint, «CHINT,» Mayo 2021. [En línea]. Available: https://www.chint.eu/content/download/7134/file/Chint_Catálogo2021_SOLUCIONES PARA LA INDUSTRIA - RELES TERMICOS.pdf.

[16] R. Y. L. M. Vicente Gerrero, Comunicaciones Industriales, Marcombo, 2017.

[17] Cisco, «Cisco,» 2022. [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13769-5.html.

[18] F. Candelas, «Protocolo de Mensajes de Control de Internet,» [En línea]. Available: https://rua.ua.es/dspace/bitstream/10045/11605/1/Pr2-2009-10.pdf. [Último acceso: 30 Septiembre 2022].

[19] Wireshark, «WakeOnLan,» [En línea]. Available: https://wiki.wireshark.org/WakeOnLAN.md. [Último acceso: 1 Octubre 2022].

[20] ccnadesdecero, «¿Qué es Wake-on-LAN y Cómo Habilitarlo?,» [En línea]. Available: https://ccnadesdecero.es/que-es-wake-on-lan/. [Último acceso: 1 Octubre 2022].

[21] yatritrivedi, «What Is Wake-on-LAN, and How Do I Enable It?,» [En línea]. Available: https://www.howtogeek.com/70374/how-to-geek-explains-what-is-wake-on-lan-and-how-do-i-enable-it/. [Último acceso: 1 Octubre 2022].

[22] IONOS, «IONOS,» 2022. [En línea]. Available: https://www.ionos.es/digitalguide/servidores/know-how/ethernet-ieee-8023/.

[23] Dell, «Dell Technologies,» 2021. [En línea]. Available: https://www.dell.com/support/kbdoc/es-pe/000150398/terminolog%C3%ADa-y-explicaciones-de-ieee-802-11-wireless.

[24] Cloudflare, «Cloudflare,» [En línea]. Available: https://www.cloudflare.com/es-es/learning/video/what-is-http-live-streaming/.

[25] «WNI,» 2022. [En línea]. Available: https://wni.mx/index.php/izqtienda?page=shop.product_details&category_id=79&flypage=flypage_new.tpl&product_id=569#:~:text=RouterOS%20es%20el%20sistema%20operativo,Enrutamiento.

[26] Mikrotik, «MikroTik Documentation,» [En línea]. Available: https://wiki.mikrotik.com/wiki/Manual:System/Scheduler. [Último acceso: 6 Noviembre 2022].

[27] M. LABS, «MIKROTIK LABS,» 18 07 2019. [En línea]. Available: https://www.mikrotiklabs.com/2019/07/18/como-crear-una-red-bridge-lan-wlan/. [Último acceso: 2022].

[28] L. P. Belomonte, Comunicaciones industriales y WinCC, España: Marcombo, 2018.

[29] M. Bowne, «PI North America,» 2020. [En línea]. Available: https://us.profinet.com/como-elegir-una-topolgia-de-red/. [Último acceso: 6 Agosto 2022].

[30] d. B. Camara de Comercio, «Gerencia de equipos remotos usando tecnologias,» Bogotaa, 2021.

[31] J. A. Castillo, «Profesional Review,» 5 Abril 2020. [En línea]. Available: https://www.profesionalreview.com/2020/04/05/openvpn-que-es/. [Último acceso: 2022 Agosto 2022].

[32] D. Garcia Muñoz, Implementacion deuna VPN tipo cliente para una entidad financiera, Lima: Universidad Tecnologica de Peru, 2021.

[33] FFmpeg, «FFmpeg,» [En línea]. Available: https://www.ffmpeg.org/about.html.

[34] D. Rodriguez, «Programming Historian,» 20 12 2018. [En línea]. Available: https://programminghistorian.org/es/lecciones/introduccion-a-ffmpeg.

[35] R. Porras, Descripción de un laboratorio de automatización y control industrial, Lima: Universidad César Vallejo, 2017.

[36] Contaval, «Contaval,» 21 Enero 2016. [En línea]. Available: https://www.contaval.es/programacion-tipo-ladder/. [Último acceso: 27 Enero 2022].

[37] P. I. Carlos Calderón, Diseño e implementación de un entorno virtual y laboratorio remoto para el aprendizaje de la catedra de teoría electromagnética., Riobamba - Ecuador: Universidad Nacional de Chimborazo, 2019.

[38] P. P. Estefania Bravo, Desarrollo de laboratorio remoto virtual para secuencias de cilindros hidráulicos de un banco de pruebas en el laboratorio de neumática y oleohidráulica de la facultad de mecánica., Riobamba - Ecuador: Escuela Superior Politécnica de Chimborazo, 2019.

[39] C. Arguedas, Diseño y desarrollo de un Laboratorio Remoto para la enseñanza de la física en la UNED de Costa Rica., Costa Rica: Universidad Nacional del Litoral, 2017.

[40] "Mikrotik," 2022. [Online]. Available: https://mikrotik.com/product/RB2011UiAS-2HnD-IN. [Accessed 1 Septiembre 2022].

[41] «Arubanetworks,» 2016. [En línea]. Available: https://www.arubanetworks.com/assets/_es/ds/DS_1920SwitchSeries.pdf.

[42] «SIEMENS,» 2022. [En línea]. Available: https://mall.industry.siemens.com/mall/en/ww/catalog/product/6es7215-1bg40-0xb0.

[43] SIEMENS, «SIEMENS INDUSTRY MALL,» 2022. [En línea]. Available: https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7212-1BE40-0XB0.

[44] SIEMENES, «INDUSTRY MALL CM 1241,» 2022. [En línea]. Available: https://mall.industry.siemens.com/mall/es/WW/Catalog/Product/6ES7241-1CH32-0XB0.

[45] «Codigoelectronica,» 2018. [En línea]. Available: http://codigoelectronica.com/blog/raspberry-pi-1-modelo-b.

[46] DELTAACDrivers, «DELTAACDrivers,» 2020. [En línea]. Available: https://deltaacdrives.com/deltadop-b03e211-human-machine-interface/.

[47] RSdelivers, «rsdelivers,» 2020. [En línea]. Available: https://cl.rsdelivers.com/product/delta-electronics/dop-b03e211/pantalla-tactil-hmi-delta-electronics-de-43-in-tft/7951627.

[48] SIEMENS, «INDUSTRY MALL,» 2022. [En línea]. Available: https://mall.industry.siemens.com/mall/es/WW/Catalog/Product/6ES7222-1HF32-0XB0.

[49] Siemens, «Industry Mall Siemens,» 2020. [En línea]. Available: https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/5SL3220-7In.

[50] DELTA, «mechtric,» 2018. [En línea]. Available: https://www.mechtric.com.au/wp-content/uploads/2018/11/DTB_Manual.pdf. [Último acceso: 20 Enero 2023].

[51] SIEMENS, «Siemens,» 2 Octubre 2022. [En línea]. Available: https://fichastecnicas.s3-us-west-2.amazonaws.com/Siemens/%5BS60610%5D+MOTOR+TRIFASICO+1800RPM+0,75HP+220-440V+1LA7+073-4YA60+++1LE0142-0DB26-4AA4-Z.pdf10%255D%2BMOTOR%2BTRIFASICO%2B1800RPM%2B0%2C75HP.

[52] R. Anrrango, «Configurar Mikrotik Wireless,» 2014. [En línea]. Available: https://configurarmikrotikwireless.com/blog/conceptos-winbox-configurar-mikrotik.html.

[53] Mikrotik, «Manual:API,» [En línea]. Available: https://wiki.mikrotik.com/wiki/Manual:API. [Último acceso: 1 Octubre 2022].

[54] E. Maya, «Automatización del proceso de reconexión de usuarios en fechas de corte con uso de la API de Mikrotik,» Universidas de Antioquia, Medellin, 2021.

[55] S. NordVPN, «NordVPN,» 2022. [En línea]. Available: https://support.nordvpn.com/es/Informaci%C3%B3n-general/1821135152/-Qu%C3%A9-es-OpenVPN.htm. [Último acceso: 10 Agosto 2022].

[56] H. RouterOS, «Help Mikrotik,» 2022. [En línea]. Available: https://help.mikrotik.com/docs/display/ROS/OpenVPN. [Último acceso: 10 Agosto 2022].

[57] S. Borges, «infranetworking,» 9 Junio 2020. [En línea]. Available: https://blog.infranetworking.com/servidor-lamp/.

[58] Universidad Michoacana de San Nicolás de Hidalgo, «Curso de SQL,» [En línea]. Available: https://www.fcca.umich.mx/descargas/apuntes/academia%20de%20informatica/Base%20de%20Datos%20%20I%20%20%20%20G.A.G.C/Curso%20de%20SQL.pdf. [Último acceso: 05 Octubre 2022].

[59] Universidad Autónoma del Estado de Hidalgo, «Introducción a SQL,» [En línea]. Available: http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro14/51_introduccin_a_sql.html. [Último acceso: 05 Octubre 2022].

[60] PHP.NET, «Manual PHP,» [En línea]. Available: https://www.php.net/manual/es/intro-whatis.php. [Último acceso: 05 Octubre 2022].

[61] M. Alvarez, «DesarrolloWeb Manual de PHP,» [En línea]. Available: https://waltercarnero.com/cfp/tpprgweb/Manual_Basico_PHP.pdf. [Último acceso: 05 Octubre 2022].

[62] O. Rieder, «HelpWire,» 8 Noviembre 2021. [En línea]. Available: https://www.helpwire.app/blog/rdp-vs-anydesk/. [Último acceso: 7 Agosto 2022].

[63] TeamViewer, «TeamViewer,» 2022. [En línea]. Available: https://www.teamviewer.com/es-mx/. [Último acceso: 7 Agosto 2022].

[64] J. R. Vaello, «FESTO,» 2022. [En línea]. Available: https://www.festo.com/es/es/e/tendencias/tia-portal-id_828990/.

[65] CADe Simu, «CADe Simu,» 2022. [En línea]. Available: https://cade-simu.com/.

[66] Telectronica, «Telectronica,» 2018. [En línea]. Available: https://www.telectronika.com/articulos/ti/que-es-gns3/.

[67] B. G. S. University, «BGSU,» 2016. [En línea]. Available: https://www.bgsu.edu/content/dam/BGSU/libraries/documents/collab-lab/Sketchup-Tutorial.pdf.

[68] F. I/O, «Factory I/O,» 2021. [En línea]. Available: https://docs.factoryio.com.

[69] A. d. León, «Hosting Diario,» [En línea]. Available: https://hostingdiario.com/tipos-de-servidores-web/. [Último acceso: 07 Octubre 2022].

[70] Video.js, «github,» [En línea]. Available: https://github.com/videojs/video.js.

[71] Compel, «Compel,» [En línea]. Available: https://www.compel.ru/pdf-items/delta/pn/dtb-4848-vr/538ea80c14d8054cd879e7287c575522. [Último acceso: 2022].

[72] A. G. Higuera, El control automatico en la industria, Cuenca: Ediciones de la Universidad de Castilla-La Mancha, 2005.

[73] Tecnoplc, «Tecnoplc,» 2022. [En línea]. Available: https://www.tecnoplc.com/tia-portal-utilidades-del-software/.

[74] IOT Security News, «IoT Security News,» 2021. [En línea]. Available: https://iotsecuritynews.com/delta-electronics-dopsoft-update-a/.

[75] ByteMind, «Byte Mind,» 26 Octubre 2017. [En línea]. Available: https://www.24x7servermanagement.com/installations/Install-LNMP-Stack.

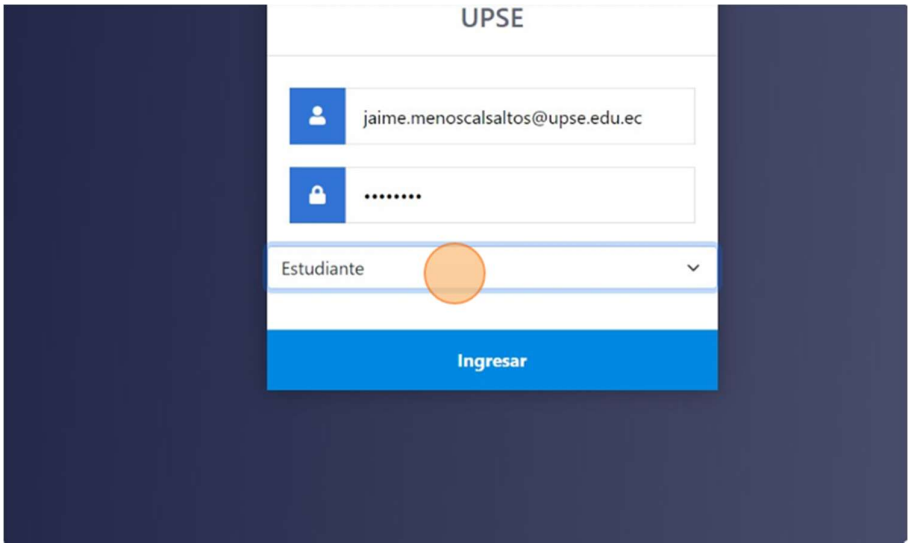
[76] MIkrotik, «MikroTik Documentation,» [En línea]. Available: https://wiki.mikrotik.com/wiki/Manual:Scripting. [Último acceso: 6 Noviembre 2022].

ANEXOS

ANEXO 1: AGENDAMIENTO DE TURNO EN APLICATIVO WEB

Una vez recibido por correo los datos para el "logueo" en el aplicativo web, se ingresa a https://www.labremaut.me

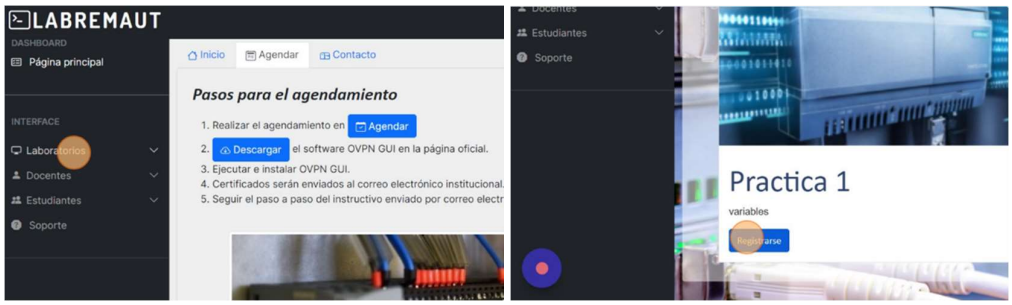
Se introduce el correo, contraseña y el tipo de usuario.



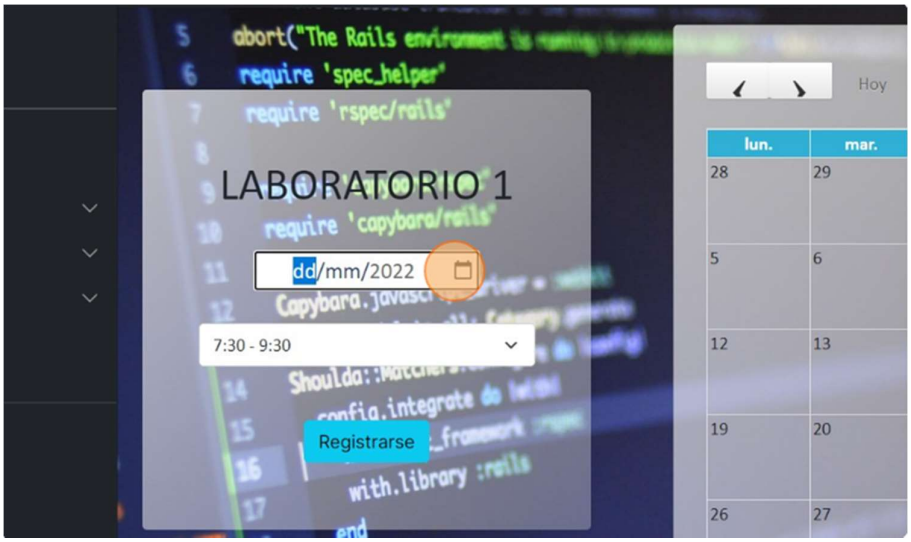
Una vez dentro de la página web, existen dos alternativas para entrar al apartado del agendamiento.

La primera es ir a la pestaña Agendar y seguir los pasos que se describen.

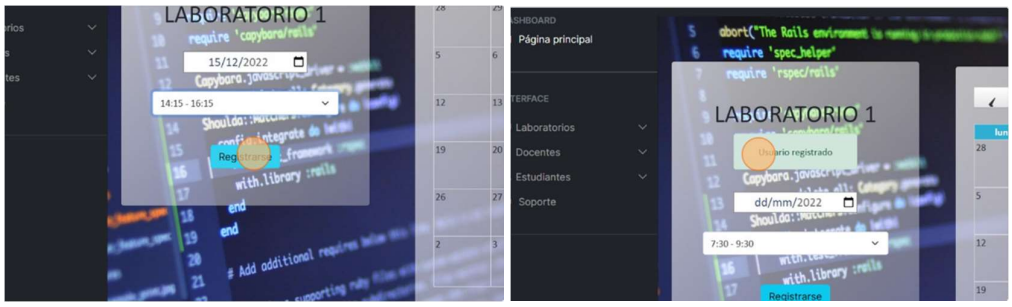
La segunda opción es ir al apartado de Laboratorios – Agendar, seguido de aquello se selecciona entre los 2 laboratorios disponibles por el momento.



Una vez seleccionada la Práctica o laboratorio, se selecciona el día del mes en curso, seguido del horario en el cual va a hacer uso del laboratorio.

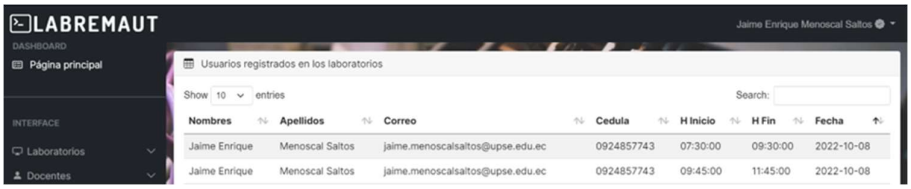


Y registrarse.



En la parte derecha se actualizará el calendario con el agendamiento respectivo, visualizando los horarios ocupados por día.

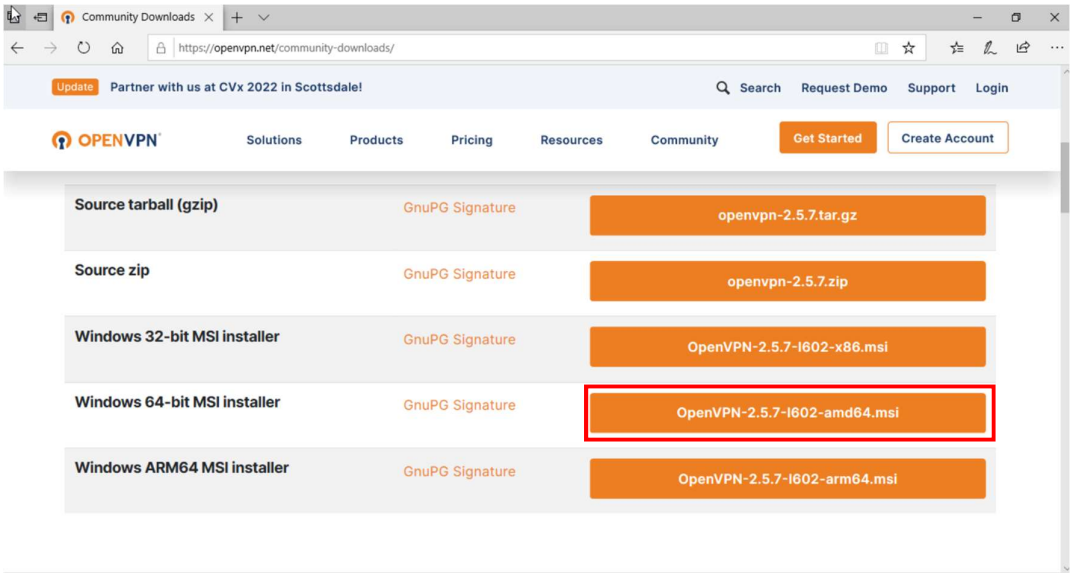
Si el usuario tiene los permisos necesarios, podrá visualizar los usuarios registrados con el horario que el mismo ocupará.



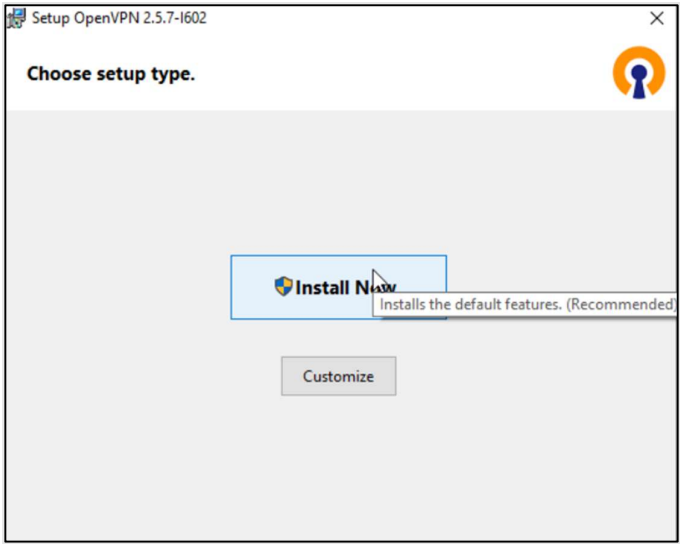
El estudiante podrá registrarse una vez por semana por cada laboratorio disponible, en el caso de registrarse en un horario ya ocupado, saldrá un error.

ANEXO 2: CONEXIÓN REMOTA DEL CLIENTE CON OpenVPN GUI

Cualquier cliente remoto que desee realizar prácticas de automatización, primero necesita tener instalado el software OpenVPN GUI, que puede ser descargado desde su página oficial, dependiendo de la versión de sistema operativo con que cuente, en caso de Windows si es de 32 o 64 bits. En la siguiente figura se muestra las versiones disponibles a la fecha de edición del presente documento, y en el presente ejemplo se procederá con la descarga de la versión de 64 bits para Windows.



Una vez descargado el instalador, se procede a ejecutar y seleccionar “Instalar Ahora”, se debe dar permiso de administrador en caso de solicitarlo, y finalizar el instalador cuando la instalación haya concluido.

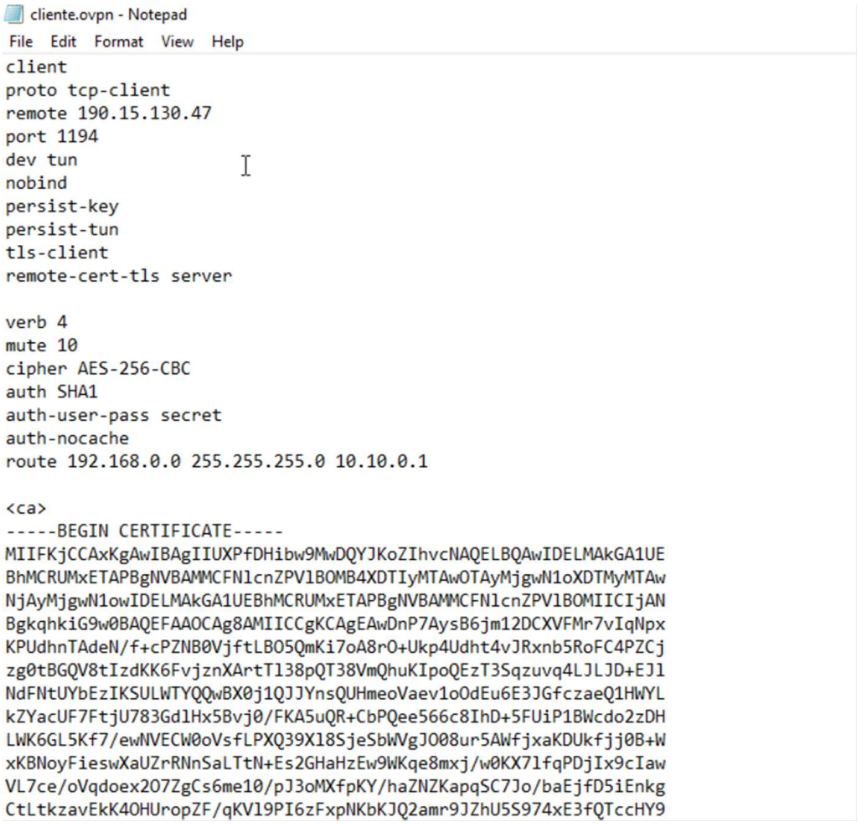


El software OpenVPN requiere de un archivo en específico donde se incluya las llaves y certificados cifrados además de los demás parámetros de configuración que concuerden con las configuraciones realizadas previamente en el servidor VPN. Este archivo se facilitará previamente a cada estudiante y docente para su conexión, y en él se incluyen las instrucciones que se muestran a continuación.

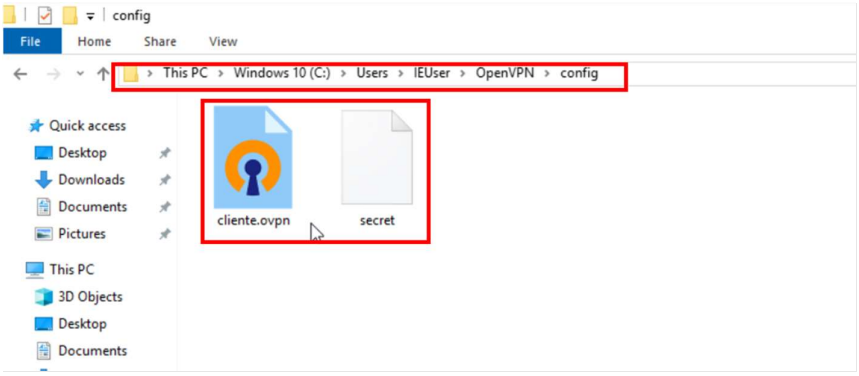
```
client
proto tcp-client
remote 190.15.130.47
port 1194
dev tun
nobind
persist-key
persist-tun
tls-client
remote-cert-tls server

verb 4
mute 10
cipher AES-256-CBC
auth SHA1
auth-user-pass secret
auth-nocache
route 192.168.0.0 255.255.255.0 10.0.0.1

CA.crt
cert cliente-OpenVPN.crt
key cliente-OpenVPN.key
```

En la configuración anterior se presentan todos los parámetros para que la conexión sea válida, y a su vez se indica que los certificados y la llave se encuentran en otros archivos externos, para nuestra implementación incluiremos dichos certificados dentro del mismo archivo con extensión ".OpenVPN" y solo requerir de un único archivo externo, que sería donde se coloca las credenciales usadas en la sección "Secret" al momento de crear el usuario, dicho archivo no deberá tener extensión alguna.

El archivo ".OpenVPN" para nuestro ejemplo será el que se muestra en la siguiente figura.

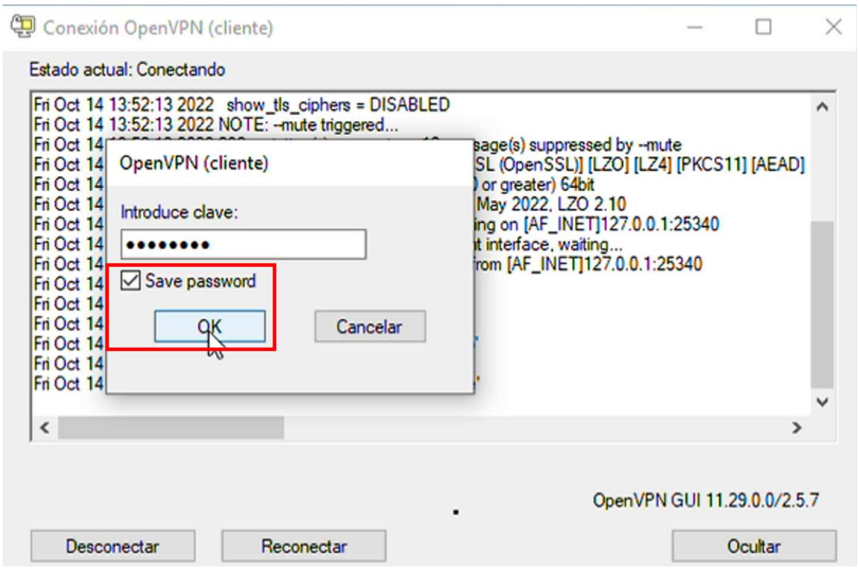


Una vez que se encuentren listos los archivos de configuración, se procede a copiarlos en la carpeta de OpenVPN en el siguiente directorio: "C:\Users\'nombre_usuario'\OpenVPN\config\" (nombre_usuario se refiere al nombre de usuario con que cuenta su sesión activa), tal como se muestra en la figura siguiente.

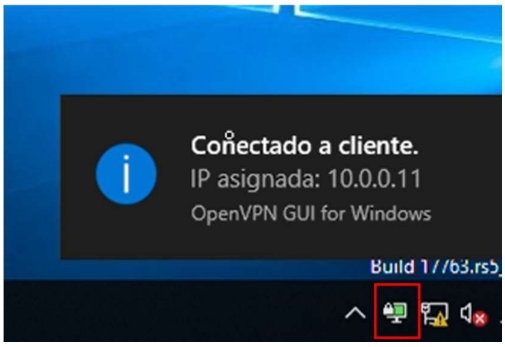


Para activar la conexión con la VPN se debe de dar clic derecho al icono de OpenVPN en la barra de notificaciones y seleccionar "Conectar".

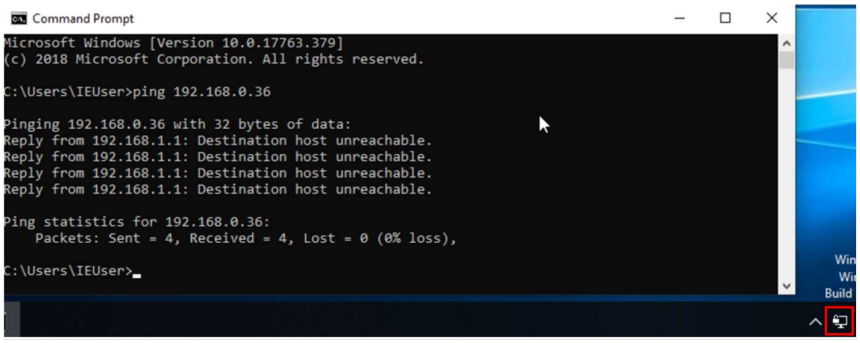
Cuando se ejecute la primera vez la conexión, el software va a solicitar el ingreso de la frase de paso que se usó al momento de exportar el certificado del cliente, y se debe de marcar la opción de "Almacenar contraseña" para que no nos solicite la frase cada vez que se requiera la conexión con la VPN.

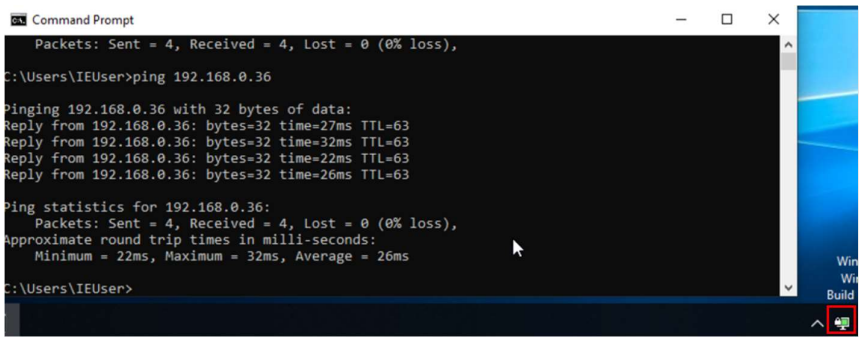


Cuando se concluya el proceso de autenticación con el servidor VPN, deberá aparecer el incono del cliente OpenVPN en color verde, y si está usando Windows 8 o superior, deberá aparecer una notificación con la dirección IP virtual asignada al cliente.



Ahora para demostrar que la VPN está funcionando de manera correcta, se procederá a realizar una prueba con el protocolo ICMP desde el cliente remoto hacia una IP privada dentro de la red de laboratorio, primero con la VPN sin conexión y luego habilitando la conexión VPN, los resultados serán ilustrados en las siguientes figuras.





La Figura superior indica que el host de destino es desconocido o no se conoce la ruta para llegar hasta el, por el contrario, una vez que se conecta la VPN, en la Figura inferior se obtienen los tiempos en que se tarda en llegar la respuesta desde el host del laboratorio hasta el host del cliente.

Todo lo anterior indica que el servicio OpenVPN se encuentra operativo y funcionando de manera correcta.

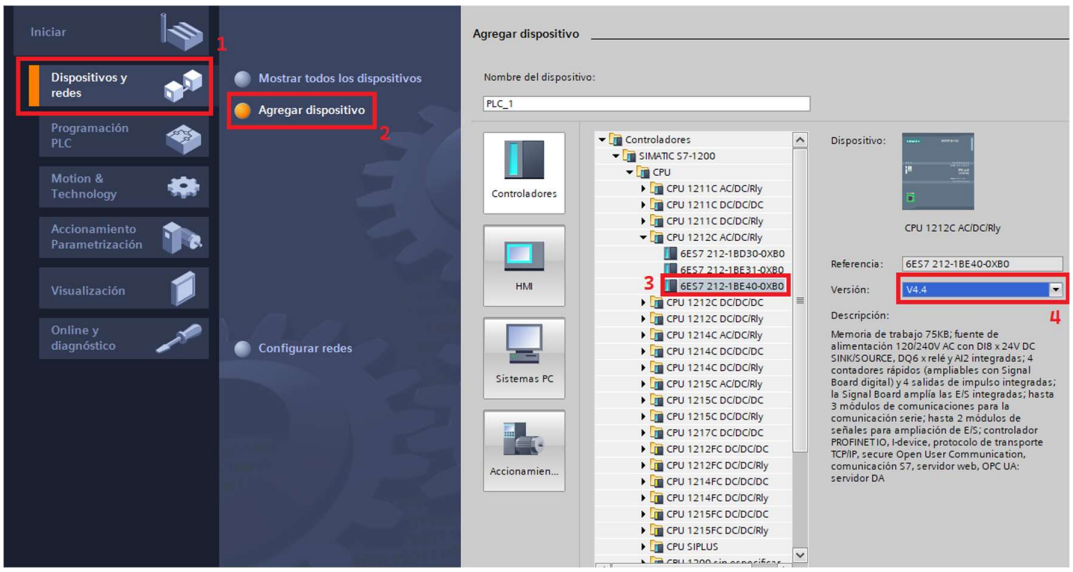
ANEXO 3: INSTRUCTIVO DE TIA PORTAL

Crear un nuevo proyecto

Se debe de ingresar a la aplicación TIA Portal v16 y luego crear un nuevo proyecto definiendo la ruta donde se irán almacenando los archivos.

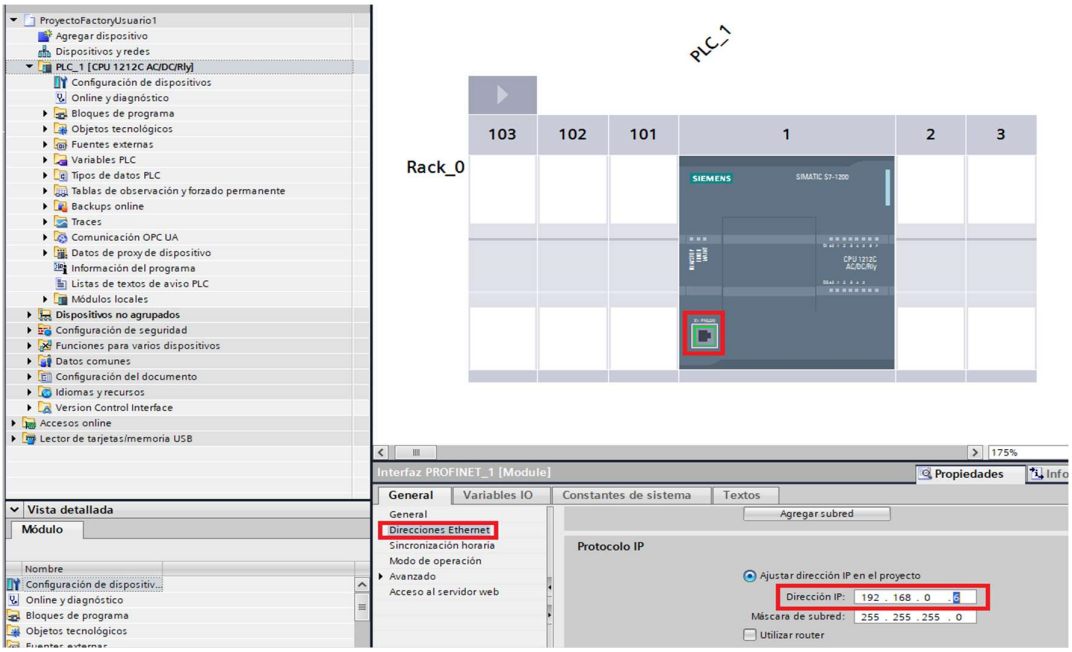
Selección del dispositivo

Para seleccionar el dispositivo físico con el que contamos, primero seleccionamos la pestaña de “Dispositivos y redes”, luego damos clic en “Agregar dispositivos” y dentro de los controladores elegimos el modelo respectivo del PLC a utilizar y la versión de firmware con el que cuenta.

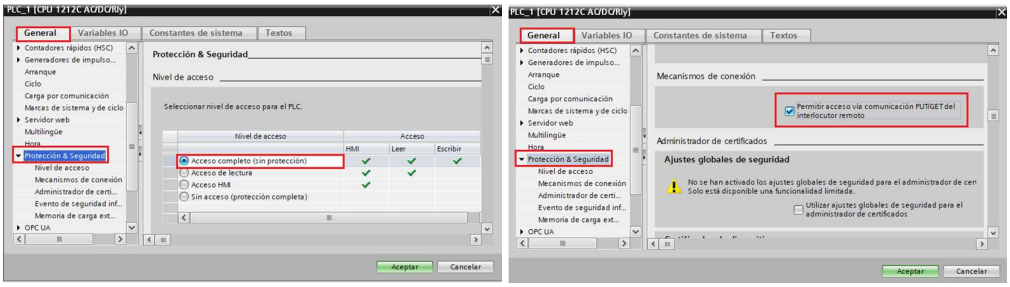


Direccionamiento IP y habilitación de PUT/GET

Una vez elegido el dispositivo se debe de asignar una dirección IP que sea única dentro de la red del laboratorio, para ellos cada PLC cuenta con una dirección IP previamente asignada por el docente, ahora, para configurarla, desde la Vista de proyecto se da doble clic izquierdo sobre la interfaz ethernet del PLC y en la sección de “Direcciones Ethernet” colocamos la dirección correspondiente al PLC a utilizar.



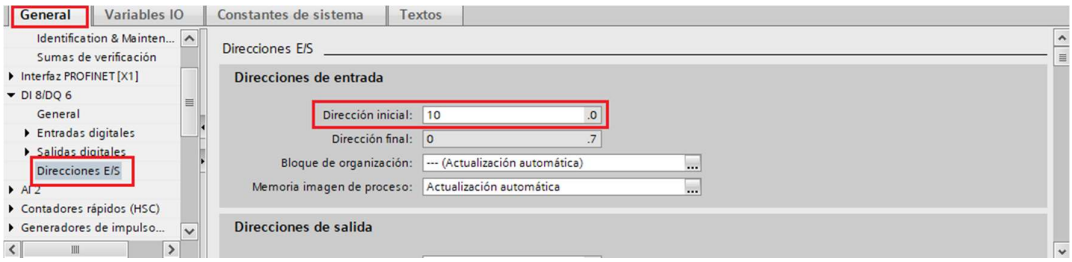
Ahora solo falta un paso antes de empezar con la programación del PLC, esta servirá para establecer la conexión con el software Factory IO. En el "Árbol del proyecto" se selecciona con clic derecho el dispositivo y en el menú emergente elegimos "Propiedades", esto abrirá una ventana de configuración en donde se debe seleccionar la sección de "Protección y seguridad" dentro de la pestaña "General", aquí debemos de verificar que este seleccionado el nivel de acceso como "Acceso completo" y que está marcada la opción "Permitir acceso vía comunicación PUT/GET del interlocutor remoto", caso contrario seleccionar las opciones requeridas.



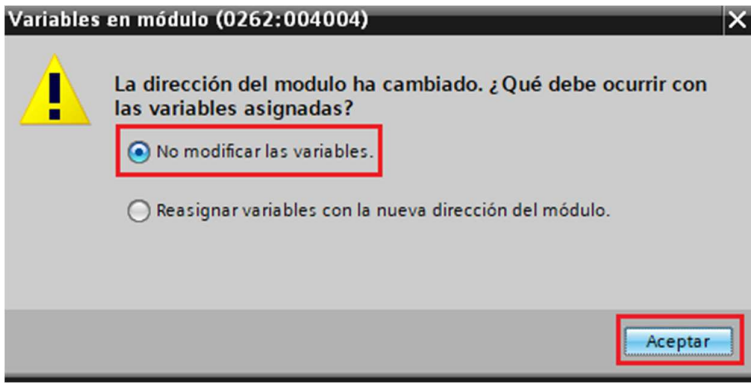
Cambio de las direcciones E/S

Para no tener problemas de sobreescritura al momento de intercambiar valores de las variables entre el PLC y Factory IO debemos de cambiar la dirección inicial de entrada, esto lo hacemos desde la configuración general del PLC en la sección de "Direcciones

E/S”, cambiando el valor inicial por uno superior que se encuentre a una distancia a la que pensemos no llegar a utilizar dentro del proyecto.



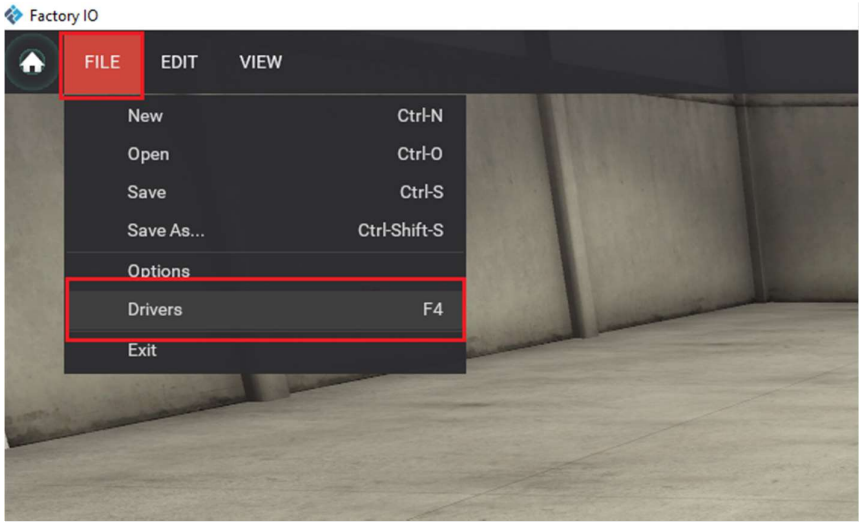
En caso de que previamente hayamos realizado algún tipo de programación dentro del proyecto, o en caso de existir variables creadas al momento de realizar el cambio, aparecerá un anuncio en el cual se debe elegir la opción de “No modificar las variables” y se procede a aceptar.



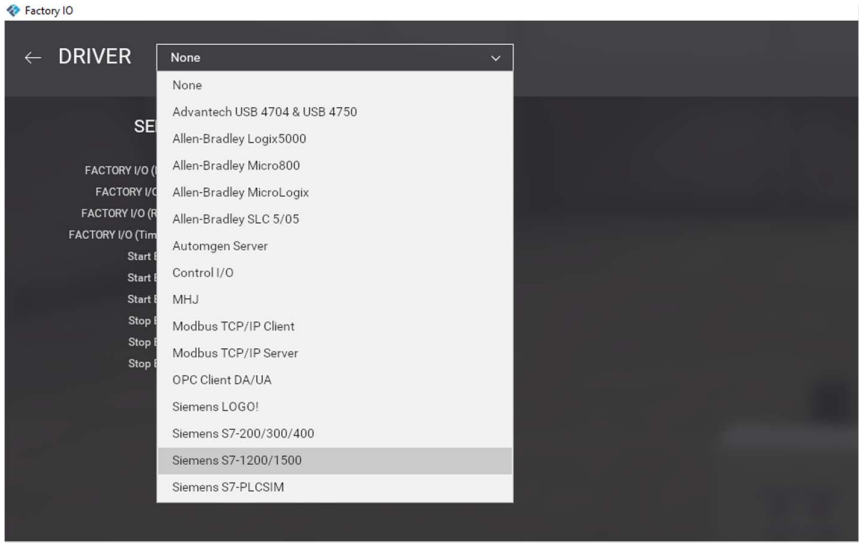
Con todos estos pasos previos, la conexión del Factory IO con el PLC no presentara ningún problema, y a su vez tampoco se generarán errores de sobreescrituras de las variables lógicas del PLC con sus entradas físicas.

ANEXO 4: CONEXIÓN DE FACTORY IO CON PLC

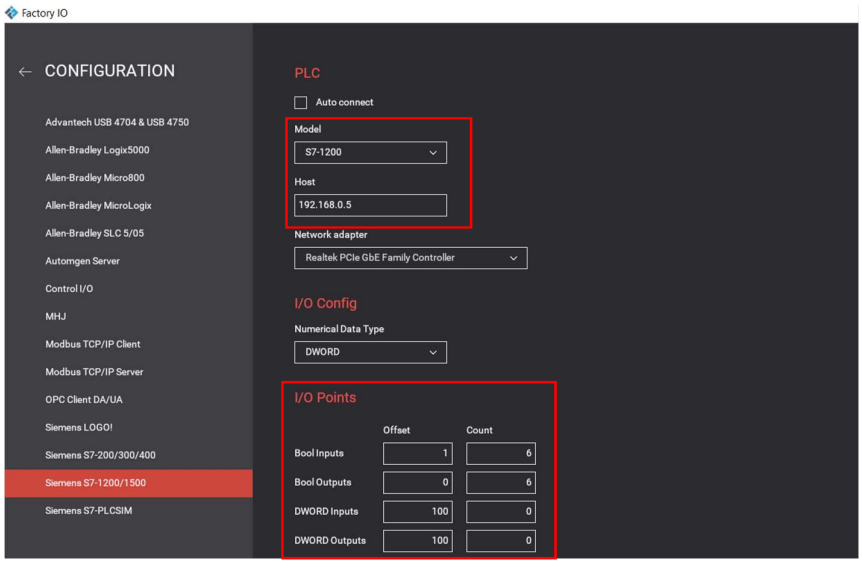
Para realizar la conexión desde Factory IO, seleccionamos el botón “FILE” y posteriormente dar clic en “Drivers”, también se puede acceder presionando directamente la tecla F4.



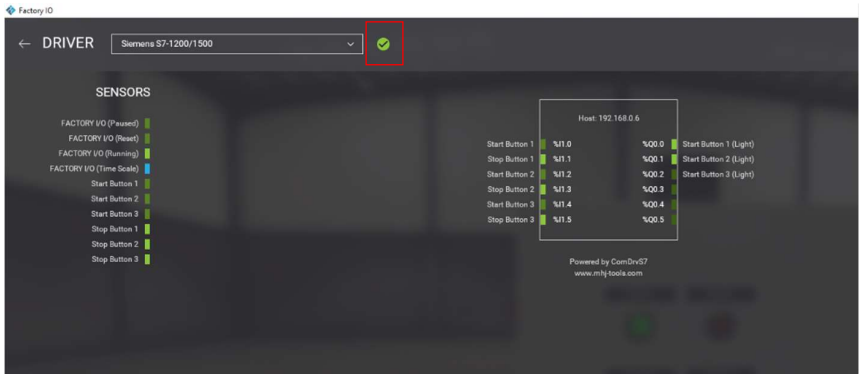
Una vez en la ventana de “Drivers” se procede a seleccionar el tipo de PLC a utilizar, en nuestro caso se debe de elegir el controlador “Siemens S7-1200/1500”, para luego poder configurarlo.



Una vez seleccionado el controlador se debe de configurar, eligiendo la cantidad de entradas y salidas requeridas para desarrollar el ejercicio, además de la dirección IP del PLC, enfatizando que esto es requerido para establecer la conexión.



Finalmente establecemos la conexión con la opción “CONNECT” verificando que aparezca un visto color verde alado del controlador indicando que conexión se dio correctamente.



ANEXO 5: HOJA DE DATOS PLC SIEMENS S7 1200

SIEMENS

Data sheet **6ES7212-1BE40-0XB0**

Figure similar

SIMATIC S7-1200, CPU 1212C, compact CPU, AC/DC/relay, onboard I/O: 8 DI 24 V DC; 6 DO relay 2 A; 2 AI 0-10 V DC, Power supply: AC 85-264 V AC at 47-63 Hz, Program/data memory 75 KB

General information	
Product type designation	CPU 1212C AC/DC/relay
Firmware version	V4.5
Engineering with	
• Programming package	STEP 7 V17 or higher
Supply voltage	
Rated value (AC)	
• 120 V AC	Yes
• 230 V AC	Yes
permissible range, lower limit (AC)	85 V
permissible range, upper limit (AC)	264 V
Line frequency	
• permissible range, lower limit	47 Hz
• permissible range, upper limit	63 Hz
Input current	
Current consumption (rated value)	80 mA at 120 V AC; 40 mA at 240 V AC
Current consumption, max.	240 mA at 120 V AC; 120 mA at 240 V AC
Inrush current, max.	20 A; at 264 V
I^2t	0.8 $A^2 \cdot s$
Output current	
for backplane bus (5 V DC), max.	1 000 mA; Max. 5 V DC for SM and CM
Encoder supply	
24 V encoder supply	
• 24 V	20.4 to 28.8V
Power loss	
Power loss, typ.	11 W
Memory	
Work memory	
• integrated	75 kbyte
• expandable	No
Load memory	
• integrated	2 Mbyte
• Plug-in (SIMATIC Memory Card), max.	with SIMATIC memory card
Backup	
• present	Yes
• maintenance-free	Yes
• without battery	Yes

CPU processing times	
for bit operations, typ.	0.08 µs; / instruction
for word operations, typ.	1.7 µs; / instruction
for floating point arithmetic, typ.	2.3 µs; / instruction
CPU-blocks	
Number of blocks (total)	DBs, FCs, FBs, counters and timers. The maximum number of addressable blocks ranges from 1 to 65535. There is no restriction, the entire working memory can be used
OB	
• Number, max.	Limited only by RAM for code
Data areas and their retentivity	
Retentive data area (incl. timers, counters, flags), max.	14 kbyte
Flag	
• Size, max.	4 kbyte; Size of bit memory address area
Local data	
• per priority class, max.	16 kbyte; Priority class 1 (program cycle): 16 KB, priority class 2 to 26: 6 KB
Address area	
Process image	
• Inputs, adjustable	1 kbyte
• Outputs, adjustable	1 kbyte
Hardware configuration	
Number of modules per system, max.	3 comm. modules, 1 signal board, 2 signal modules
Time of day	
Clock	
• Hardware clock (real-time)	Yes
• Backup time	480 h; Typical
• Deviation per day, max.	±60 s/month at 25 °C
Digital inputs	
Number of digital inputs	8; Integrated
• of which inputs usable for technological functions	6; HSC (High Speed Counting)
Source/sink input	Yes
Number of simultaneously controllable inputs	
all mounting positions	
— up to 40 °C, max.	8
Input voltage	
• Rated value (DC)	24 V
• for signal "0"	5 V DC at 1 mA
• for signal "1"	15 V DC at 2.5 mA
Input delay (for rated value of input voltage)	
for standard inputs	
— parameterizable	0.2 ms, 0.4 ms, 0.8 ms, 1.6 ms, 3.2 ms, 6.4 ms and 12.8 ms, selectable in groups of four
— at "0" to "1", min.	0.2 ms
— at "0" to "1", max.	12.8 ms
for interrupt inputs	
— parameterizable	Yes
for technological functions	
— parameterizable	Single phase: 3 @ 100 kHz & 3 @ 30 kHz, differential: 3 @ 80 kHz & 3 @ 30 kHz
Cable length	
• shielded, max.	500 m; 50 m for technological functions
• unshielded, max.	300 m; for technological functions: No
Digital outputs	
Number of digital outputs	6; Relays
Switching capacity of the outputs	
• with resistive load, max.	2 A
• on lamp load, max.	30 W with DC, 200 W with AC
Output delay with resistive load	
• "0" to "1", max.	10 ms; max.

● "1" to "0", max.	10 ms; max.
Relay outputs	
● Number of relay outputs	6
● Number of operating cycles, max.	mechanically 10 million, at rated load voltage 100 000
Cable length	
● shielded, max.	500 m
● unshielded, max.	150 m
Analog inputs	
Number of analog inputs	2
Input ranges	
● Voltage	Yes
Input ranges (rated values), voltages	
● 0 to +10 V	Yes
— Input resistance (0 to 10 V)	≥100k ohms
Cable length	
● shielded, max.	100 m; twisted and shielded
Analog outputs	
Number of analog outputs	0
Analog value generation for the inputs	
Integration and conversion time/resolution per channel	
● Resolution with overrange (bit including sign), max.	10 bit
● Integration time, parameterizable	Yes
● Conversion time (per channel)	625 µs
Encoder	
Connectable encoders	
● 2-wire sensor	Yes
1. Interface	
Interface type	PROFINET
Isolated	Yes
automatic detection of transmission rate	Yes
Autonegotiation	Yes
Autocrossing	Yes
Interface types	
● RJ 45 (Ethernet)	Yes
● Number of ports	1
● integrated switch	No
Protocols	
● PROFINET IO Controller	Yes
● PROFINET IO Device	Yes
● SIMATIC communication	Yes
● Open IE communication	Yes; Optionally also encrypted
● Web server	Yes
● Media redundancy	No
PROFINET IO Controller	
● Transmission rate, max.	100 Mbit/s
Services	
— PG/OP communication	Yes; encryption with TLS V1.3 pre-selected
— Isochronous mode	No
— IRT	No
— PROFIenergy	No
— Prioritized startup	Yes
— Number of IO devices with prioritized startup, max.	16
— Number of connectable IO Devices, max.	16
— Number of connectable IO Devices for RT, max.	16
— of which in line, max.	16
— Activation/deactivation of IO Devices	Yes
— Number of IO Devices that can be simultaneously activated/deactivated, max.	8

— Updating time	The minimum value of the update time also depends on the communication component set for PROFINET IO, on the number of IO devices and the quantity of configured user data.
PROFINET IO Device	
Services	
— PG/OP communication	Yes; encryption with TLS V1.3 pre-selected
— Isochronous mode	No
— IRT	No
— PROFIenergy	Yes
— Shared device	Yes
— Number of IO Controllers with shared device, max.	2
Protocols	
Supports protocol for PROFINET IO	Yes
PROFIsafe	No
PROFIBUS	Yes; CM 1243-5 (master) or CM 1242-5 (slave) required
OPC UA	Yes; OPC UA Server
AS-Interface	Yes; CM 1243-2 required
Protocols (Ethernet)	
• TCP/IP	Yes
• DHCP	No
• SNMP	Yes
• DCP	Yes
• LLDP	Yes
Redundancy mode	
Media redundancy	
— MRP	No
— MRPD	No
SIMATIC communication	
• S7 routing	Yes
Open IE communication	
• TCP/IP	Yes
— Data length, max.	8 kbyte
• ISO-on-TCP (RFC1006)	Yes
— Data length, max.	8 kbyte
• UDP	Yes
— Data length, max.	1 472 byte
Web server	
• supported	Yes
• User-defined websites	Yes
OPC UA	
• Runtime license required	Yes; "Basic" license required
• OPC UA Server	Yes; data access (read, write, subscribe), method call, runtime license required
— Application authentication	Available security policies: None, Basic128Rsa15, Basic256Rsa15, Basic256Sha256
— User authentication	"anonymous" or by user name & password
— Number of sessions, max.	10
— Number of subscriptions per session, max.	50
— Sampling interval, min.	100 ms
— Publishing interval, min.	200 ms
— Number of server methods, max.	20
— Number of monitored items, max.	1 000
— Number of server interfaces, max.	2
— Number of nodes for user-defined server interfaces, max.	2 000
Further protocols	
• MODBUS	Yes
communication functions / header	
S7 communication	
• supported	Yes

● as server	Yes
● as client	Yes
● User data per job, max.	See online help (S7 communication, user data size)
Number of connections	
● overall	PG Connections: 4 reserved / 4 max; HMI Connections: 12 reserved / 18 max; S7 Connections: 8 reserved / 14 max; Open User Connections: 8 reserved / 14 max; Web Connections: 2 reserved / 30 max; OPC UA Connections: 0 reserved / 10 max; Total Connections: 34 reserved / 64 max
Test commissioning functions	
Status/control	
● Status/control variable	Yes
● Variables	Inputs/outputs, memory bits, DBs, distributed I/Os, timers, counters
Forcing	
● Forcing	Yes
Diagnostic buffer	
● present	Yes
Traces	
● Number of configurable Traces	2
● Memory size per trace, max.	512 kbyte
Interrupts/diagnostics/status information	
Diagnostics indication LED	
● RUN/STOP LED	Yes
● ERROR LED	Yes
● MAINT LED	Yes
Integrated Functions	
Counter	
● Number of counters	6
● Counting frequency, max.	100 kHz
Frequency measurement	Yes
controlled positioning	Yes
Number of position-controlled positioning axes, max.	8
Number of positioning axes via pulse-direction interface	Up to 4 with SB 1222
PID controller	Yes
Number of alarm inputs	4
Potential separation	
Potential separation digital inputs	
● Potential separation digital inputs	500V AC for 1 minute
● between the channels, in groups of	1
Potential separation digital outputs	
● Potential separation digital outputs	Relays
● between the channels	No
● between the channels, in groups of	2
EMC	
Interference immunity against discharge of static electricity	
● Interference immunity against discharge of static electricity acc. to IEC 61000-4-2	Yes
— Test voltage at air discharge	8 kV
— Test voltage at contact discharge	6 kV
Interference immunity to cable-borne interference	
● Interference immunity on supply lines acc. to IEC 61000-4-4	Yes
● Interference immunity on signal cables acc. to IEC 61000-4-4	Yes
Interference immunity against voltage surge	
● Interference immunity on supply lines acc. to IEC 61000-4-5	Yes
Interference immunity against conducted variable disturbance induced by high-frequency fields	
● Interference immunity against high-frequency radiation acc. to IEC 61000-4-6	Yes
Emission of radio interference acc. to EN 55 011	
● Limit class A, for use in industrial areas	Yes; Group 1

● Limit class B, for use in residential areas	Yes; When appropriate measures are used to ensure compliance with the limits for Class B according to EN 55011
Degree and class of protection	
IP degree of protection	IP20
Standards, approvals, certificates	
CE mark	Yes
UL approval	Yes
cULus	Yes
FM approval	Yes
RCM (formerly C-TICK)	Yes
KC approval	Yes
Marine approval	Yes
Ambient conditions	
Free fall	
● Fall height, max.	0.3 m; five times, in product package
Ambient temperature during operation	
● min.	-20 °C
● max.	60 °C; Number of simultaneously activated inputs or outputs 4 or 3 (no adjacent points) at 60 °C horizontal or 50 °C vertical, 8 or 6 at 55 °C horizontal or 45 °C vertical
● horizontal installation, min.	-20 °C
● horizontal installation, max.	60 °C
● vertical installation, min.	-20 °C
● vertical installation, max.	50 °C
Ambient temperature during storage/transportation	
● min.	-40 °C
● max.	70 °C
Air pressure acc. to IEC 60068-2-13	
● Operation, min.	795 hPa
● Operation, max.	1 080 hPa
● Storage/transport, min.	660 hPa
● Storage/transport, max.	1 080 hPa
Altitude during operation relating to sea level	
● Installation altitude, min.	-1 000 m
● Installation altitude, max.	5 000 m; Restrictions for installation altitudes > 2 000 m, see manual
Relative humidity	
● Operation, max.	95 %; no condensation
Vibrations	
● Vibration resistance during operation acc. to IEC 60068-2-6	2 g (m/s²) wall mounting, 1 g (m/s²) DIN rail
● Operation, tested according to IEC 60068-2-6	Yes
Shock testing	
● tested according to IEC 60068-2-27	Yes; IEC 68, Part 2-27 half-sine: strength of the shock 15 g (peak value), duration 11 ms
Pollutant concentrations	
● SO2 at RH < 60% without condensation	S02: < 0.5 ppm; H2S: < 0.1 ppm; RH < 60% condensation-free
configuration / header	
configuration / programming / header	
Programming language	
— LAD	Yes
— FBD	Yes
— SCL	Yes
Know-how protection	
● User program protection/password protection	Yes
● Copy protection	Yes
● Block protection	Yes
Access protection	
● protection of confidential configuration data	Yes
● Protection level: Write protection	Yes
● Protection level: Read/write protection	Yes
● Protection level: Complete protection	Yes

programming / cycle time monitoring / header	
● cycle monitoring time / adjustable	Yes
Dimensions	
Width	90 mm
Height	100 mm
Depth	75 mm
Weights	
Weight, approx.	425 g

last modified: 4/1/2022

ANEXO 6: HOJA DE DATOS MÓDULO SM 1222

SIEMENS

Hoja de datos **6ES7222-1BF32-0XB0**

SIMATIC S7-1200, módulo de salidas digitales SM 1222, 8 DO, DC 24V, Transistor 0,5 A

Información general	
Designación del tipo de producto	SM 1222, DQ 8x24 VDC/0,5 A
Tensión de alimentación	
Rango admisible, límite inferior (DC)	20,4 V
Rango admisible, límite superior (DC)	28,8 V
Intensidad de entrada	
de bus de fondo 5 V DC, máx.	120 mA
Pérdidas	
Pérdidas, típ.	1,5 W
Salidas digitales	
Número de salidas	8
● En grupos de	1
Protección contra cortocircuito	No; a prever externamente
Limitación de la sobretensión inductiva de corte a	típ. (L+) -48 V
Poder de corte de las salidas	
● con carga resistiva, máx.	0,5 A
● con carga tipo lámpara, máx.	5 W
Tensión de salida	
● Valor nominal (DC)	24 V
● para señal "0", máx.	0,1 V; con carga de 10 kOhm
● para señal "1", mín.	20 V DC
Intensidad de salida	
● para señal "1" valor nominal	0,5 A
● para señal "0" intensidad residual, máx.	10 µA
Retardo a la salida con carga resistiva	
● "0" a "1", máx.	50 µs
● "1" a "0", máx.	200 µs
Corriente total de salidas (por grupo)	
Posición de montaje horizontal	
— hasta 50 °C, máx.	4 A; Corriente por común
Salidas de relé	
Poder de corte de los contactos	
— con carga inductiva, máx.	0,5 A
— con carga tipo lámpara, máx.	5 W
— con carga resistiva, máx.	0,5 A
Longitud del cable	
● apantallado, máx.	500 m
● no apantallado, máx.	150 m
Alarmas/diagnósticos/información de estado	

Alarmas	
● Alarma de diagnóstico	Sí
LED señalizador de diagnóstico	
● para el estado de las salidas	Sí
Aislamiento galvánico	
Aislamiento galvánico módulos de S digitales	
● entre los canales, en grupos de	1
● entre los canales y bus de fondo	500 V AC
Grado de protección y clase de protección	
Grado de protección IP	IP20
Normas, homologaciones, certificados	
Marcado CE	Sí
Homologación CSA	Sí
Homologación UL	Sí
cULus	Sí
Homologación FM	Sí
RCM (anteriormente C-TICK)	Sí
Homologación KC	Sí
Homologaciones navales	Sí
Condiciones ambientales	
Caída libre	
● Altura de caída, máx.	0,3 m; Cinco veces, en embalaje de envío
Temperatura ambiente en servicio	
● mín.	-20 °C
● máx.	60 °C
● Posición de montaje horizontal, mín.	-20 °C
● Posición de montaje horizontal, máx.	60 °C
● Posición de montaje vertical, mín.	-20 °C
● Posición de montaje vertical, máx.	50 °C
● Cambio permitido de temperatura	5°C a 55°C, 3°C/minuto
Temperatura ambiente en almacenaje/transporte	
● mín.	-40 °C
● máx.	70 °C
Presión atmosférica según IEC 60068-2-13	
● Almacenamiento/transporte, mín.	660 hPa
● Almacenamiento/transporte, máx.	1 080 hPa
Humedad relativa del aire	
● Funcionamiento a 25 °C sin condensación, máx.	95 %
sistema de conexión / título	
Conector frontal requerido	Sí
Elementos mecánicos/material	
Material de la caja (en el frente)	
● Plástico	Sí
Dimensiones	
Ancho	45 mm
Altura	100 mm
Profundidad	75 mm
Pesos	
Peso, aprox.	180 g

Última modificación: 26/2/2021

ANEXO 7: HOJA DE DATOS MÓDULO CM 1241 RS 422/485

SIEMENS

Hoja de datos **6ES7241-1CH32-0XB0**

Figura similar

SIMATIC S7-1200, Módulo de comunicación CM 1241, RS422/485, Sub-D, 9 polos (conector hembra) Soporta Freeport

Información general	
Designación del tipo de producto	CM 1241 RS 422 / 485
Tensión de alimentación	
Valor nominal (DC)	24 V
Rango admisible, límite inferior (DC)	20,4 V
Rango admisible, límite superior (DC)	28,8 V
Intensidad de entrada	
Consumo, máx.	220 mA; De bus de fondo 5 V DC
Pérdidas	
Pérdidas, típ.	1,1 W
Interfaces	
Interfaces/tipo de bus	RS 422 / 485 (X.27)
Nº de interfaces	1
Acoplamiento punto a punto	
• Longitud del cable, máx.	1 000 m
Drivers de protocolo integrados	
— Freeport	Sí
— ASCII	Sí; disponible como función de librería
— RTU maestro Modbus	Sí
— RTU esclavos Modbus	Sí
— USS	Sí; disponible como función de librería
Protocolos	
Protocolos integrados	
Freeport	
— Longitud de telegrama, máx.	1 kbyte
— Bits por carácter	7 u 8
— Número de bits de parada	1 (estándar), 2
— Paridad	Sin paridad (estándar); par, impar, marca (bit de paridad siempre a 1); espacio (bit de paridad siempre a 0)
3964 (R)	
— Longitud de telegrama, máx.	1 kbyte
— Bits por carácter	7 u 8
— Número de bits de parada	1 (estándar), 2
— Paridad	Sin paridad (estándar); par, impar, marca (bit de paridad siempre a 1); espacio (bit de paridad siempre a 0)
RTU maestro Modbus	
— Área de direcciones	1 a 49 999 (direccionamiento estándar de Modbus)
— N.º de esclavos, máx.	247; 1 a 247, máximo 32 dispositivos por cada segmento de red MODBUS, se precisan repetidores adicionales para ampliar la red a la

	máxima configuración
RTU esclavos Modbus	
— Área de direcciones	1 a 49 999 (direccionamiento estándar de Modbus)
Alarmas/diagnósticos/información de estado	
Función de diagnóstico	Sí
LED señalizador de diagnóstico	
• para el estado de las salidas	Sí
Grado de protección y clase de protección	
Grado de protección IP	IP20
Normas, homologaciones, certificados	
Marcado CE	Sí
Homologación CSA	Sí
Homologación UL	Sí
cULus	Sí
Homologación FM	Sí
RCM (anteriormente C-TICK)	Sí
Homologación KC	Sí
Homologaciones navales	Sí
Condiciones ambientales	
Caída libre	
• Altura de caída, máx.	0,3 m; Cinco veces, en embalaje de envío
Temperatura ambiente en servicio	
• mín.	-20 °C
• máx.	60 °C
• Posición de montaje horizontal, mín.	-20 °C
• Posición de montaje horizontal, máx.	60 °C
• Posición de montaje vertical, mín.	-20 °C
• Posición de montaje vertical, máx.	50 °C
• Cambio permitido de temperatura	5°C a 55°C, 3°C/minuto
Temperatura ambiente en almacenaje/transporte	
• mín.	-40 °C
• máx.	70 °C
Presión atmosférica según IEC 60068-2-13	
• En servicio mín.	795 hPa
• En servicio máx.	1 080 hPa
• Almacenamiento/transporte, mín.	660 hPa
• Almacenamiento/transporte, máx.	1 080 hPa
Humedad relativa del aire	
• Funcionamiento a 25 °C sin condensación, máx.	95 %
Dimensiones	
Ancho	30 mm
Altura	100 mm
Profundidad	75 mm
Pesos	
Peso, aprox.	155 g

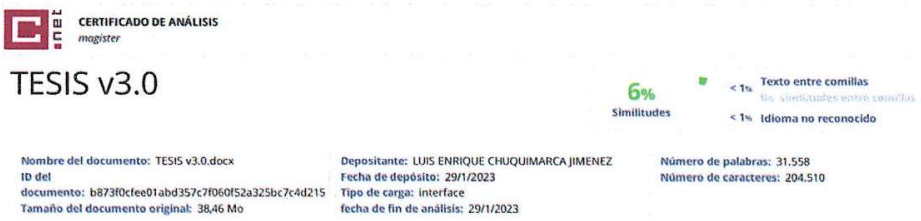
Última modificación: 26/2/2021

La Libertad, 30 de enero de 2023

Señor
Ing. José Sánchez Aquino Msc.
DIRECTOR DE CARRERA DE ELECTRÓNICA Y TELECOMUNICACIONES
En su despacho.-

De mi consideración:

Cumplo en informar el resultado obtenido en la revisión de plagio realizado por el software COMPILATIO, del trabajo de titulación, "IMPLEMENTACIÓN DE UN LABORATORIO REMOTO ORIENTADO AL DESARROLLO DE PRÁCTICAS DE AUTOMATIZACIÓN INDUSTRIAL PARA LA CARRERA ELECTRÓNICA Y AUTOMATIZACIÓN DE LA UPSE", elaborado por los señores estudiantes de la Carrera de Electrónica y Telecomunicaciones JAIME ENRIQUE MENOSCAL SALTOS y LUIS MIGUEL ARAUZ PINELA, el cual dio como resultado el 6% de similitudes.


CERTIFICADO DE ANÁLISIS
magister

TESIS v3.0

6% Similitudes

< 1% Texto entre comillas
No similitudes entre comillas
< 1% Idioma no reconocido

Nombre del documento: TESIS v3.0.docx
ID del documento: b873f0cfee01abd357c7f060f52a325bc7c4d215
Tamaño del documento original: 38,46 Mo

Depositante: LUIS ENRIQUE CHUQUIMARCA JIMENEZ
Fecha de depósito: 29/1/2023
Tipo de carga: interface
fecha de fin de análisis: 29/1/2023

Número de palabras: 31.558
Número de caracteres: 204.510

Atentamente,

Ing. Luis Enrique Chuquimarca Jimenez MSc.
TUTOR DE TRABAJO DE TITULACION