UNIVERSIDAD SANTO TOMÁS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA

FACULTAD INGENIERÍA ELECTRÓNICA

Laboratorio 5: Comunicaciones Industriales

Universidad Santo Tomas

Realizado por:
Ferney Arturo Amaya Gómez
David Esteban Diaz Castro
Jhonny Alejandro Mejia Leon

Presentado a:
ING Diego Alejandro Barragán Vargas

Noviembre 2025

1. RESUMEN

El presente informe detalla el desarrollo experimental de tres módulos fundamentales en la automatización industrial moderna: la infraestructura de red (IT), la comunicación de campo (OT) y el control lógico (PLC). Se logró implementar una arquitectura de red enrutada validando la segmentación de dominios de difusión mediante ARP. Posteriormente, se estableció una comunicación robusta Maestro-Esclavo utilizando el estándar Modbus RTU sobre RS485. Finalmente, se virtualizó un entorno de control utilizando Siemens TIA Portal, validando la lógica Ladder mediante simulación en tiempo real.

2. INTRODUCCIÓN

La industria 4.0 exige la convergencia entre las tecnologías de la información (IT) y las tecnologías de operación (OT). Para un ingeniero, no basta con programar un PLC; es necesario comprender cómo los datos de ese PLC viajan a través de buses de campo hacia pasarelas (Gateways) y cómo se enrutan a través de redes IP segmentadas. Este laboratorio tiene como propósito unificar estos conceptos mediante la práctica experimental, abordando desde la capa física (cableado RS485) y de enlace (ARP/Switching), hasta la capa de red (IP Routing) y de aplicación (Lógica de control y visualización).

3. MARCO TEÓRICO

3.1. Arquitectura de Red y Protocolo ARP

En redes Ethernet, la comunicación se basa en direcciones físicas (MAC). Sin embargo, el enrutamiento se basa en direcciones lógicas (IP). El protocolo **ARP (Address Resolution Protocol)** es el encargado de mapear una dirección IP conocida a una dirección MAC desconocida. Una característica crítica de ARP es que opera mediante difusión (Broadcast), por lo que sus solicitudes no pueden atravesar Routers. Esto define los límites de una red de área local (LAN).

3.2. Estándar RS485 y Modbus RTU

RS485 es un estándar de capa física que utiliza señalización diferencial (Líneas A y B) para transmitir datos. Esta técnica ofrece alta inmunidad al ruido electromagnético, permitiendo distancias de hasta 1200 metros. Sobre esta capa física se implementa **Modbus RTU**, un protocolo de capa de aplicación que define una estructura de trama (Dirección, Función, Datos, CRC) para el intercambio de información entre un Maestro y múltiples Esclavos.

3.3. Controladores Lógicos y Lenguaje Ladder

El PLC (Controlador Lógico Programable) es el cerebro de la automatización. El lenguaje **Ladder (KOP)**, estandarizado bajo la norma IEC 61131-3, representa la lógica de control mediante esquemas de contactos eléctricos, facilitando la transición de la lógica cableada a la programada.

4. DESARROLLO EXPERIMENTAL Y RESULTADOS

PUNTO 1: ANÁLISIS DE ARQUITECTURA DE RED Y ENRUTAMIENTO

4.1. Descripción del Montaje Se implementó una topología de red jerárquica para simular la interconexión entre dos plantas industriales separadas geográficamente. El montaje constó de los siguientes elementos:

- **Nivel de Acceso:** Switches de capa 2 encargados de la conmutación local.
- **Nivel de Core:** Un Router encargado del enrutamiento de paquetes entre subredes.
- **Hosts:** Equipos de cómputo (PC y Raspberry Pi) configurados como nodos finales.

En la siguiente figura se presenta el despliegue físico de los equipos utilizados para las pruebas de conectividad:

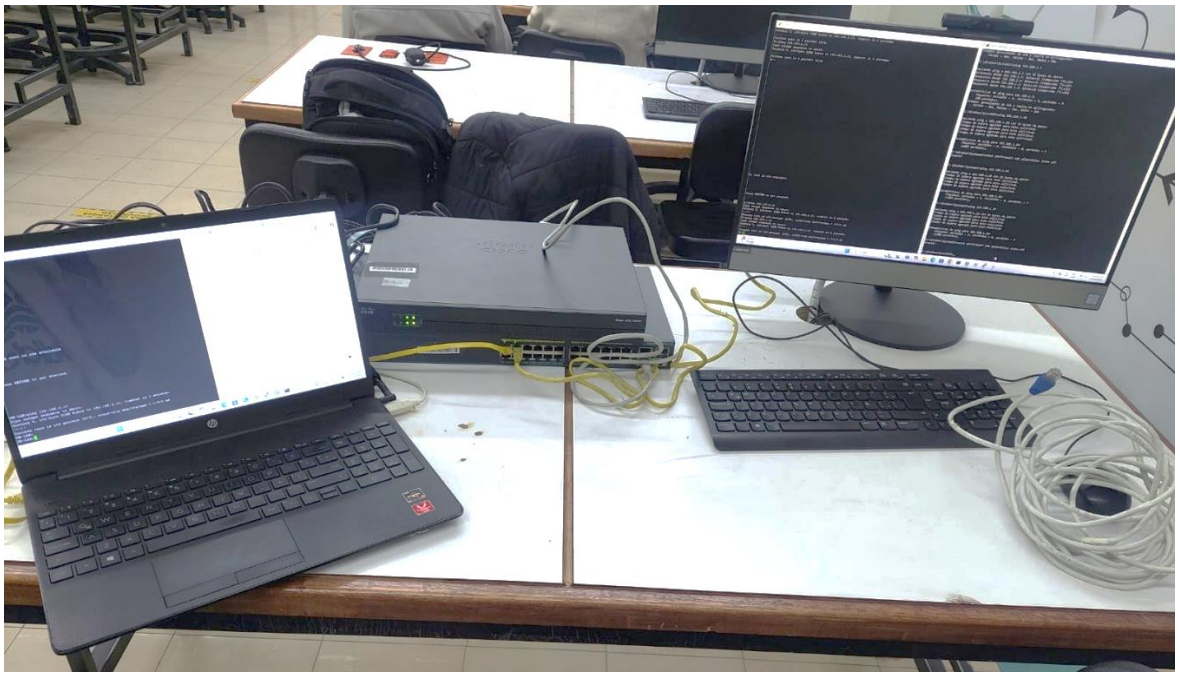


Figura 1. Montaje experimental de la infraestructura de red.

4.2. Configuración de Direccionamiento Se definieron dos segmentos de red clase C para validar el aislamiento de tráfico:

- **Red A (Izquierda):** `192.168.10.0 /24` – Gateway: `192.168.10.1`
- **Red B (Derecha):** `192.168.20.0 /24` – Gateway: `192.168.20.1`

4.3. Análisis de Resultados (ARP e IP) Se realizó una prueba de conectividad (Ping) desde un Host en la Red A hacia un Host en la Red B. La prueba fue exitosa, lo que confirma la correcta operación del Router.

Sin embargo, el hallazgo más relevante se obtuvo al inspeccionar la tabla ARP del equipo transmisor (`arp -a`).

- **Observación:** La tabla ARP **no contenía la dirección MAC del equipo receptor remoto**. En su lugar, la dirección IP remota se asociaba al tráfico saliente hacia la dirección MAC del Gateway local.
- **Análisis Técnico:** Esto demuestra experimentalmente que ARP es un protocolo de enlace local. En una red enrutada, los dispositivos finales no necesitan (ni pueden) conocer la dirección física de los dispositivos fuera de su subred; delegan la entrega del paquete al Router (Gateway). Esto optimiza el ancho de banda al contener las tormentas de broadcast dentro de cada segmento.

PUNTO 2: COMUNICACIÓN INDUSTRIAL RS485 (MODBUS RTU)

4.1. Configuración del Maestro (Raspberry Pi) Para habilitar la Raspberry Pi como un controlador industrial, fue necesario modificar la configuración del kernel de Linux. Se utilizó la herramienta `raspi-config` para desvincular la consola serial del puerto UART, permitiendo que este sea utilizado exclusivamente por la aplicación de usuario.

- **Librerías utilizadas:** Se emplearon `pyserial` para el manejo del puerto y `minimalmodbus` para la implementación de la capa de aplicación Modbus.

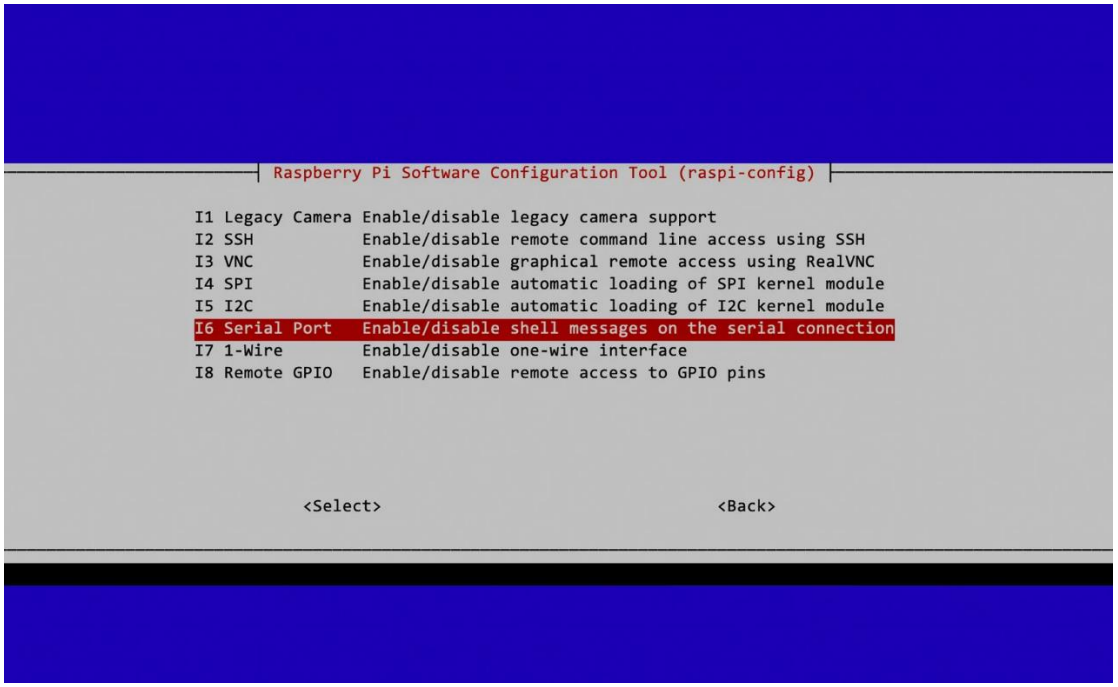


Figura 2. Configuración de interfaces en Raspberry Pi OS.

4.2. Implementación Física La conexión física se realizó mediante transceptores MAX485, los cuales convierten los niveles lógicos TTL (0-3.3V) del microcontrolador a niveles de voltaje diferencial (+/- 5V). Se respetó la topología de bus lineal, conectando las líneas A-A y B-B, y se verificó la polaridad para evitar errores de comunicación.

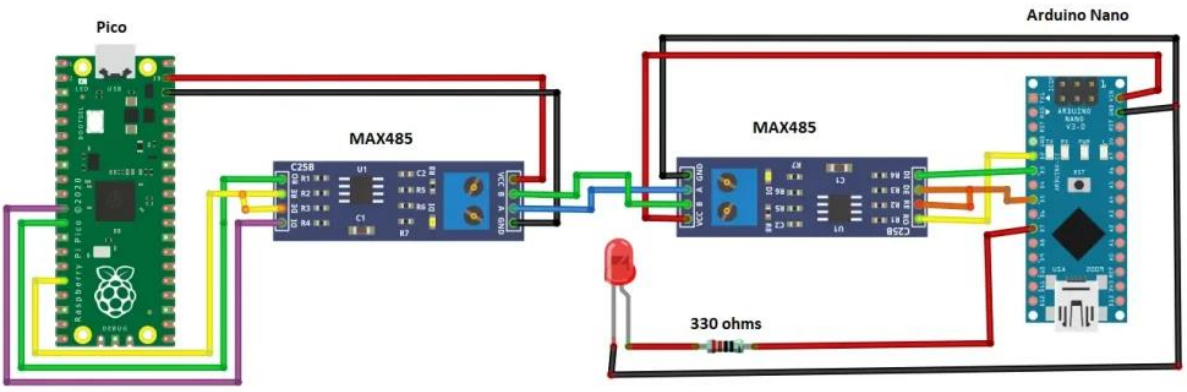


Figura 3. Diagrama esquemático de la conexión diferencial RS485.

4.3. Desarrollo de Software y Pruebas Se desarrolló un script en Python que implementa un Maestro Modbus RTU. El script se configuró con los siguientes parámetros de comunicación serial, típicos en la industria:

- **Baudrate:** 9600 bps
- **Bits de datos:** 8
- **Paridad:** Ninguna
- **Bits de parada:** 1

El código realiza una petición cíclica (Polling) al registro de memoria `0` del Esclavo (dirección 1).

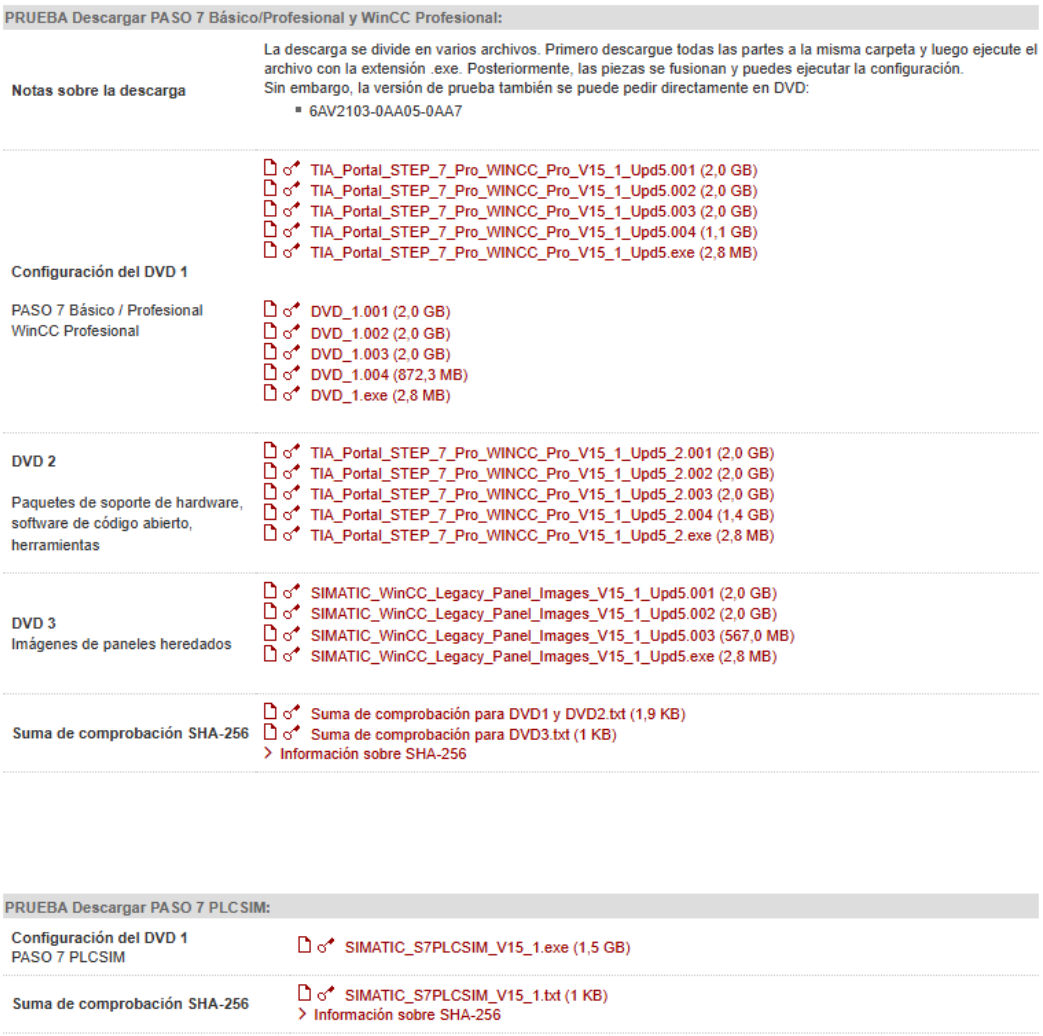
Resultados: La comunicación se estableció de manera estable. La librería `minimalmodbus` gestionó correctamente el cálculo del CRC (Cyclic Redundancy Check), asegurando que los datos de temperatura recibidos fueran íntegros y descartando cualquier trama afectada por ruido eléctrico.

PUNTO 3: AUTOMATIZACIÓN Y VIRTUALIZACIÓN DE PROCESOS (TIA PORTAL)

4.1. Entorno de Desarrollo e Instalación del TIA Portal

Se utilizó la suite **Siemens TIA Portal**, integrando la configuración de hardware y la programación lógica en una sola interfaz. Para la validación, se empleó **S7-PLCSIM**, permitiendo emular el comportamiento de una CPU física con alta fidelidad. Antes de desarrollar el proyecto, se llevó a cabo la instalación completa del entorno TIA Portal.

1. **Descarga desde Siemens Support.**



PRUEBA Descargar PASO 7 Básico/Profesional y WinCC Profesional:

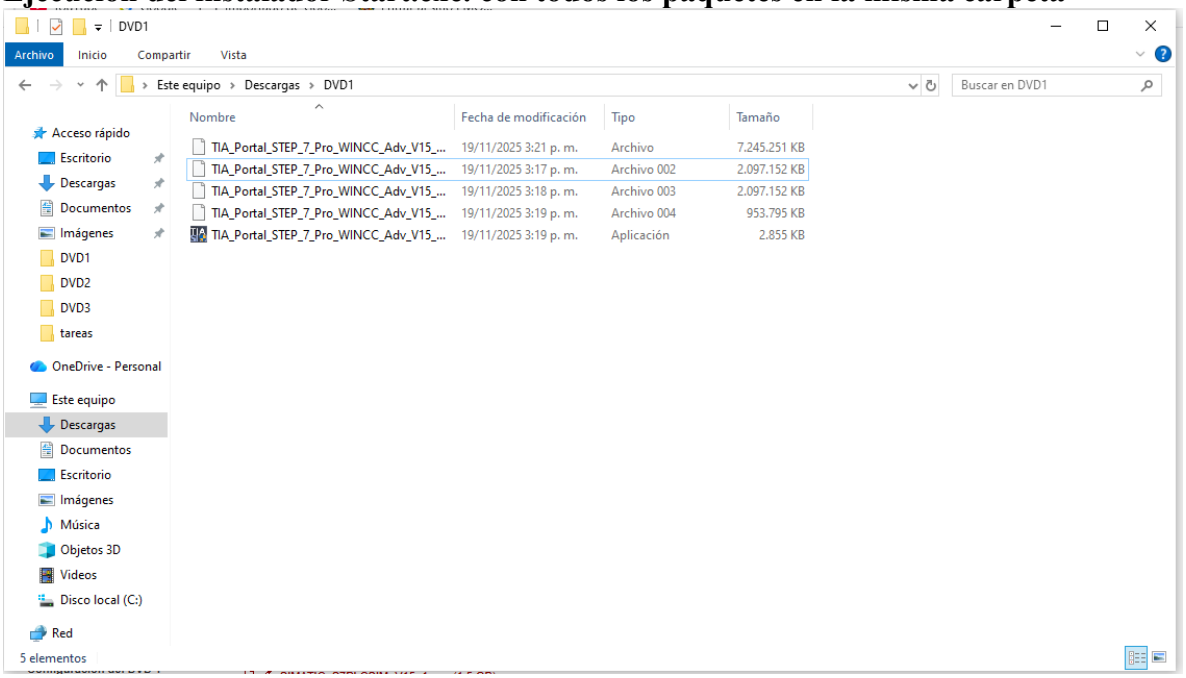
Notas sobre la descarga	La descarga se divide en varios archivos. Primero descargue todas las partes a la misma carpeta y luego ejecute el archivo con la extensión .exe. Posteriormente, las piezas se fusionan y puedes ejecutar la configuración. Sin embargo, la versión de prueba también se puede pedir directamente en DVD: ▪ 6AV2103-0AA05-0AA7
Configuración del DVD 1 PASO 7 Básico / Profesional WinCC Profesional	TIA_Portal_STEP_7_Pro_WINCC_Pro_V15_1_Upd5.001 (2,0 GB) TIA_Portal_STEP_7_Pro_WINCC_Pro_V15_1_Upd5.002 (2,0 GB) TIA_Portal_STEP_7_Pro_WINCC_Pro_V15_1_Upd5.003 (2,0 GB) TIA_Portal_STEP_7_Pro_WINCC_Pro_V15_1_Upd5.004 (1,1 GB) TIA_Portal_STEP_7_Pro_WINCC_Pro_V15_1_Upd5.exe (2,8 MB) DVD_1.001 (2,0 GB) DVD_1.002 (2,0 GB) DVD_1.003 (2,0 GB) DVD_1.004 (872,3 MB) DVD_1.exe (2,8 MB)
DVD 2 Paquetes de soporte de hardware, software de código abierto, herramientas	TIA_Portal_STEP_7_Pro_WINCC_Pro_V15_1_Upd5_2.001 (2,0 GB) TIA_Portal_STEP_7_Pro_WINCC_Pro_V15_1_Upd5_2.002 (2,0 GB) TIA_Portal_STEP_7_Pro_WINCC_Pro_V15_1_Upd5_2.003 (2,0 GB) TIA_Portal_STEP_7_Pro_WINCC_Pro_V15_1_Upd5_2.004 (1,4 GB) TIA_Portal_STEP_7_Pro_WINCC_Pro_V15_1_Upd5_2.exe (2,8 MB)
DVD 3 Imágenes de paneles heredados	SIMATIC_WinCC_Legacy_Panel_Images_V15_1_Upd5.001 (2,0 GB) SIMATIC_WinCC_Legacy_Panel_Images_V15_1_Upd5.002 (2,0 GB) SIMATIC_WinCC_Legacy_Panel_Images_V15_1_Upd5.003 (567,0 MB) SIMATIC_WinCC_Legacy_Panel_Images_V15_1_Upd5.exe (2,8 MB)
Suma de comprobación SHA-256	Suma de comprobación para DVD1 y DVD2.txt (1,9 KB) Suma de comprobación para DVD3.txt (1 KB) › Información sobre SHA-256

PRUEBA Descargar PASO 7 PLCSIM:

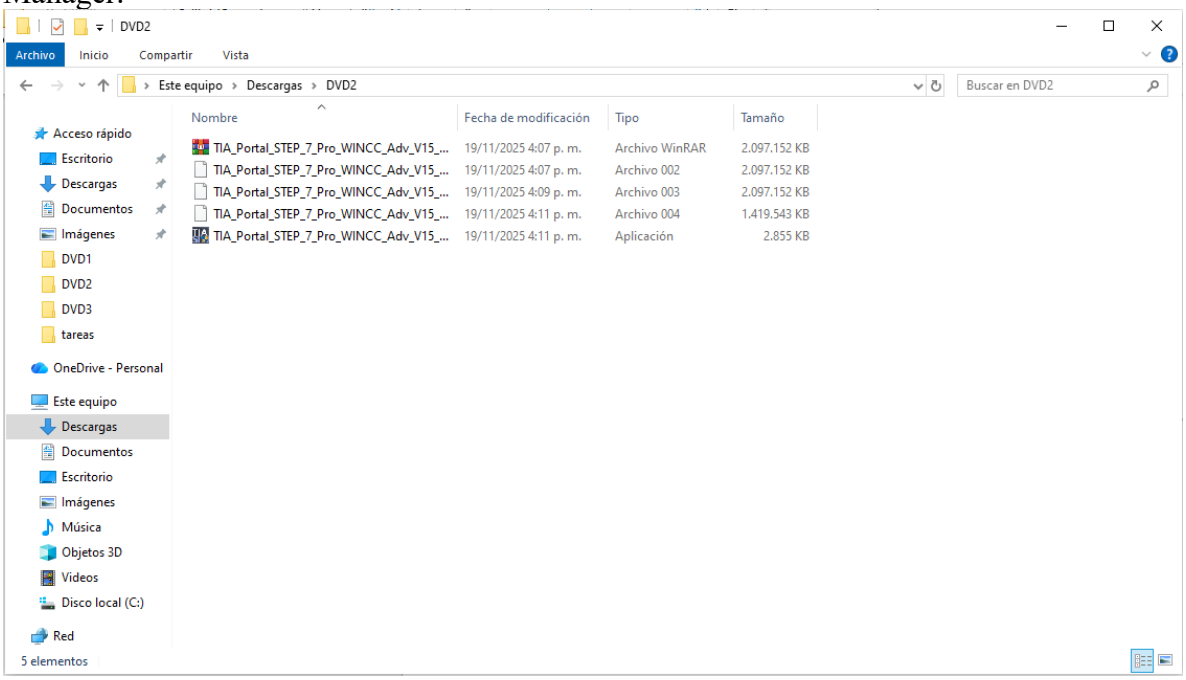
Configuración del DVD 1 PASO 7 PLCSIM	SIMATIC_S7PLCSIM_V15_1.exe (1,5 GB)
Suma de comprobación SHA-256	SIMATIC_S7PLCSIM_V15_1.txt (1 KB) › Información sobre SHA-256

Figura 4. Página oficial de descarga de TIA Portal.

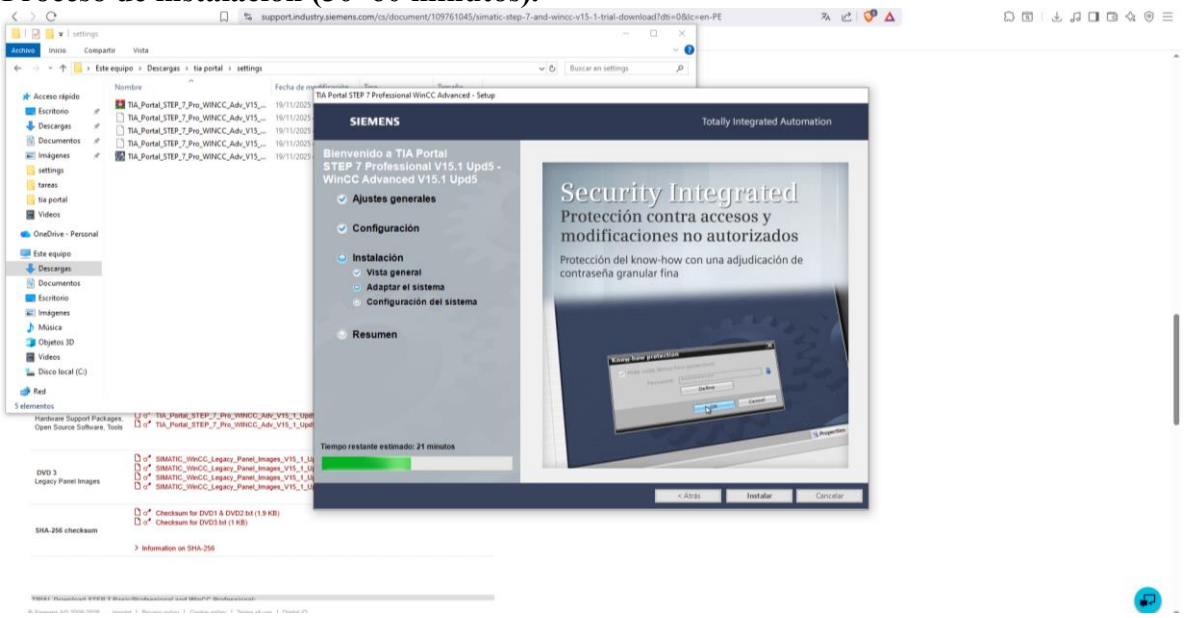
2. **Ejecución del instalador Start.exe. con todos los paquetes en la misma carpeta**



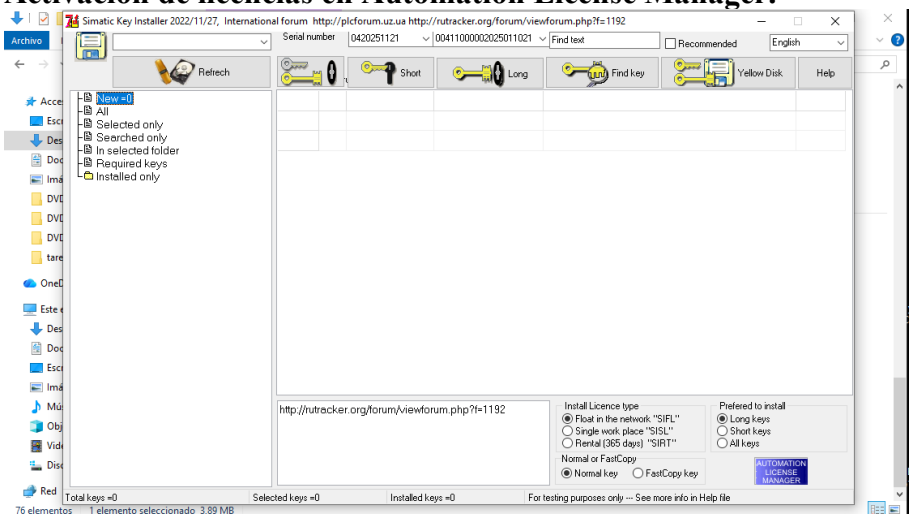
3. **Realizar lo mismo con los componentes:** STEP 7, WinCC, Automation License Manager.



4. **Proceso de instalación (30–60 minutos).**



5. **Reinicio del sistema.**
6. **Activación de licencias en Automation License Manager.**



4.2. Configuración de Hardware (S7-1200) Se seleccionó una CPU **1212C DC/DC/DC**. Esta elección técnica implica:

1. Alimentación de la CPU a 24V DC.
2. Entradas digitales a 24V DC.
3. Salidas digitales a transistor (DC), ideales para conmutación rápida.

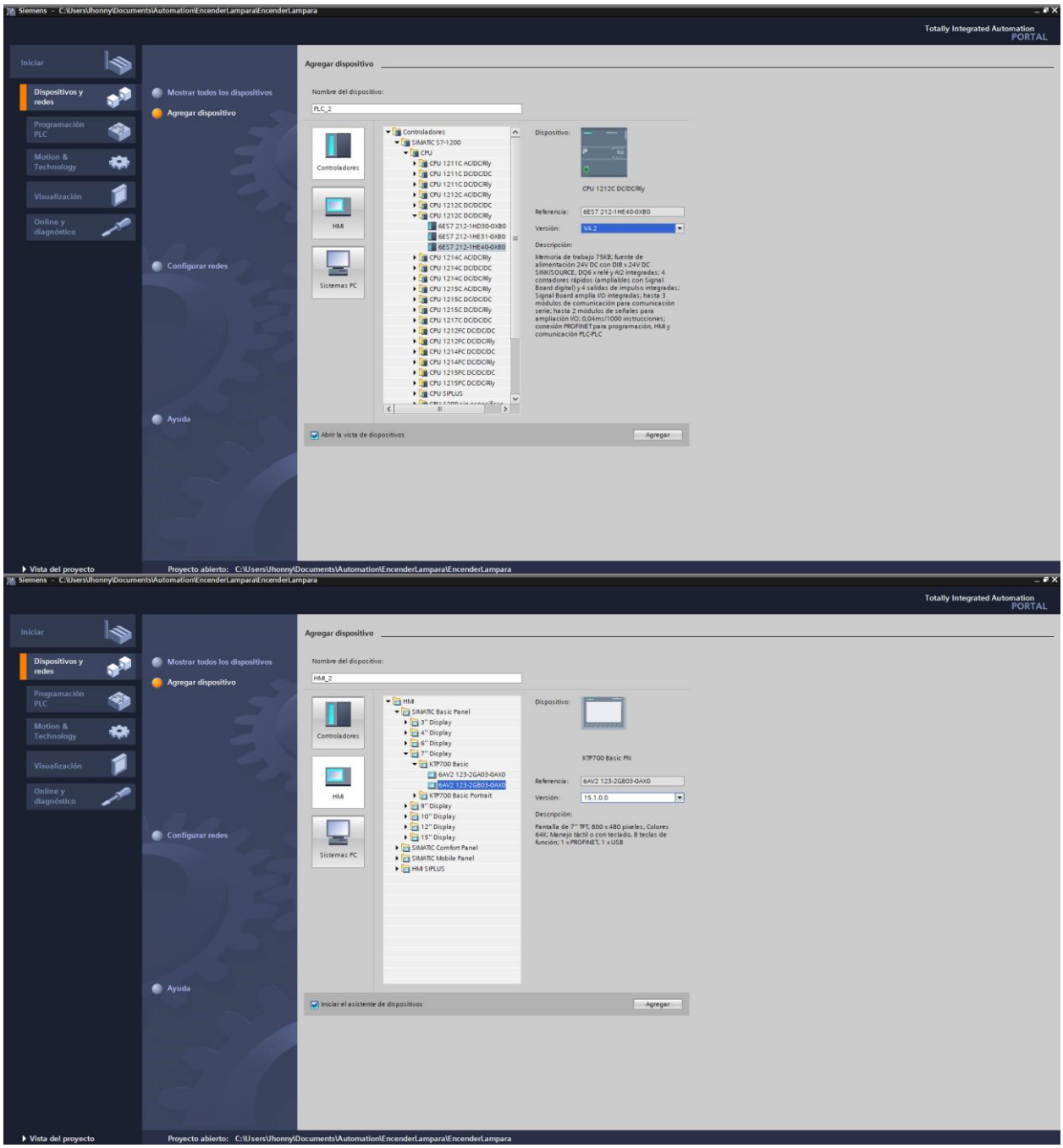


Figura 5. Configuración de dispositivos en TIA Portal.

4.3. Direccionamiento y Variables Se aplicó direccionamiento simbólico para mejorar la mantenibilidad del código. Se mapearon las siguientes variables en la tabla del PLC:

- Entrada `%M0.0` asignada a la etiqueta `Start_Button`.
- Salida `%Q0.0` asignada a la etiqueta `Motor_Lamp`.

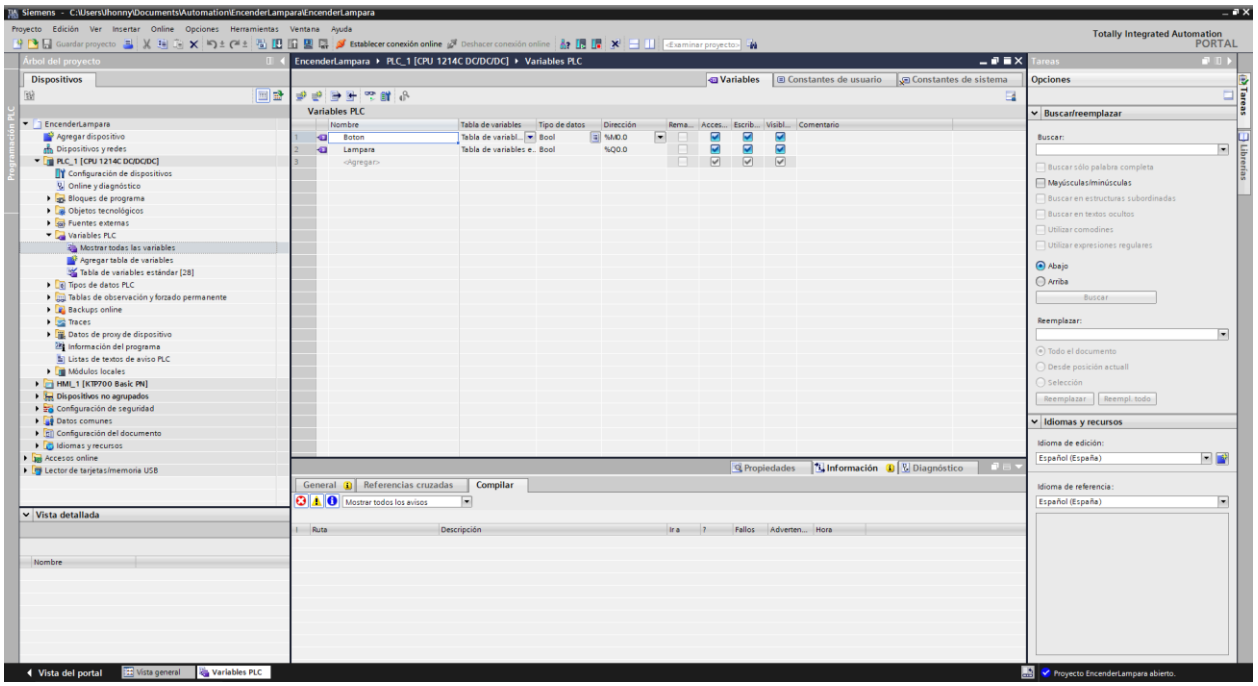


Figura 6. Definición de Tags del PLC.

4.4. Lógica de Control (Ladder) Se implementó un circuito de mando directo en el Bloque de Organización 1 (**Main OB1**). La lógica consiste en un contacto normalmente abierto (NO) que, al ser energizado, cierra el circuito lógico y activa la bobina de salida.

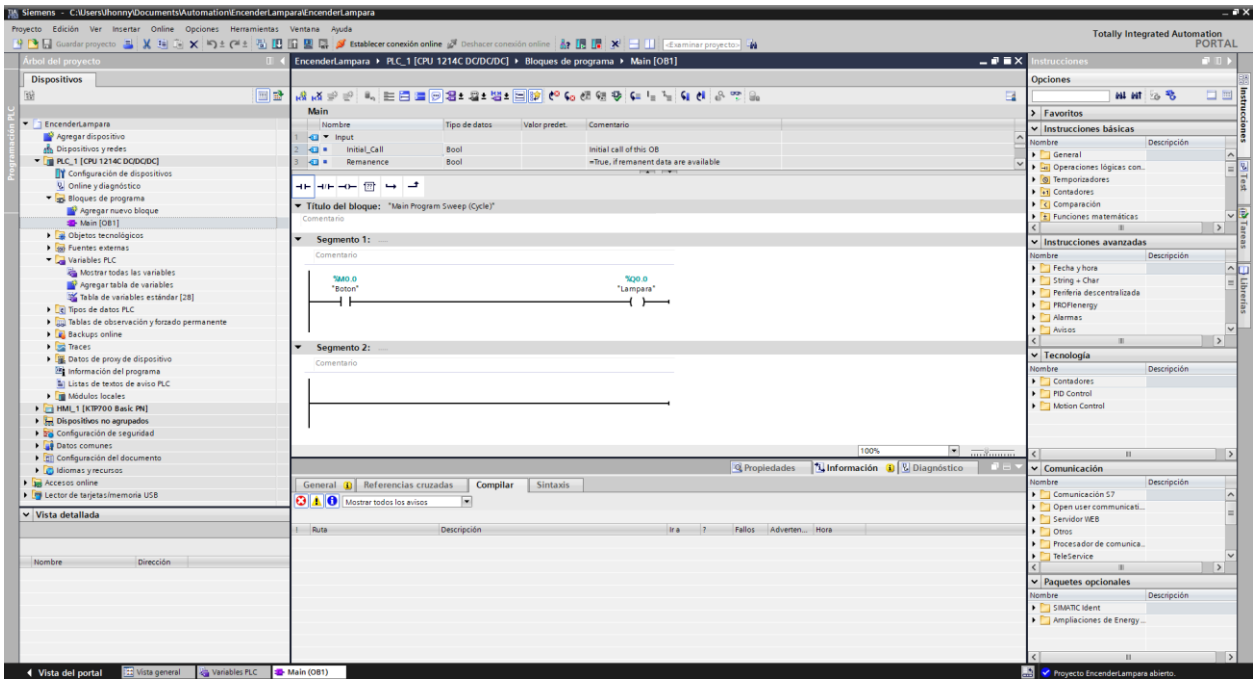


Figura 7. Lógica Ladder implementada para el control de arranque.

4.5. Validación y Simulación Mediante PLCSIM, se forzaron las variables de entrada para validar la respuesta del sistema. La simulación en modo "Online" permitió visualizar el flujo de corriente virtual (líneas verdes), confirmando que la lógica responde correctamente a los estímulos externos.

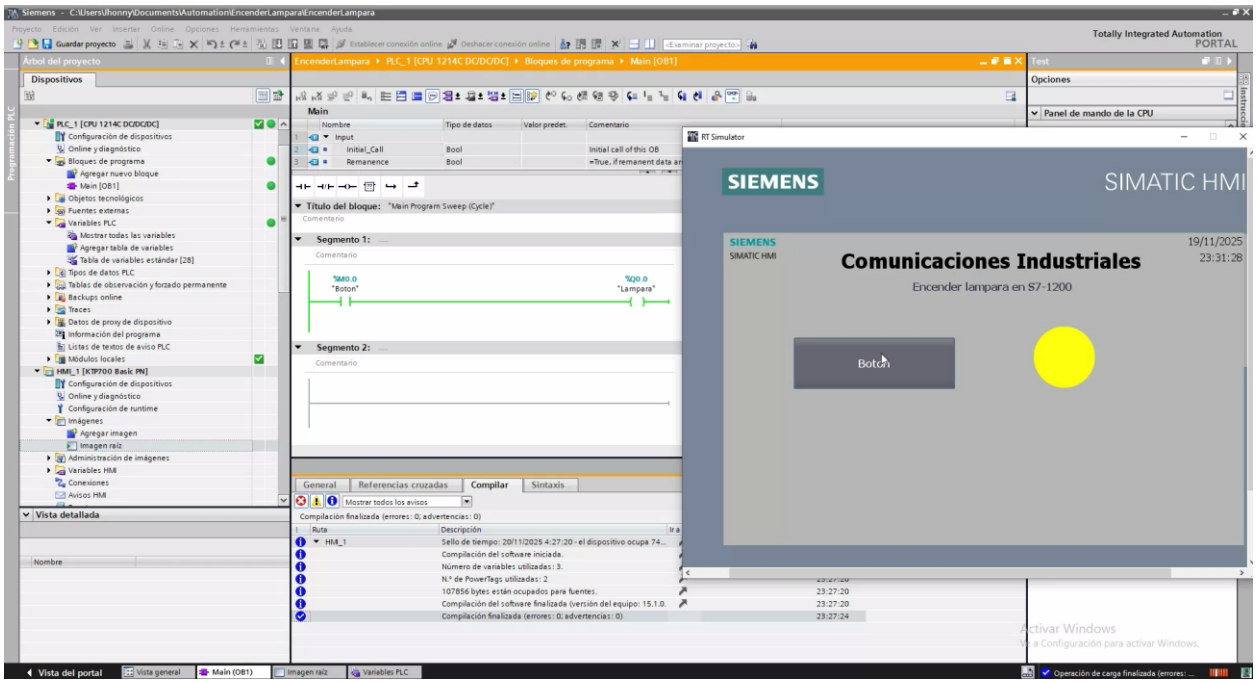


Figura 8. Validación en tiempo real mediante S7-PLCSIM.

5. CONCLUSIONES

1. **Segmentación y Seguridad:** La práctica de redes demostró que la división de una red industrial en subredes (VLANs o segmentos físicos enrutados) no solo organiza el tráfico, sino que aísla los dominios de broadcast. Se evidenció que ARP es un protocolo estrictamente local, lo cual es un concepto clave para el diseño de redes escalables.
2. **Robustez de Modbus RTU:** La implementación del bus RS485 validó su vigencia en la industria. A pesar de ser una tecnología con décadas de antigüedad, su simplicidad y la inmunidad al ruido del par diferencial lo hacen superior a comunicaciones simples (como TTL directo) para entornos ruidosos. El uso de librerías estandarizadas en el Maestro (Raspberry Pi) facilitó la integración sin necesidad de gestionar bits individuales.
3. **Virtualización como Herramienta de Ingeniería:** El uso de PLCSIM y TIA Portal demostró que es posible validar la lógica de control completa (Virtual Commissioning) antes de realizar inversiones en hardware físico. Se verificó exitosamente el ciclo de escaneo del PLC, el direccionamiento de memoria y la ejecución lógica Ladder.

6. BIBLIOGRAFÍA

1. Tanenbaum, A. S. (2012). *Redes de Computadoras*. Pearson Educación.
2. Siemens AG. (2019). *SIMATIC S7-1200 Programmable Controller - System Manual*.
3. Modbus Organization. (2020). *Modbus Application Protocol Specification V1.1b3*.