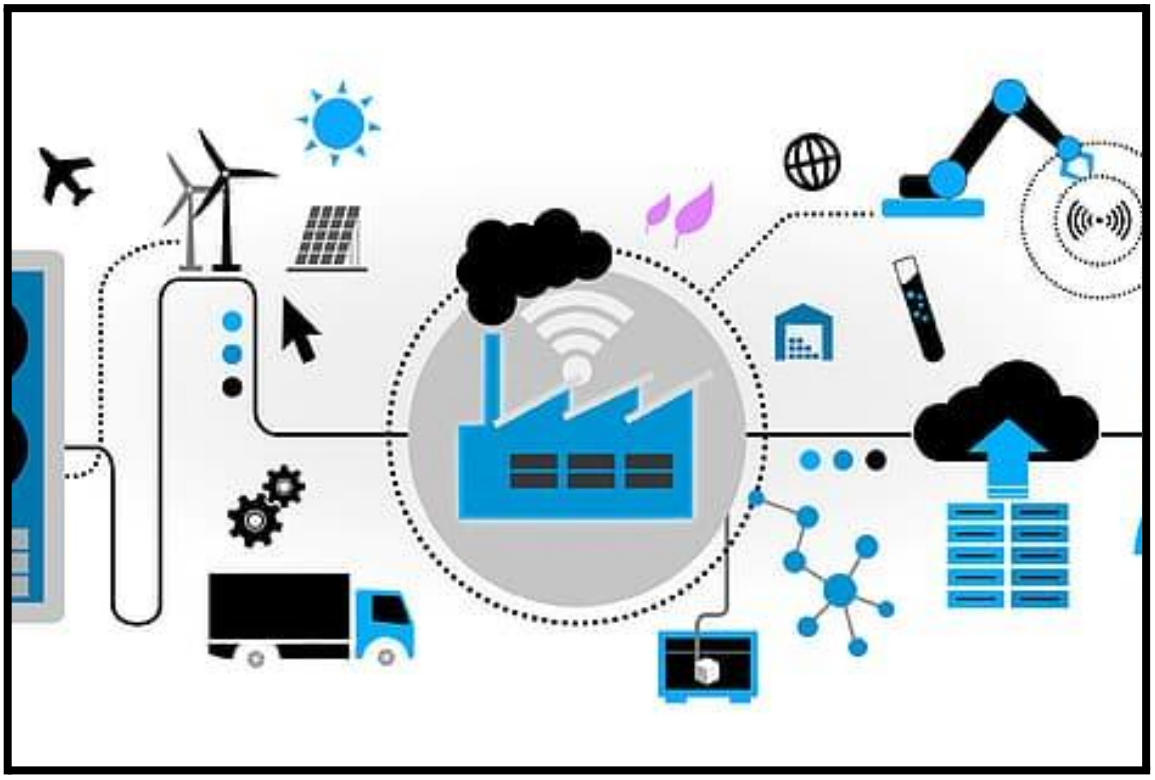
Escuela de Innovación Profesional
Berrikuntza Profesionalen Eskola

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

Financiado por la Unión Europea
NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

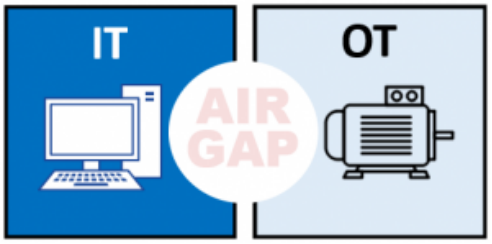
DESPLIEGUE DE UN LABORATORIO VIRTUALIZADO ESCENARIO INDUSTRIA 4.0



Convergencia de una red IT (Tecnología Información) con una red OT (Tecnologías Operación).

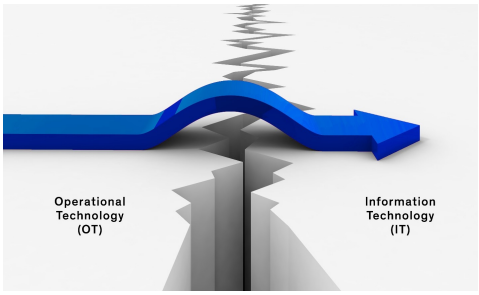
Descripción del escenario

Tradicionalmente, las tecnologías centradas en la información (en adelante IT, Information Technologies) y aquellas centradas en la operación (OT, Operational Tecnologies) se han mantenido aisladas entre sí, estando sus equipos enfocados en tareas, objetivos distintos e incluso vinculado con perfiles laborales diferentes, manteniendo poca o nula comunicación y coordinación entre ambas áreas



Sin embargo, los nuevos procesos y técnicas de análisis permiten (gracias a la gran cantidad de datos generados en los sistemas productivos) obtener resultados nuevos y generar información detallada sobre qué y cómo ocurre el proceso de producción y poder realizar correcciones, optimizaciones, generar informes de valor para las capas de negocio y, en general, abrir un abanico de herramientas que permitan tomar mejores decisiones desde el negocio.

Este enfoque requiere para ello que ambos entornos IT/OT estén conectados entre ellos, saltando con ello el “gap” tradicional existente.



Ahora bien, esta conexión entre ambos entornos debe de realizarse con la premisa de comprender perfectamente los requisitos de ciberseguridad que se deben implementar para garantizar la confidencialidad, integridad y disponibilidad de los diferentes procesos que se realizarán en ambos entornos.

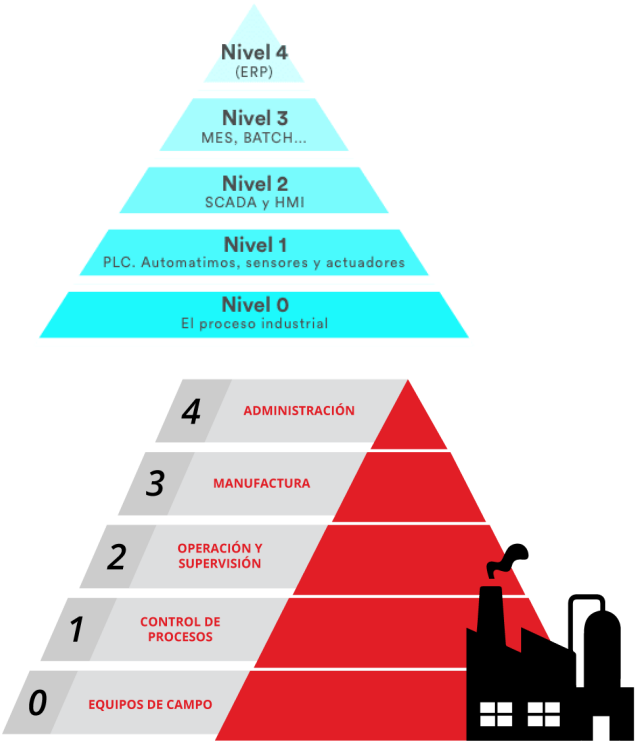
Entre las estrategias de ciberseguridad que se deben aplicar destacamos fundamentalmente:

- La segmentación física de las redes a través de firewall
- La configuración de ACL's (Listas control Acceso) que aseguren que únicamente se autoriza el tráfico que se necesita desde un origen/destino específico.

Esta estrategia trae consigo la premisa de identificar cuáles son los procesos y requisitos de seguridad que se desarrollan en las redes IT y OT con el objetivo de definir los niveles de segmentación más adecuados que puedan garantizar la segura interoperabilidad estrictamente necesaria entre ambos entornos.

Normativa ISA 95 automatización industrial

La **Norma ISA-95** es un estándar internacional que facilita la integración de todos los sistemas de información que puedan estar involucrados en un entorno de fabricación, desde las funciones empresariales hasta los sistemas de control en planta.
Define 5 niveles de segmentación identificando los procesos/equipos que se ubican en cada uno de ellos.



Niveles ISA 95

Nivel 0:

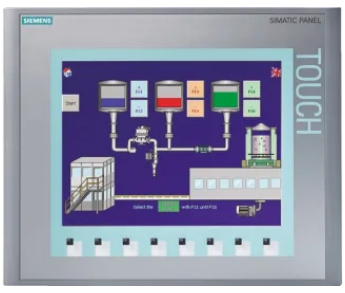
constituye el proceso industrial en sí mismo, la maquinaria y los recursos humanos necesarios. La parte más física de la propia empresa. (sensores, actuadores, motores...)

Nivel 1:

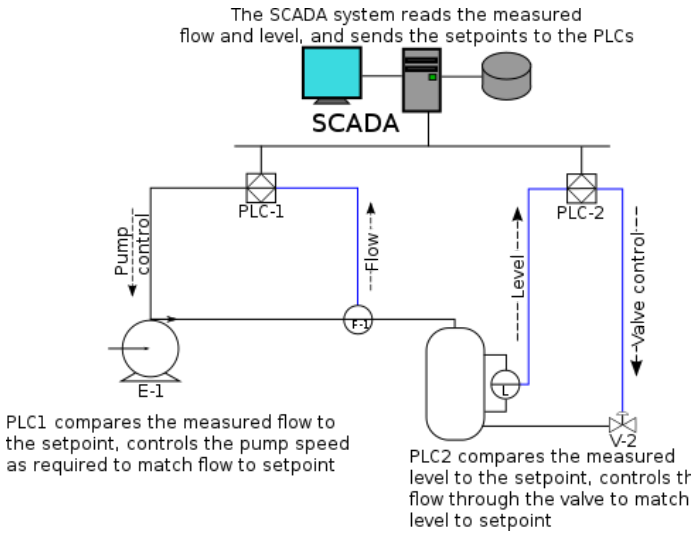
Corresponde a la interacción entre la parte física (sensores y actuadores del nivel 0) con los sistemas de control más básicos, los **PLC's**
Los PLCs son máquinas electrónicas simples que realizan y analizan un programa cíclicamente.

Nivel 2:

Corresponde a la interacción del hombre con los elementos de la planta, principalmente con dos métodos, los **HMI** o monitores de operarios, donde tenemos pantallas de operador que controlan una determinada parte del proceso



y los sistemas **SCADA**, aplicaciones para ordenador donde poder monitorizar y gestionar la planta.



Nivel 3:

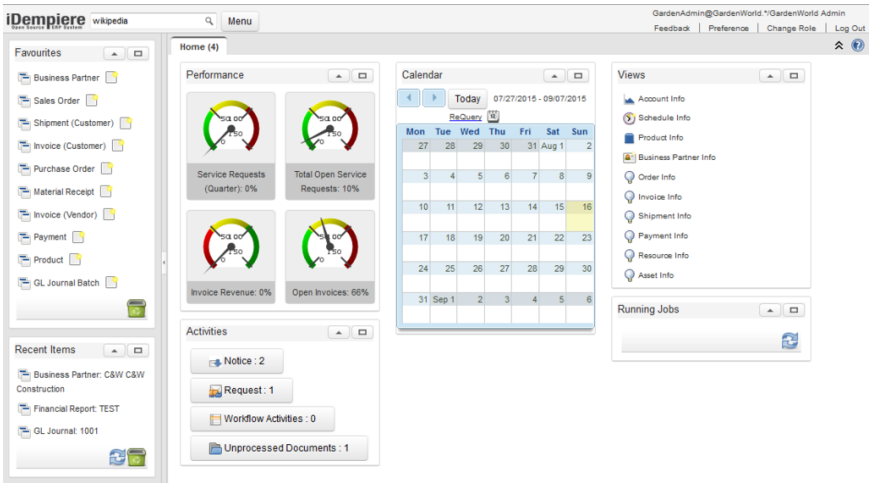
En este nivel se recogen los datos enviados por los PLC/SCADA en procesos **BATCH** y ficheros **Históricos.**

Estos datos son posteriormente interpretados, analizados y explotados en procesos de gestión y planificación, evitando que equipos y personal ubicados en los niveles de segmentación más próximos a la red IT necesiten acceder a esta información directamente desde la fuente que los ha producido (nivel OT)

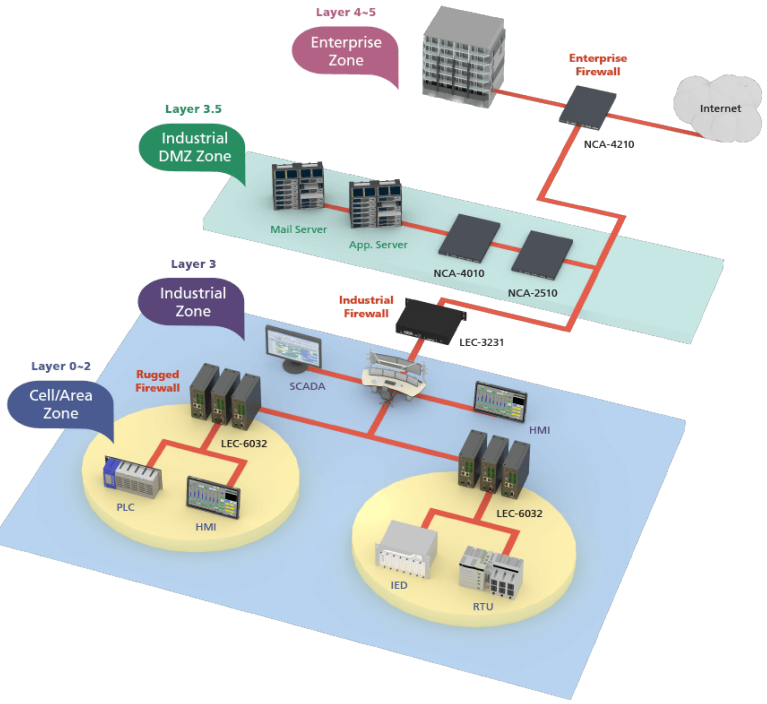
El **MES** (Manufacturing Execution System) es una interface entre el nivel 4 (donde se realizan los estudios de marketing y contabilidad) y el nivel 2 (donde tenemos la planta). Es la unión entre la inteligencia de la empresa (BI) y el proceso. Es importante esta interacción en tiempo real, donde conociendo la demanda podemos gestionar una mayor o menor regulación del flujo de producción

Nivel 4:

En el último nivel estarían los programas puramente económicos, contables y de marketing. Entre las herramientas en esta parte, tenemos los **ERP**, programas que gestionan los inventarios la facturación, contabilidad y la logística, estas aplicaciones nos permiten llevar todas las facturas emitidas por todas las personas de la empresa, los gastos y el inventarió.



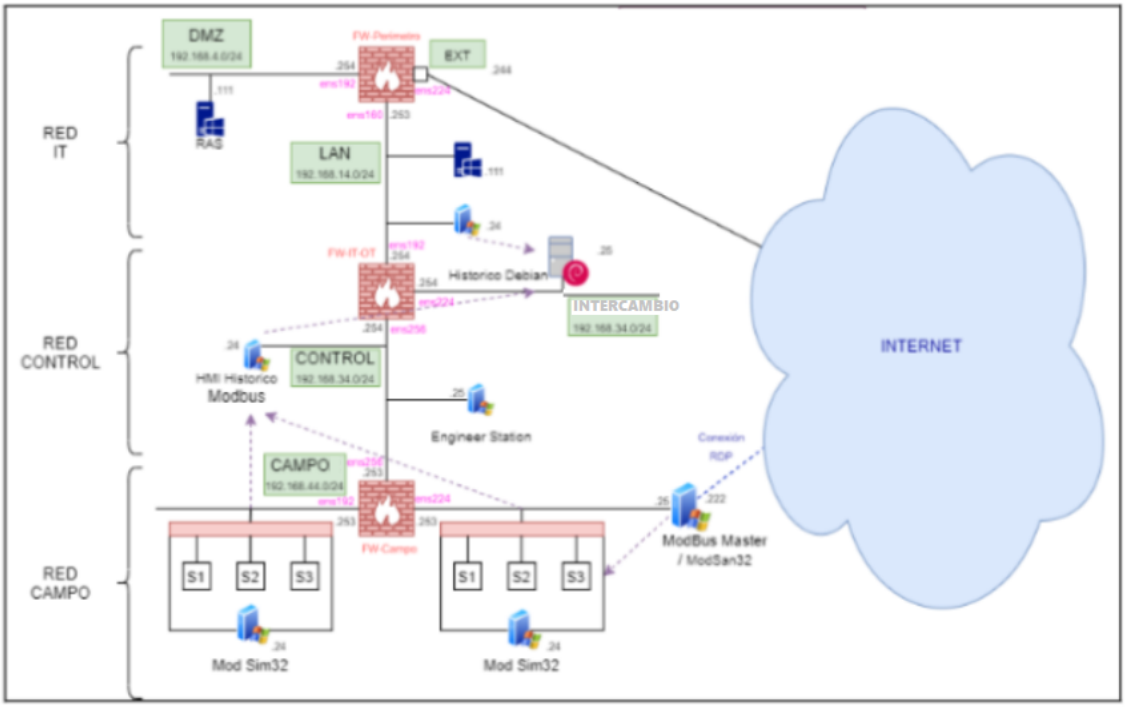
Ejemplo de diseño y segmentación entre los diferentes niveles descritos



Simulación de un entorno IT/OT a través de la virtualización de redes y equipos.

Diseño de redes y correspondencia con los niveles ISA

Para poder abordar el aprendizaje de la segmentación y seguridad en entornos integrados de redes IT y OT, planteamos la realización de un laboratorio de virtualización que integre diferentes segmentos de red relacionados con los niveles descritos anteriormente.
En el diagrama adjunto la correspondencia con los niveles ISA es la siguiente:



Nivel **RED IT**: corresponde con los **niveles 4 y 3** en ISA 95. En él se incluyen el equipamiento y personal vinculado a la red IT o red empresarial

Nivel **RED CONTROL**: Corresponde con el **nivel 2** en ISA 95 y contempla el despliegue de los sistemas de control basados en HMI así como el registro en los ficheros Históricos.
En este nivel se incorpora una red DMZ intermedia entre la red de IT y la primera capa de la red OT con objeto de recoger una copia de los ficheros históricos de la red control de manera que desde la red IT se pueda trabajar con esta información sin necesidad de acceso a la primera capa de la red OT

Nivel **RED CAMPO**: Corresponde con los **niveles 1 y 0** en ISA 95. Por simplificar el diseño, en este segmento se incorporan equipos linux que con el software adecuado,

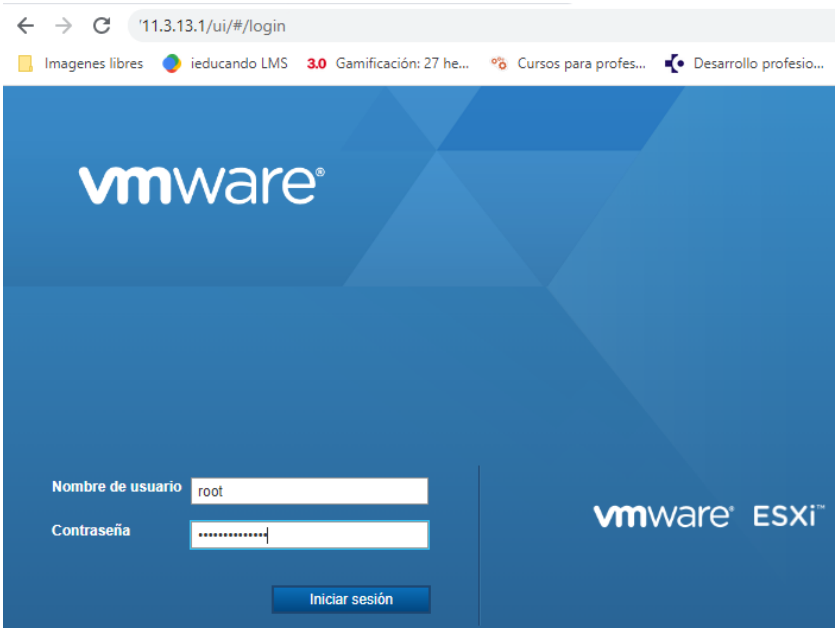
emulan el funcionamiento de un PLC (nivel 1) y de un equipo de campo (nivel 2) que recoge datos a través de sensórica.

Las líneas de datos, representados con trazos de puntos, reflejan los flujos de datos necesarios que deberán ser por ello securizados convenientemente mediante la configuración de reglas en los 3 firewall perimetrales y especialmente en los dos inferiores que segmentan la red IT/CONTROL y CONTROL/CAMPO

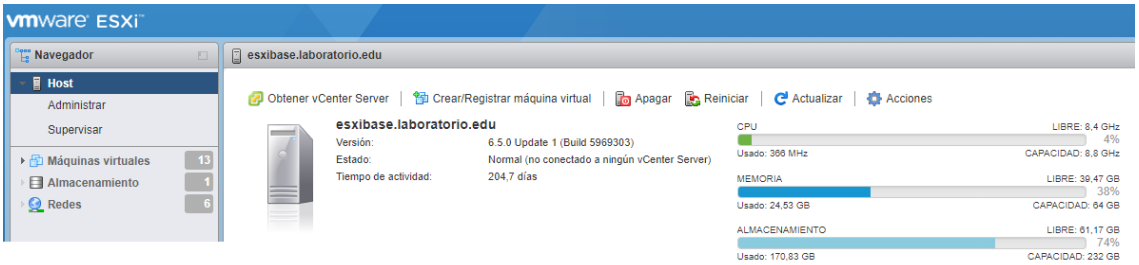
Virtualización de redes con VMWARE ESXI

Para la creación del entorno de red descrito vamos a utilizar el entorno de virtualización VMWARE basado en servidores ESXI.

Una vez configurado el servidor ESXI accedemos a su configuración a través de su dirección IP (definida durante su creación). En nuestro ejemplo usaremos la IP: 11.3.13.1 identificándonos con las credenciales configuradas previamente.



Una vez logueados, podemos visualizar los recursos asignados al mismo (CPU, memoria, espacio disco) y las carpetas principales “Máquinas virtuales”, “almacenamiento” y “Redes”



Definición de los segmentos de red

Atendiendo al diseño del laboratorio propuesto identificamos la necesidad de los siguientes segmentos de red:

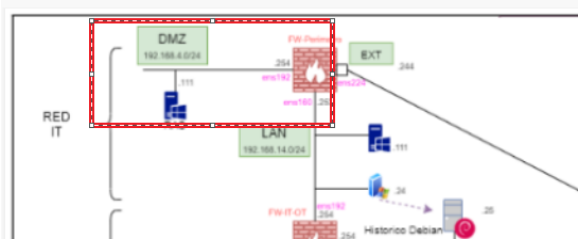
La **red EXTerna**:

Ubicada en el segmento superior, vinculada a la red IT, ofrece la salida hacia Internet

La **red LAN**:

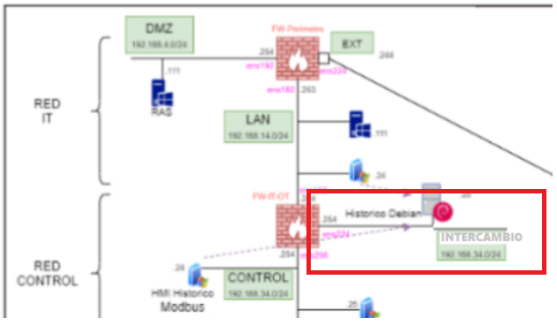
Situada entre el firewall perimetral (IT) y el primer firewall de la red OT. En ella su ubican los equipos de los empleados de la red IT

La **red DMZ**:



Segmento de la red IT para ubicar servidores y servicios que deban ser accesibles desde el exterior (Internet) como un servidor WEB, FTP, …

La **red INTERCAMBIO**:

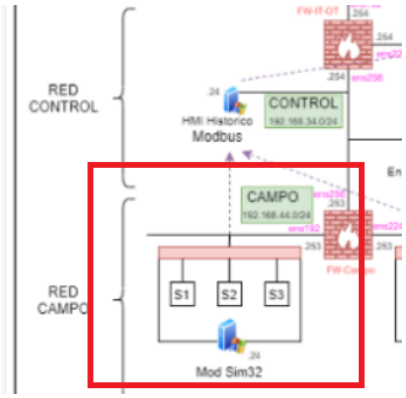


Segmento DMZ a partir del primer firewall de la red OT para albergar la réplica del servidor Histórico

La **red CONTROL**:

Ubicada entre los firewalls de la red industrial, ubica la estación de trabajo del ingeniero así como los componentes HMI y fichero Histórico.

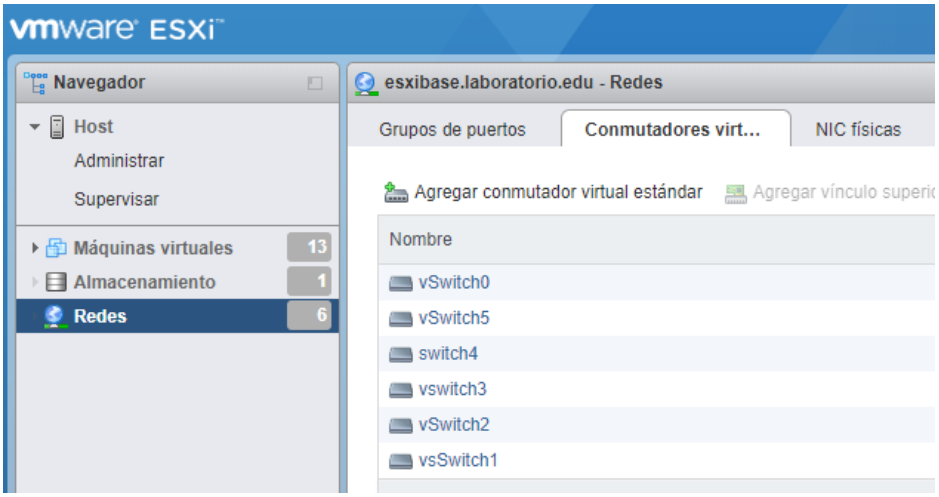
La **red CAMPO**:



El último nivel de segmentación contiene los equipos finales (sensores y actuadores) y en este diseño, por simplificar el modelo, representa también a los PLC's.
A nivel práctico, en este segmento se ubican equipos Linux con un software de simulación de **PLC** con protocolo de comunicación **modbus** generando aleatoriamente datos que representen la información recogida por **sensores** de temperatura o humedad por ej.

Configuración de los segmentos de red entorno ESXI

Para la configuración de los segmentos de red definidos anteriormente se procede desde el servidor ESXI a la opción de **redes**

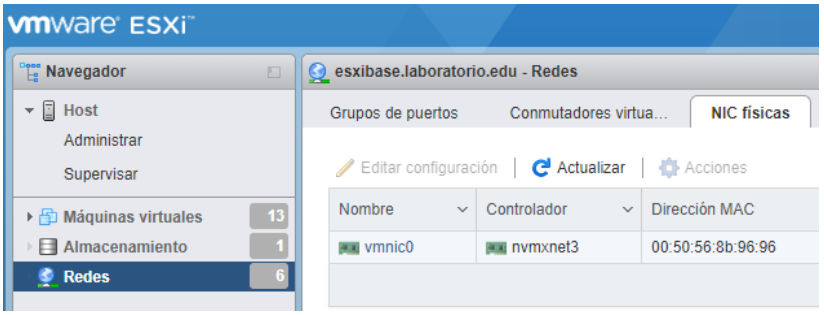


Una vez situados en este menú encontramos en la parte superior derecha las opciones de NIC físicas, Conmutadores virtuales, Grupos de puertos.

La opción de **NIC físicas:**

Muestra las tarjetas de red asignadas al servidor ESXI. En nuestro caso únicamente está declarada una tarjeta de red a través de la cual se conectará nuestro ESXI con el

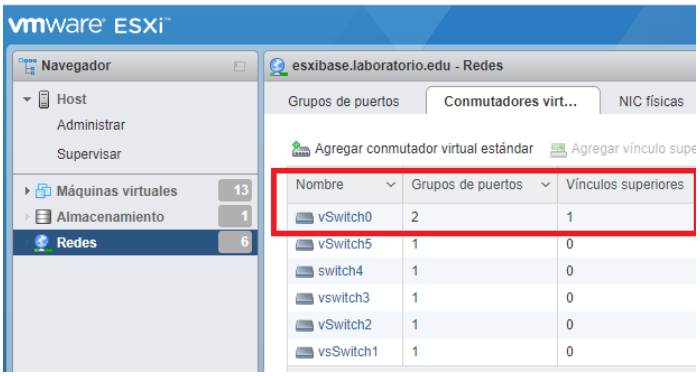
exterior (Internet) de manera similar a la configuración en modo “bridge” de un entorno VMWARE Workstation/Player



La opción **conmutadores virtuales:**

Incluye la creación de todos los switches virtuales necesarios para la definición de los segmentos de red necesarios.

Durante la creación de los switch virtuales, debemos seleccionar cual de ellos será el que se conectara con el exterior (emulando el modo “bridge”) mediante la asignación de “vínculo superior” con alguna de las tarjetas NIC físicas existentes (En nuestro caso solo hay una disponible).

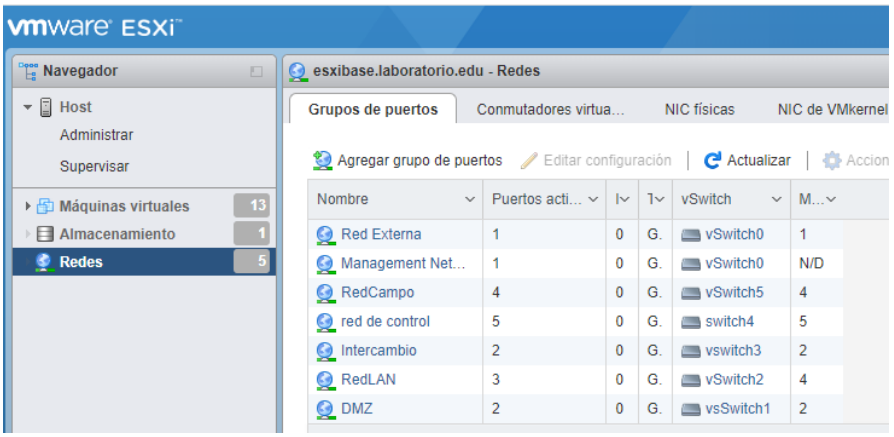


Una vez asignado un switch con vínculo superior ya NO es posible asignar a otro switch otro vínculo superior (a menos que se disponga de más tarjetas NIC físicas sin asignar).

En nuestro diseño se han identificado 6 segmentos de red necesarios por lo que debemos de crear por tanto 6 conmutadores virtuales nombrados en el ejemplo como vSwitch0 a vSwitch5. (obviando los errores tipográficos mostrados en la imagen)

La opción Grupos de puertos:

Es la cadena final utilizada para representar los segmentos finales de red a utilizar.



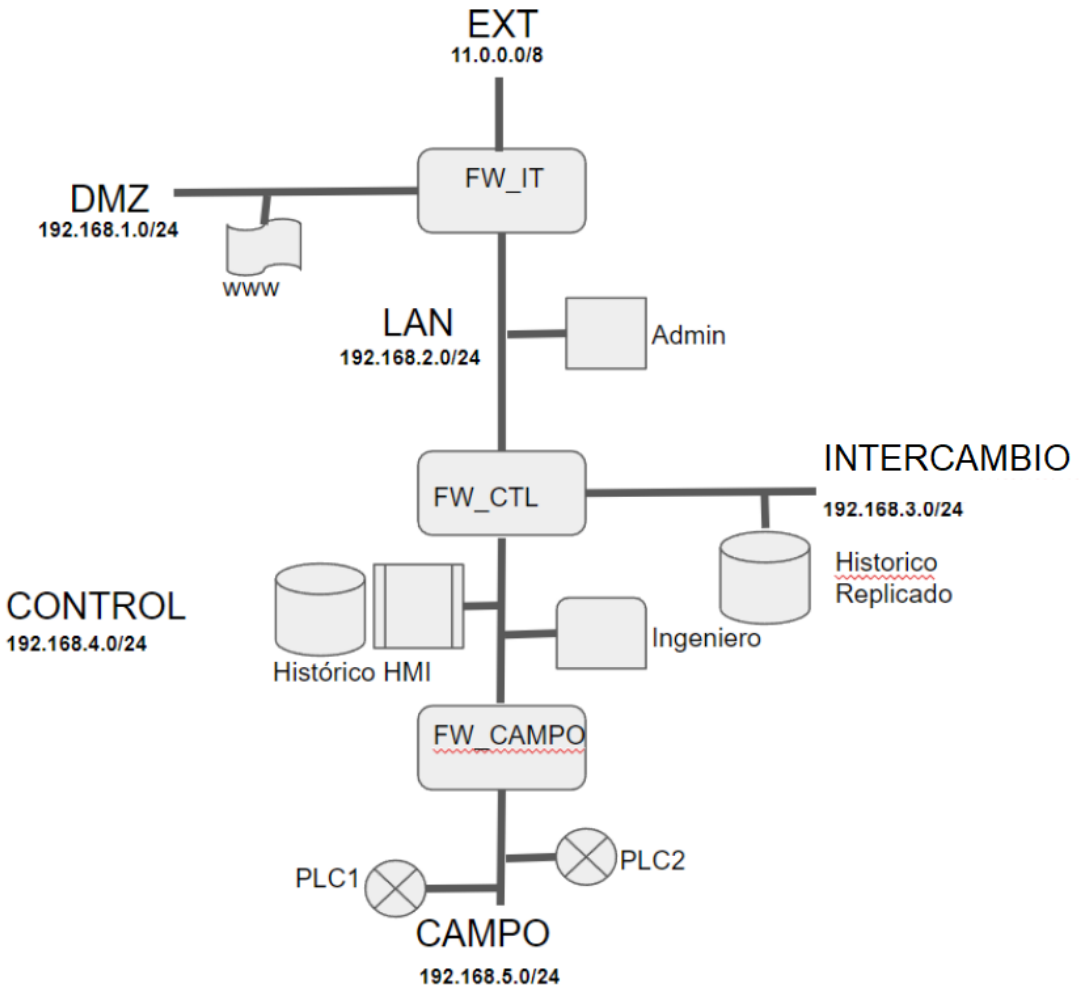
Durante la creación de cada grupo de puertos es necesario vincularlo con alguno de los conmutadores virtuales creados previamente. En la imagen se aprecia como el primer switch (vSwitch0) es compartido por dos grupos de puertos, **Red Externa** y **Management Network**.
El identificado como **Red Externa** es el que permite la salida hacia Internet de nuestro laboratorio, mientras que el identificado como **Management Network** es necesario para el propio acceso al servidor ESXI como tal (desde su IP 11.3.13.1).

Posteriormente a medida que vayamos creando las máquinas virtuales deberemos de vincularlas al grupo de puertos correspondiente al segmento de red donde deseamos ubicarla. En el caso de que alguna máquina virtual tenga más de una tarjeta de red (como los equipos que actuarán como firewall) será necesario que cada una de sus tarjetas de red esté asociada con un grupo de puertos diferente.

Direccionamiento de red

Para el direccionamiento interno vamos a utilizar 6 direcciones de red del grupo 192.168.x.n, asociadas a una clase C privada NO enrutable, mientras que para la red EXTerna y por requerimiento de la red real de nuestro centro educativo seleccionaremos una dirección específica de clase A 11.0.0.0/8.

Así, el direccionamiento de red utilizado en cada uno de los segmentos es el siguiente:



Asignación IP equipos Firewall

La asignación de direcciones IP a cada una del as tarjetas de red de cada firewall es la siguiente:

FW_IT: equipado con 3 tarjetas de red con el siguiente direccionamiento:

Tarjeta EXTerna: **ens192** IP: 11.3.11.254 mascara: 255.0.0.0 gateway: 11.0.0.1	Tarjeta DMZ: **ens256** IP: 192.168.1.254 mascara: 255.255.255.0	Tarjeta LAN: **ens224** IP:192.168.2.254 mascara: 255.255.255.0

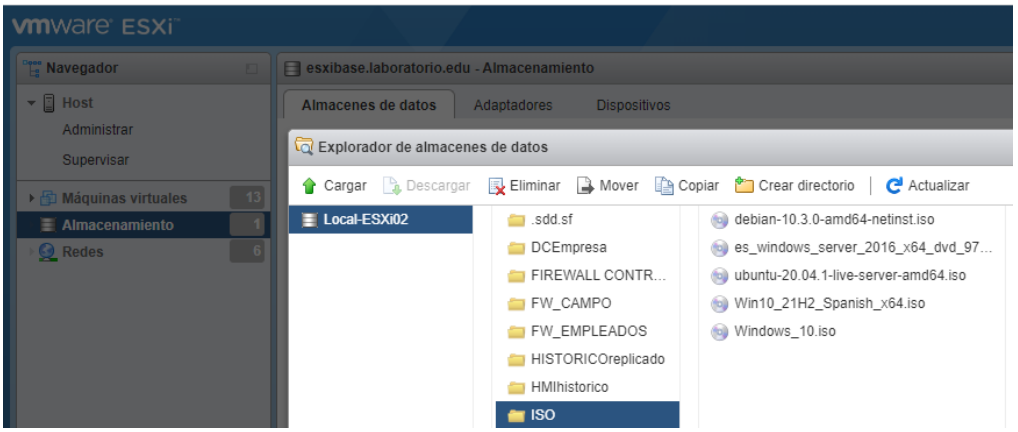
FW_CONTROL: equipado con 3 tarjetas de red con el siguiente direccionamiento:

Tarjeta LAN: IP:192.168.2.253 mascara: 255.255.255.0 gateway: 192.168.2.254	Tarjeta INTERCAMBIO: IP: 192.168.3.254 mascara: 255.255.255.0	Tarjeta CONTROL IP: 192.168.4.254 mascara:255.255.255.0

FW_CAMPO: equipado con 2 tarjetas de red con el siguiente direccionamiento:

Tarjeta CONTROL: IP:192.168.4.253 mascara: 255.255.255.0 gateway: 192.168.4.254	Tarjeta CAMPO: IP: 192.168.5.254 mascara: 255.255.255.0	

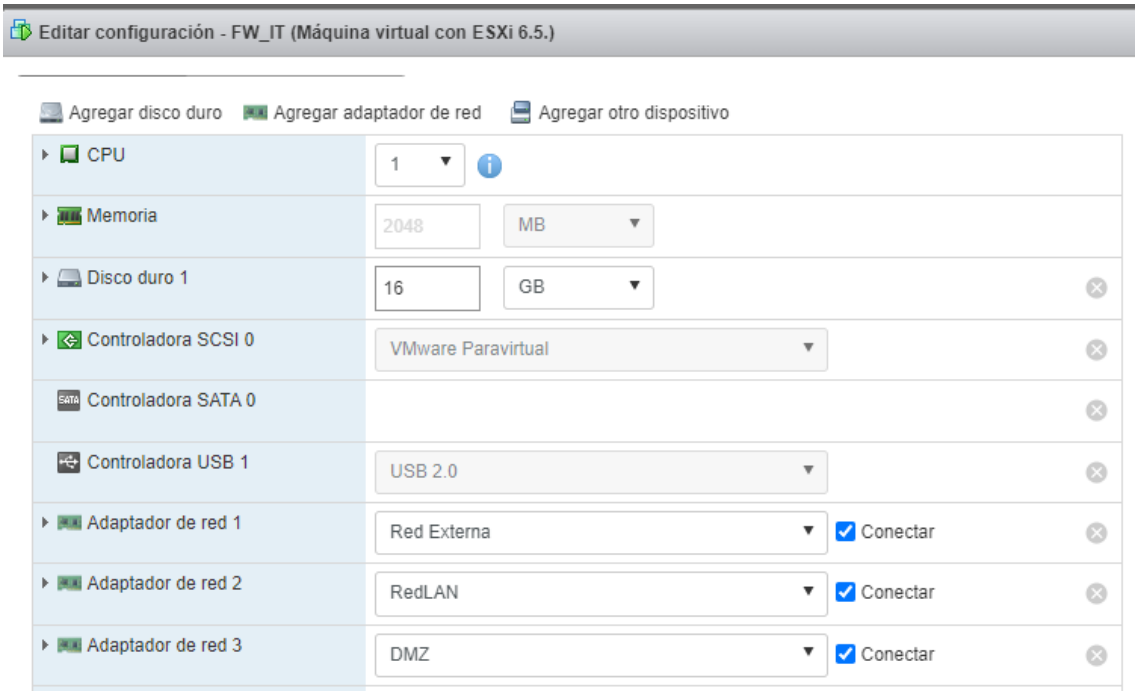
Los equipos actuando como firewall son una distribución LINUX y han sido instalados en el servidor ESXI a partir de una imagen ISO ubicada en su área de almacenamiento

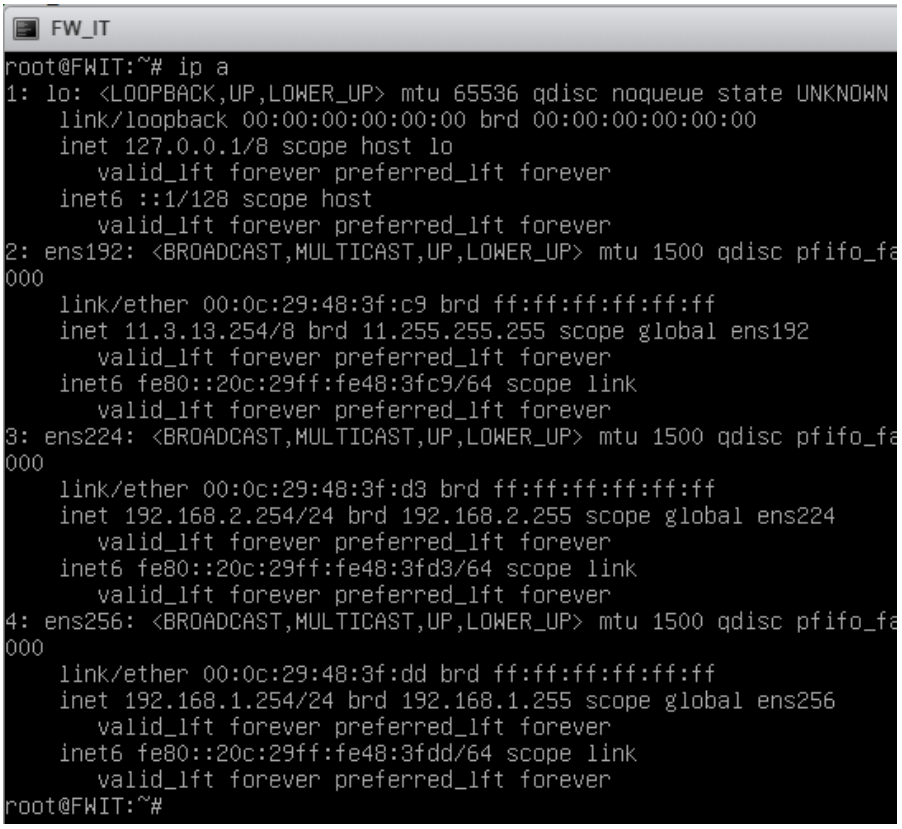


En cada uno de estos equipos se ha configurado la asignación de cada tarjeta de red a uno de los switches virtuales definidos en el apartado de red del ESXI en función del segmento/s de red en el que va a ubicarse.
A continuación se muestra esta asignación para cada uno de los firewalls así como su direccionamiento IP.
Cada una de las tarjetas de red mostradas como “adaptador de red” se corresponde en orden consecutivo con la numeración final en el equipo como “ensxx”.
Esto es:

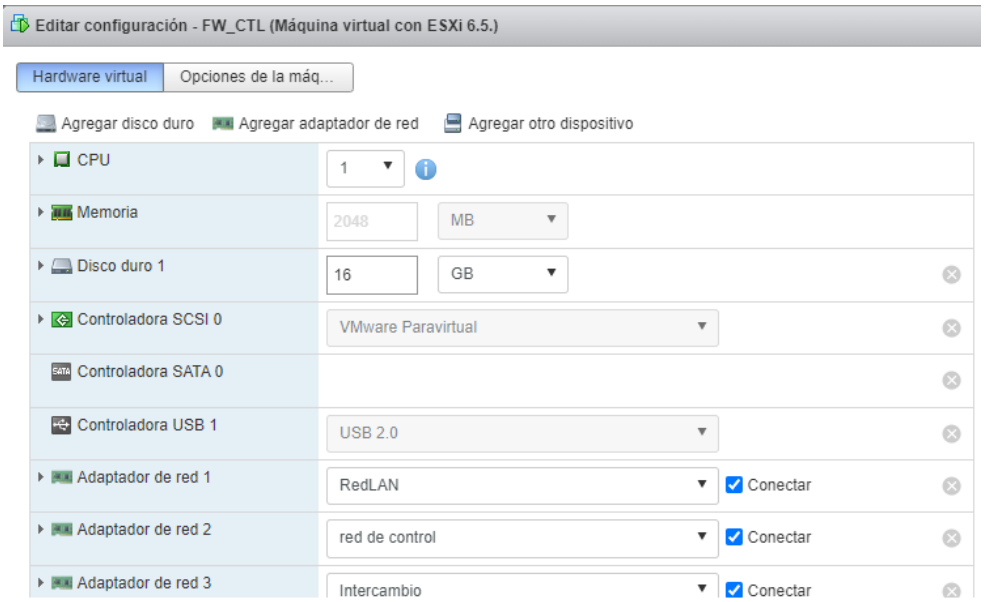
Adaptador de red 1 → ens192
Adaptador de red 2 → ens224
Adaptador de red 3 → ens256

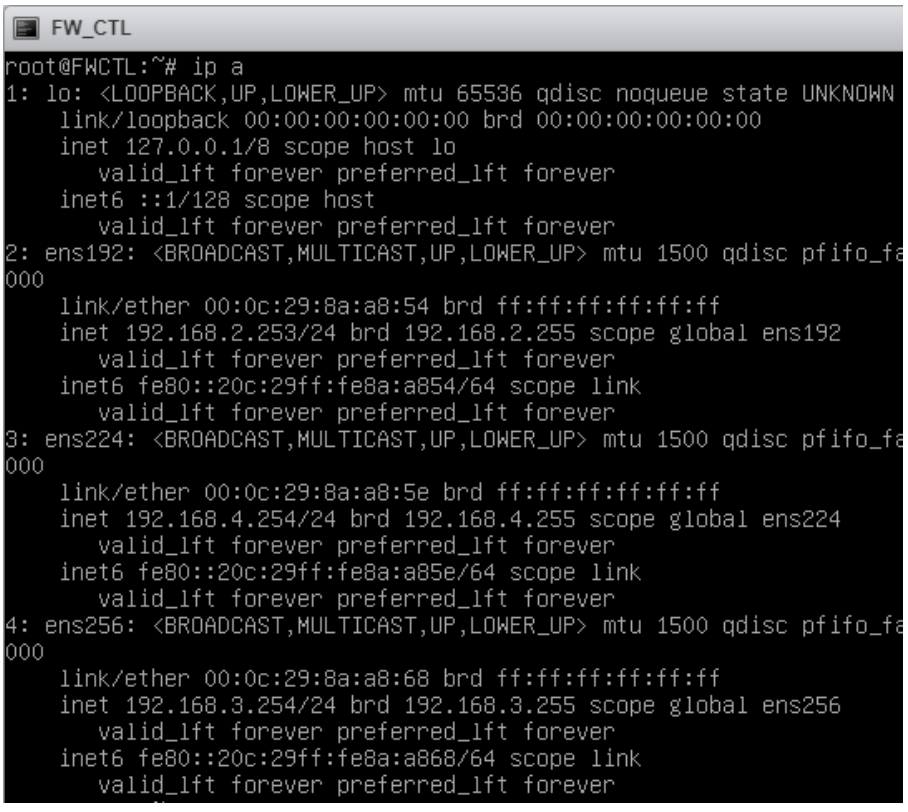
Firewall IT (FW:IT



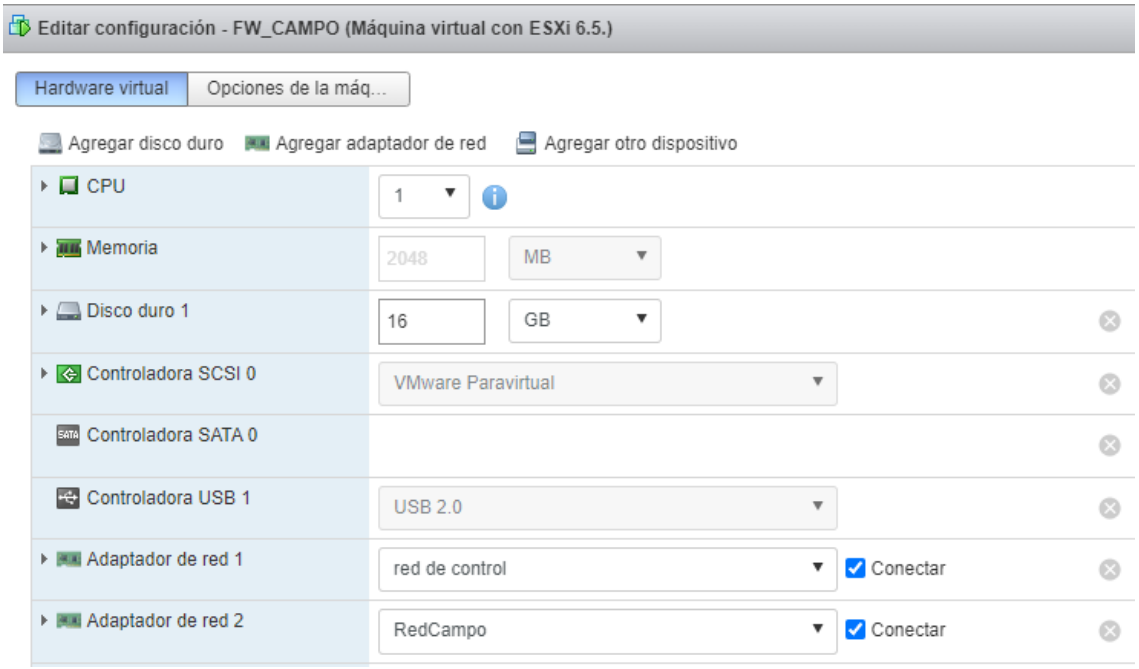


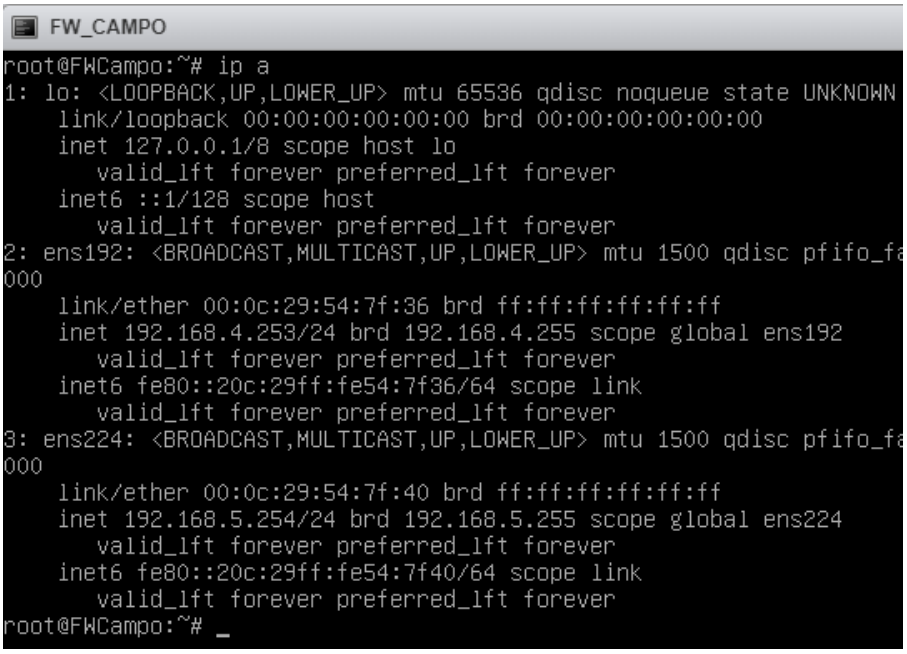
Firewall Control (FW_CTL)





Firewall Campo (FW_CAMPO)


Editar configuración - FW_CAMPO (Máquina virtual con ESXi 6.5.)
Hardware virtual
Opciones de la máq...
Agregar disco duro
Agregar adaptador de red
Agregar otro dispositivo
CPU
1
Memoria
2048
MB
Disco duro 1
16
GB
Controladora SCSI 0
VMware Paravirtual
Controladora SATA 0
Controladora USB 1
USB 2.0
Adaptador de red 1
red de control
Conectar
Adaptador de red 2
RedCampo
Conectar

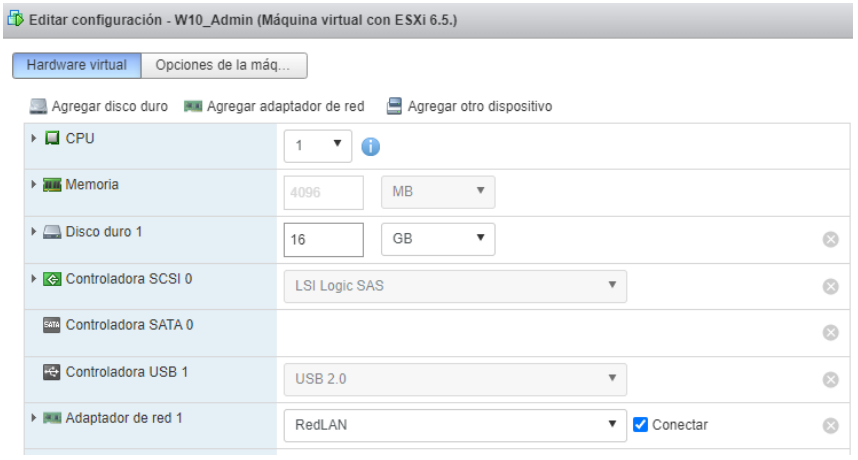

FW_CAMPO
root@FWCampo:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fa
000
link/ether 00:0c:29:54:7f:36 brd ff:ff:ff:ff:ff:ff
inet 192.168.4.253/24 brd 192.168.4.255 scope global ens192
valid_lft forever preferred_lft forever
inet6 fe80::20c:29ff:fe54:7f36/64 scope link
valid_lft forever preferred_lft forever
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fa
000
link/ether 00:0c:29:54:7f:40 brd ff:ff:ff:ff:ff:ff
inet 192.168.5.254/24 brd 192.168.5.255 scope global ens224
valid_lft forever preferred_lft forever
inet6 fe80::20c:29ff:fe54:7f40/64 scope link
valid_lft forever preferred_lft forever
root@FWCampo:~# _

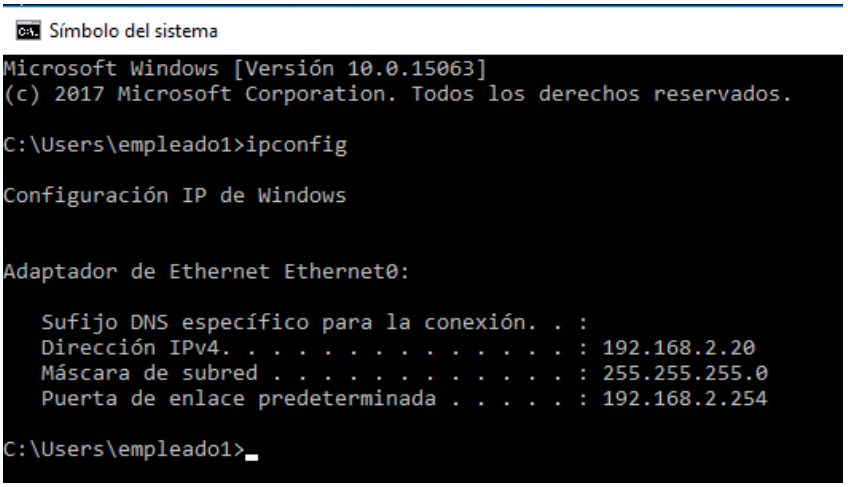
Definición y configuración IP de máquinas virtuales

Una vez establecidos los segmentos de red con su direccionamiento IP y establecidos los equipos que actuarán como firewall entre cada uno de estos segmentos, procedemos a la definición del resto de equipos que formarán el laboratorio así como el rol específico que tendrán en él.

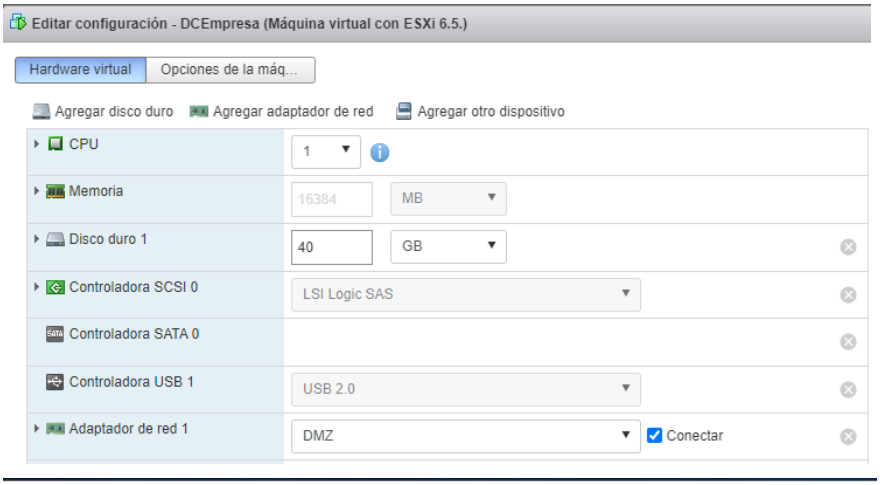
En el entorno de la **red IT**

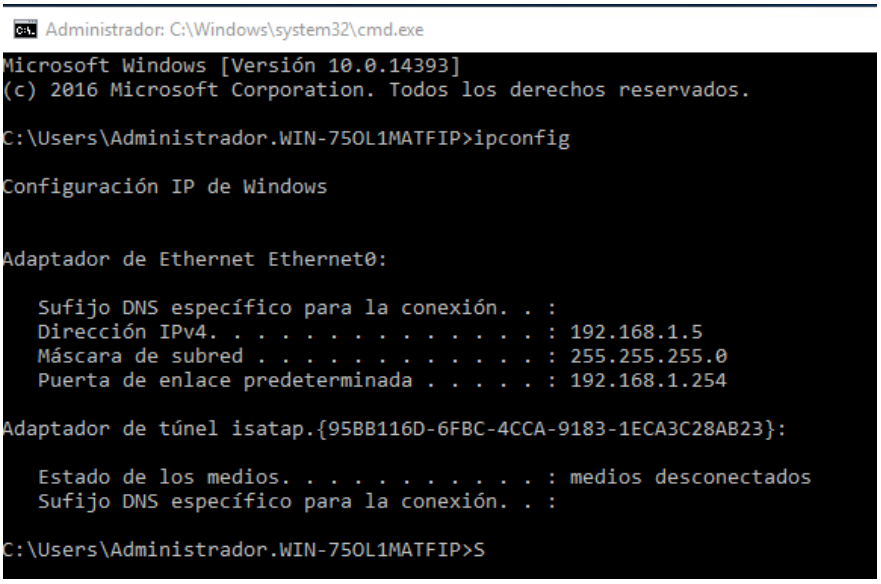
W10_Admin:
Equipo Windows 10, utilizado por el administrador de la red local con permisos para la administración del firewall de IT así como acceso al servidor Histórico Replicado ubicado en la DMZ “Supervisión”.
Su configuración de red a nivel del servidor ESXI y direccionamiento IP es la siguiente:





DC_Empresa:
Equipo Windows server 2016 ubicado en la DMZ y actuando como controlador del dominio “empresas” en el que está registrado el equipo w10_admin.





Reglas filtrado y nat en el Firewall (FW_IT)

El equipo que actúa como firewall está basado en una distribución linux debian y para su configuración como firewall vamos a utilizar IPTABLES.
El perímetro de seguridad a configurar se apoya en los siguientes supuestos:

1. Se habilita la inspección de estado
2. La política por defecto de las comunicaciones de entrada y salida hacia el firewall o de atravesarlo se establece a DENEGADO
3. Solo está permitida conexión de entrada al firewall para su gestión a través de una conexión ssh desde la red interna LAN (192.168.2.0/24) y únicamente desde el equipo del administrador (192.168.2.20)
4. Los equipos de la red local pueden:
    a. Comunicar con el equipo DC de la DMZ
    b. Conexión a Internet
5. Se permite realizar un PING entre todas las tarjetas de red firewall EXCEPTO desde la tarjeta EXTerna (ens192)
6. Todo el tráfico que salga por la tarjeta EXTerna debe ir enmascarado (NAT)
7. Se permite realizar un PING al firewall únicamente desde la red LAN

Configuración de reglas iptables para el cumplimiento de la política definida

```
  GNU nano 3.2                                    FW_IT

# Generated by xtables-save v1.8.2 on Mon May  9 08:50:58 2022
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A POSTROUTING -o ens192 -j MASQUERADE 6
COMMIT
# Completed on Mon May  9 08:50:58 2022
# Generated by xtables-save v1.8.2 on Mon May  9 08:50:58 2022
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0] 2
:OUTPUT DROP [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT 1
-A INPUT -i ens224 -p icmp -m icmp --icmp-type 8 -j ACCEPT 7
-A INPUT -i ens224 -s 192.168.2.20 -p tcp --dport 22 -j ACCEPT 3
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT 1
-A FORWARD -i !ens192 -p icmp -m icmp --icmp-type 8 -j ACCEPT 5
-A FORWARD -i ens224 -o ens256 -s 192.168.2.0/24 -d 192.168.1.5 -j ACCEPT 4a
-A FORWARD -i ens224 -o ens192 -p tcp -m multiport --dports 80,443 -j ACCEPT 4b
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT 1
COMMIT_
# Completed on Mon May  9 08:50:58 2022
```

Regla enrutado para llegar desde la LAN a la red INTERCAMBIO

```
root@FWIT:~# ip route add 192.168.3.0/24 via 192.168.2.253 dev ens224
```

En el entorno de la **red Control**

Reglas filtrado en el Firewall (FW_Control)

El equipo que actúa como firewall está basado en una distribución linux debian y para su configuración como firewall vamos a utilizar IPTABLES.
El perímetro de seguridad a configurar se apoya en los siguientes supuestos:

1. Se habilita la inspección de estado
2. La política por defecto de las comunicaciones de entrada y salida hacia el firewall o de atravesarlo se establece a DENEGADO
3. Solo está permitida conexión de entrada al firewall para su gestión a través de una conexión ssh desde la red Control y únicamente desde el equipo del Ingeniero (192.168.4.10)
4. El equipo HMI/HIST (192.168.4.5) puede conectar por SSH con el Histórico Replicado de la red de INTERCAMBIO
5. El equipo del Ingeniero puede acceder por SSH al servidor Histórico Replicado
6. Se permite realizar un PING al firewall desde todas sus tarjetas de red
7. Se permite realizar un PING a través del firewall entre todas sus tarjetas de red

Configuración de reglas iptables para el cumplimiento de la política definida

```
  GNU nano 3.2                                  firewallcontrol

# Generated by xtables-save v1.8.2 on Mon May  9 08:55:23 2022
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]    2
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT 1
-A INPUT -s 192.168.4.10/32 -p tcp -m tcp --dport 22 -j ACCEPT 3
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT 6
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT 1
-A FORWARD -p icmp -m icmp --icmp-type 8 -j ACCEPT 7
-A FORWARD -s 192.168.4.10/32 -d 192.168.3.10/32 -p tcp --dport 22 -j ACCEPT 5
-A FORWARD -s 192.168.4.5/32 -d 192.168.3.10/32 -p tcp --dport 22 -j ACCEPT 4
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT 1
COMMIT
# Completed on Mon May  9 08:55:23 2022
```

Regla enrutado para llegar a la red CAMPO

```
root@FWCTL:~# ip route add 192.168.5.0/24 via 192.168.4.254 dev ens224
```

Reglas filtrado en el Firewall (FW_Campo)

El equipo que actúa como firewall está basado en una distribución linux debian y para su configuración como firewall vamos a utilizar IPTABLES.
El perímetro de seguridad a configurar se apoya en los siguientes supuestos:

1. Se habilita la inspección de estado
2. La política por defecto de las comunicaciones de entrada y salida hacia el firewall o de atravesarlo se establece a DENEGADO
3. Solo está permitida conexión de entrada al firewall para su gestión a través de una conexión ssh desde el equipo del Ingeniero (192.168.4.10)
4. El equipo HMI/HIST puede conectar con el protocolo MODBUS con los PLC's
5. El equipo del Ingeniero puede acceder por SSH a los PLC's
6. Se permite realizar un PING al firewall desde todas sus tarjetas de red
7. Se permite realizar un PING a través del firewall entre todas sus tarjetas de red

Configuración de reglas iptables para el cumplimiento de la política definida

```
  GNU nano 3.2                                  FW_CAMPO

# Generated by xtables-save v1.8.2 on Mon May  9 08:48:14 2022
*filter
:INPUT DROP [0:0]     2
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT  1
-A INPUT -s 192.168.4.10/32 -p tcp -m tcp --dport 22 -j ACCEPT  3
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT  6
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT  1
-A FORWARD -s 192.168.4.10/32 -d 192.168.5.0/24 -p tcp -m tcp --dport 22 -j ACCEPT  5
-A FORWARD -s 192.168.4.5/32 -d 192.168.5.0/24 -p tcp -m tcp --dport 502 -j ACCEPT  4
-A FORWARD -p icmp -m icmp --icmp-type 8 -j ACCEPT  7
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT  1
COMMIT
# Completed on Mon May  9 08:48:14 2022
```

Instalación y configuración de software

Equipos en la red de campo

Sobre una distribución Linux Debian, los equipos de la red de campo van a actuar a modo de PLC's simulando tener conectado algunos sensores de temperatura y humedad.
El PLC se comunica mediante protocolo MODBUS con el equipo HMI/Histórico de la red de CONTROL

El software que vamos a utilizar para trabajar con el protocolo MODBUS son diagslave y modpoll.

Diagslave configura nuestro equipo como un "esclavo" modbus que conectará posteriormente con el equipo HMI actuando como "maestro" modbus.
Modpoll permite comprobar la lectura de los registros modbus (actuando como un "maestro")

Instalación del software

conectamos como root al equipo y creamos el directorio "modbus"

#mkdir modbus

Cambiamos al directorio modbus y desde allí procedemos a la descarga del software

cd modbus
wget https://www.modbusdriver.com/downloads/modpoll.tgz
wget https://www.modbusdriver.com/downloads/diagslave.tgz

Descomprimimos los ficheros

tar -xf diagslave.tgz
tar -xf modpoll.tgz
Cambiamos el nombre a las carpetas recién creadas (modpoll, diagslave) tras descomprimir los ficheros

mv diagslave DiagSlave
mv modpoll ModPoll

Cambiamos a la carpeta /modbus/DiagSlave/x86_64-linux-gnu

cd /modbus/DiagSlave/x86_64-linux-gnu

Copiamos desde esta carpeta (DiagSlave) ,el fichero diagslave a la carpeta /modbus

```
root@PLC1:~/modbus/DiagSlave/x86_64-linux-gnu# ls -l
total 1000
-rwxr-xr-x 1 root root 1021432 abr 14  2021 diagslave
root@PLC1:~/modbus/DiagSlave/x86_64-linux-gnu# cp diagslave ../../diagslave
```

Realizamos el mismo procedimiento desde la carpeta ModPoll

```
root@PLC1:~/modbus/ModPoll/x86_64-linux-gnu# ls -l
total 1012
-rwxr-xr-x 1 root root 1033656 abr 13  2021 modpoll
root@PLC1:~/modbus/ModPoll/x86_64-linux-gnu# cp modpoll ../../modpoll
```

Creamos los scripts:
mbstart → Iniciar el proceso modbus
mbstop → detener el proceso modbus
mbw → simular y grabar en los registros modbus datos simulados de sensorica
mbpoll → leer los registros modbus

```
root@PLC1:~/modbus# ls -l
total 2032
-rwxr--r-- 1 root root 1021432 may 23  2022 diagslave
-rwxr--r-- 1 root root      47 may 23  2022 mbpoll
-rwxr--r-- 1 root root      77 may 31  2022 mbstart
-rwxr--r-- 1 root root     100 may 31  2022 mbstop
-rwxr--r-- 1 root root     154 may 30  2022 mbw
-rwxr--r-- 1 root root 1033656 may 23  2022 modpoll
drwxr-xr-x 4 root root    4096 ene 17 19:50 temp
root@PLC1:~/modbus#
```

Contenido de los scripts

mbw

```
root@PLC1:~/modbus# cat mbw
#!/bin/bash
./modpoll -r 100 127.0.0.1 `shuf -i 0-50 -n1`  graba 1 registro (n1) a partir de la pos 100 (r100) un valor aleatorio (shuf) entre 0-50
./modpoll -r 101 127.0.0.1 `shuf -i 0-100 -n1` graba 1 registro (n1) a partir de la pos 101 (r101) un valor aleatorio (shuf) entre 0-100
./modpoll -r 102 127.0.0.1 `shuf -i 0-1200 -n1`graba 1 registro (n1) a partir de la pos 102 (r102) un valor aleatorio (shuf) entre 0-50
```

mbstart

```
root@PLC1:~/modbus# cat mbstart
#!/bin/bash
./diagslave -m tcp &>/dev/null &  Iniciar en segundo plano protocolo modbus en modo esclavo TCP
watch -n 10 ./mbw &>/dev/null &   Programa cada 10sg la grabación de datos en los registros modbus
root@PLC1:~/modbus#
```

mbstop

```
root@PLC1:~/modbus# cat mbstop
#!/bin/bash
kill -9 `ps | grep watch | cut -d"p" -f1`     Encuentra el numero de proceso asociado a "watch" y lo detiene
kill -9 `ps | grep diagslave | cut -d"p" -f1`Encuentra el número de proceso asociado a "diagslave" y lo detiene
root@PLC1:~/modbus#
```

mbpoll

```
root@PLC1:~/modbus# cat mbpoll
#!/bin/bash
./modpoll -r 100 -c 3 -l 10000  $1   Mostrar cada 10 sg(-l 10000) el valor registrado en 3 registros consecutivos
root@PLC1:~/modbus#                  (-c 3) a partir de la posición 100 (-r 100)
```

Ejemplo de ejecución scripts modbus

```
root@PLC1:~/modbus# ls
diagslave  mbpoll  mbstart  mbstop  mbw  modpoll  temp
root@PLC1:~/modbus# ./mbstart
root@PLC1:~/modbus# ./mbpoll 127.0.0.1
modpoll 3.10 - FieldTalk(tm) Modbus(R) Master Simulator
Copyright (c) 2002-2021 proconX Pty Ltd
Visit https://www.modbusdriver.com for Modbus libraries and tools.

Protocol configuration: MODBUS/TCP, FC3
Slave configuration...: address = 1, start reference = 100, count = 3
Communication.........: 127.0.0.1, port 502, t/o 1.00 s, poll rate 10000 ms
Data type.............: 16-bit register, output (holding) register table

-- Polling slave... (Ctrl-C to stop)
[100]: 37
[101]: 28
[102]: 950
-- Polling slave... (Ctrl-C to stop)

root@PLC1:~/modbus# ./mbstop
root@PLC1:~/modbus# ./mbpoll 127.0.0.1
modpoll 3.10 - FieldTalk(tm) Modbus(R) Master Simulator
Copyright (c) 2002-2021 proconX Pty Ltd
Visit https://www.modbusdriver.com for Modbus libraries and tools.

Protocol configuration: MODBUS/TCP, FC3
Slave configuration...: address = 1, start reference = 100, count = 3
Communication.........: 127.0.0.1, port 502, t/o 1.00 s, poll rate 10000 ms
Data type.............: 16-bit register, output (holding) register table

Can't reach server/slave! Check TCP/IP and firewall settings.
root@PLC1:~/modbus#
```

Reglas de filtrado de equipo

Como medida de seguridad en profundidad, además de disponer de un firewall de perímetro (FW_CONTROL) podemos aplicar reglas de filtrado con IPTABLES.
De esta forma en caso de un error o incorrecta configuración del firewall de perímetro podemos contar con medidas de seguridad adicionales complementarias.

En estos equipos solo es necesario configurar las cadenas de INPUT/OUTPUT ya que al contar únicamente con una sola tarjeta de red no hay tráfico de FORWARD.

La política de seguridad adecuada es:

1. Se habilita la inspección de estado
2. La política por defecto de las comunicaciones de entrada y salida hacia el firewall o de atravesarlo se establece a DENEGADO
3. El equipo HMI/HIST puede conectar con el protocolo MODBUS con los PLC's
4. El equipo del Ingeniero puede acceder por SSH a los PLC's
5. Se permite realizar un PING al equipo.

```
  GNU nano 3.2                          fwplc1

# Generated by xtables-save v1.8.2 on Wed Jan 18 09:32:54 2023
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]  2
:OUTPUT DROP [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT  1
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT  5
-A INPUT -s 192.168.4.10/32 -p tcp -m tcp --dport 22 -j ACCEPT  4
-A INPUT -s 192.168.4.5/32 -p tcp -m tcp --dport 502 -j ACCEPT  3
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT 1
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT  1
COMMIT
# Completed on Wed Jan 18 09:32:54 2023
```

Equipos en la red CONTROL

En la red de control se instalarán dos equipos, el HMI/Histórico y el equipo de Ingeniero (que accederá al HMI)

HMI

Recoge los datos de los PLC vía MODBUS, los presenta en formato HMI y los almacena en un fichero HISTÓRICO para su posterior análisis.
Basado en una distribución Linux (Debian) debemos instalar el software NODE-RED, si bien como requisito previo requiere la instalación de NODE-JS.

Instalación y configuración del software

Instalamos node-js

Como referencia podemos consultar la página de NodeSource
https://github.com/nodesource/distributions/blob/master/README.md

En nuestro ejemplo instalamos node-js para una distribución Linux

```
curl -fsSL https://deb.nodesource.com/setup_18.x | bash - &&\
apt-get install -y nodejs
```

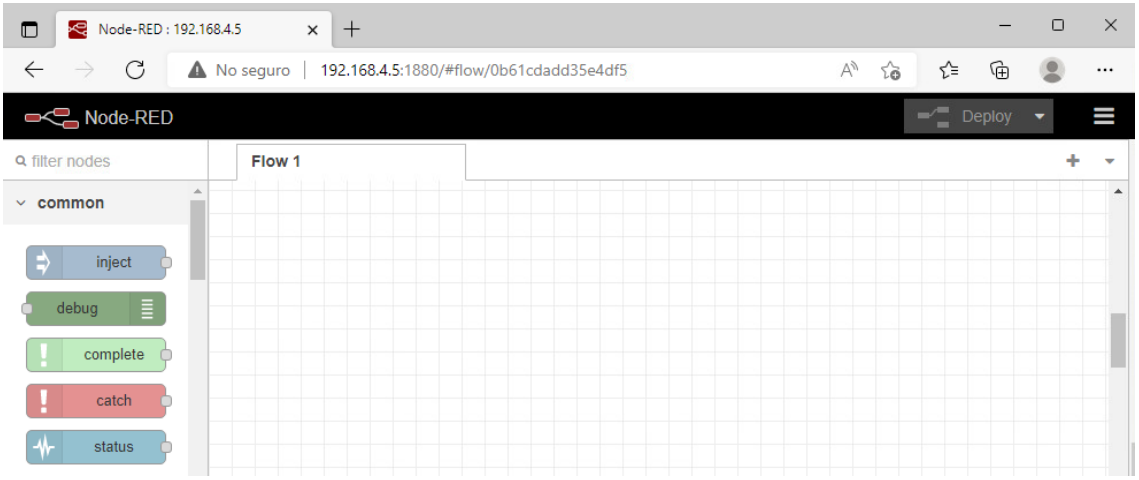
A continuación instalamos node-red que nos permitirá de manera gráfica y mediante programación de bloques habilitar el protocolo MODBUS, las funciones de HMI, Histórico, …

npm install -g - -unsafe-perm node-red

Arrancamos **node-red**

```
root@hmihistorico:~# node-red
18 Jan 10:01:42 - [info]

Welcome to Node-RED
===================

18 Jan 10:01:42 - [info] Node-RED version: v2.2.2
18 Jan 10:01:42 - [info] Node.js  version: v18.2.0
18 Jan 10:01:42 - [info] Linux 4.19.0-8-amd64 x64 LE
18 Jan 10:01:42 - [info] Loading palette nodes
18 Jan 10:01:43 - [info] Dashboard version 3.1.7 started at /ui
18 Jan 10:01:43 - [info] Settings file  : /root/.node-red/settings.js
18 Jan 10:01:43 - [info] Context store  : 'default' [module=memory]
18 Jan 10:01:43 - [info] User directory : /root/.node-red
18 Jan 10:01:43 - [warn] Projects disabled : editorTheme.projects.enabled=false
18 Jan 10:01:43 - [info] Flows file     : /root/.node-red/flows.json
18 Jan 10:01:43 - [info] Server now running at http://127.0.0.1:1880/
18 Jan 10:01:43 - [warn]

---------------------------------------------------------------------
Your flow credentials file is encrypted using a system-generated key.

If the system-generated key is lost for any reason, your credentials
file will not be recoverable, you will have to delete it and re-enter
your credentials.

You should set your own key using the 'credentialSecret' option in
your settings file. Node-RED will then re-encrypt your credentials
file using your chosen key the next time you deploy a change.
---------------------------------------------------------------------
```

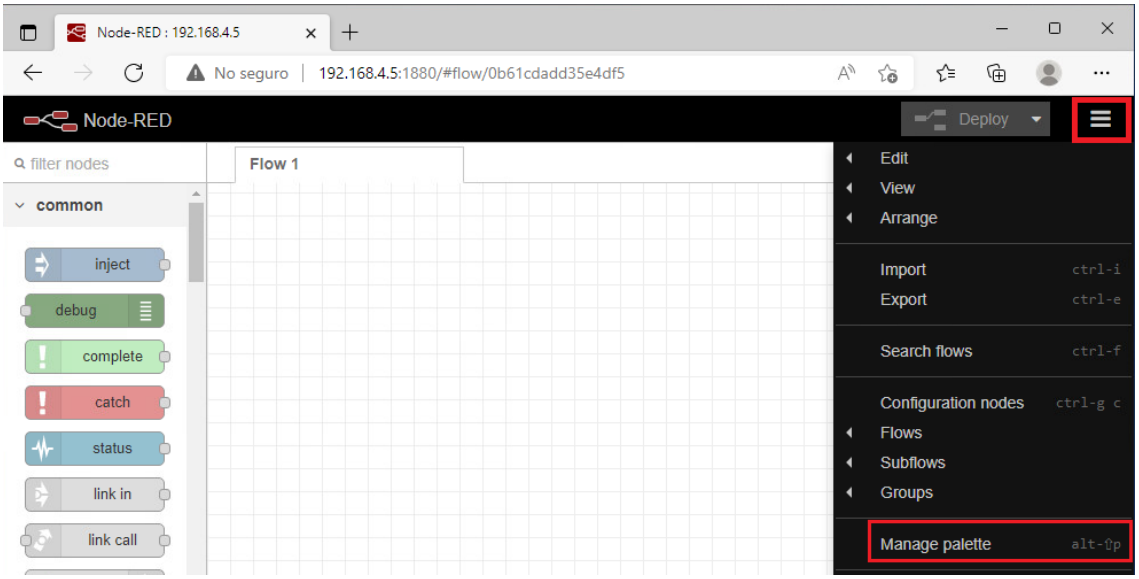
Desde otro equipo accedemos vía web a la IP del equipo puerto 1880



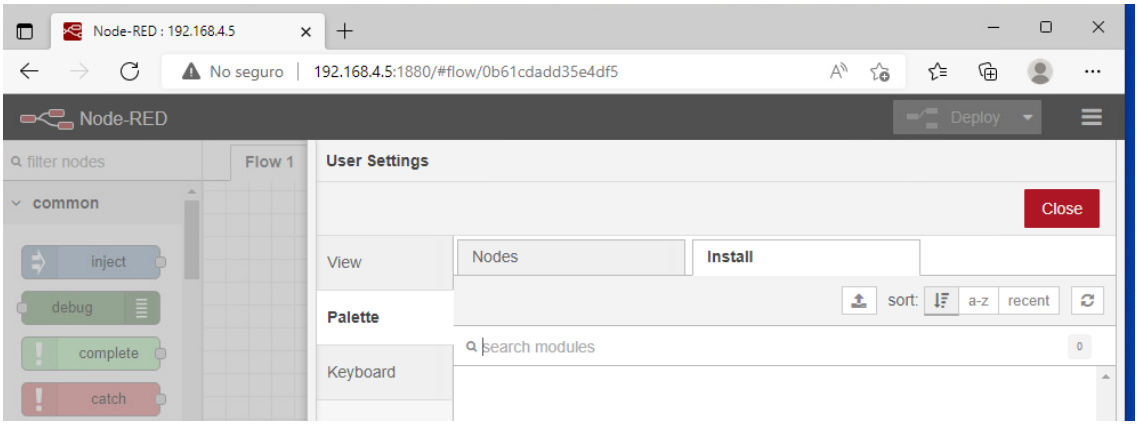
A partir de tener acceso al dashboard de node-red procedemos a instalar los plugins necesarios para trabajar con MODBUS, configurar los “gauges” para la consola HMI, etc.

Los nodos a instalar son node-red-contrib-modbus y node-red-dashboard

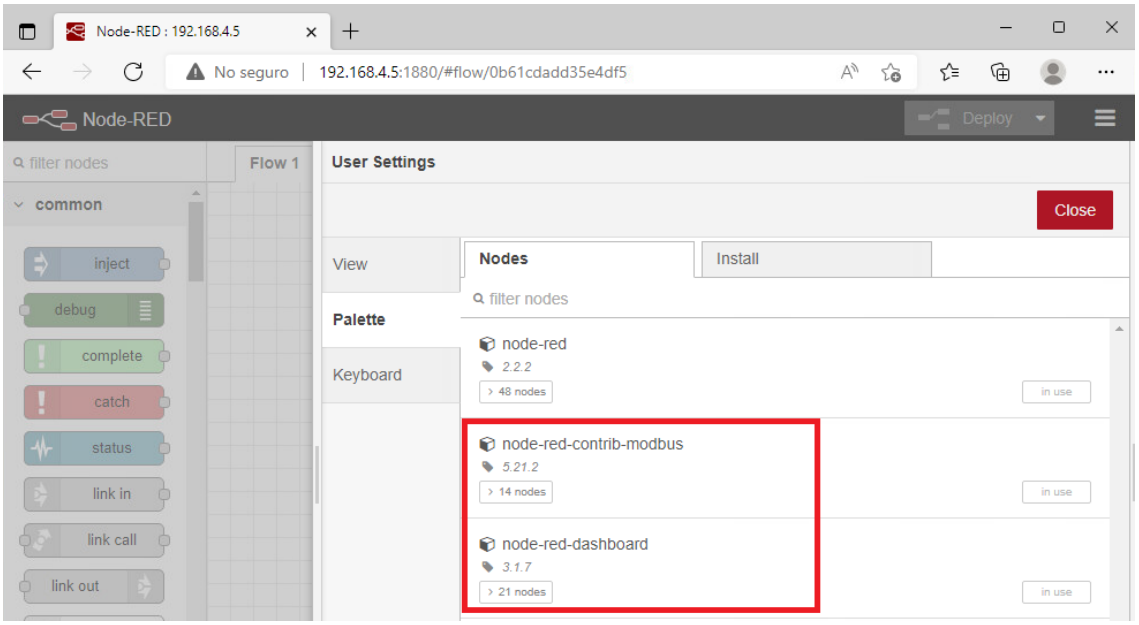
Para ello seleccionamos la opción **manage palette** accesible desde las 3 rayas horizontales de la parte superior derecha



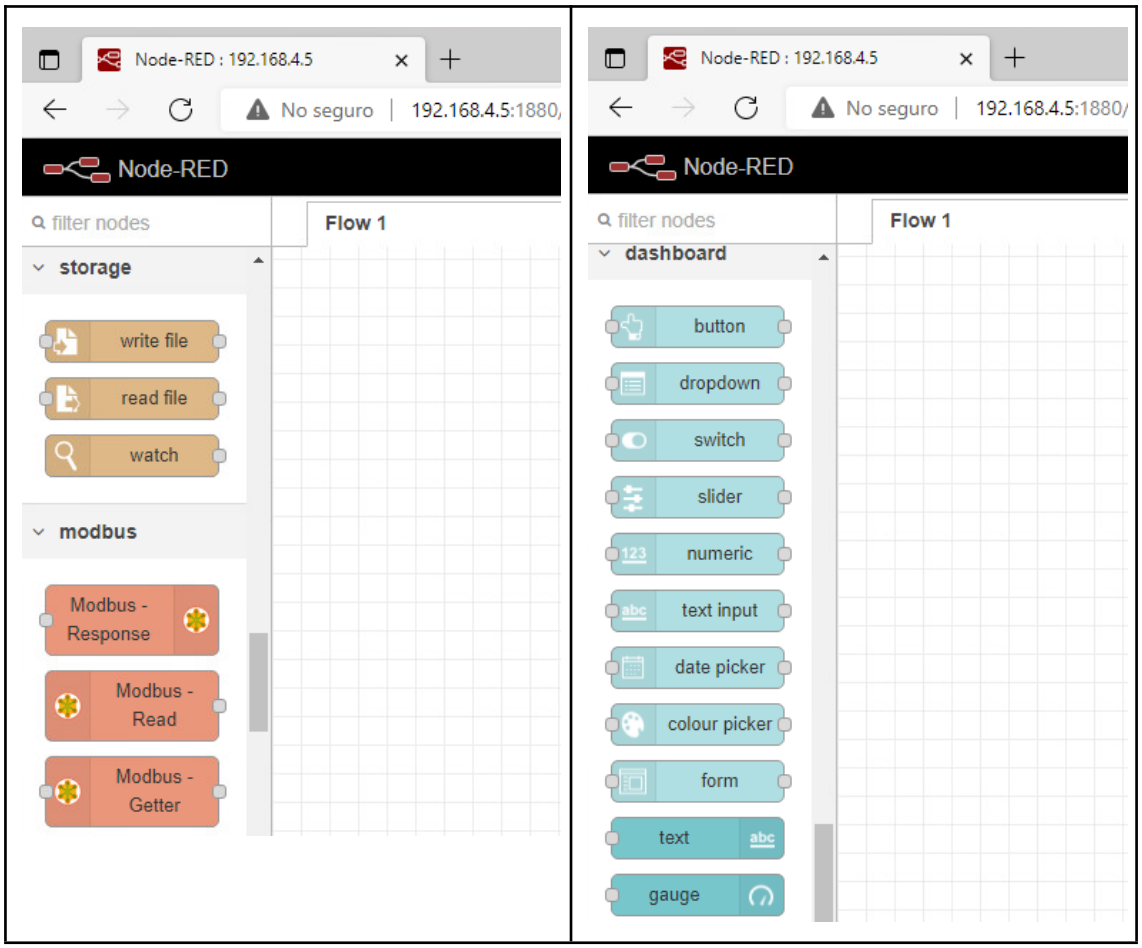
Realizamos la búsqueda de los dos módulos mencionados y los instalamos



Verificamos desde la pestaña Nodes su instalación

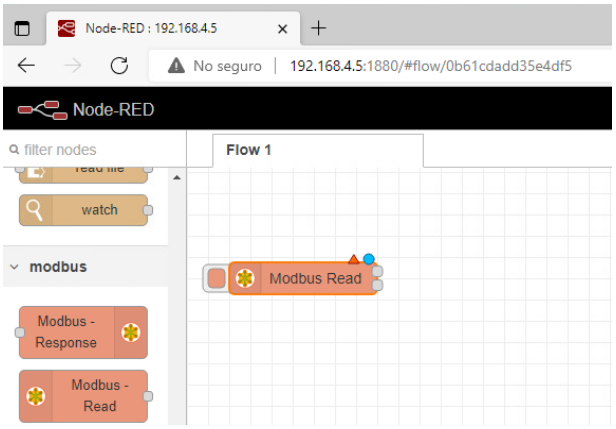


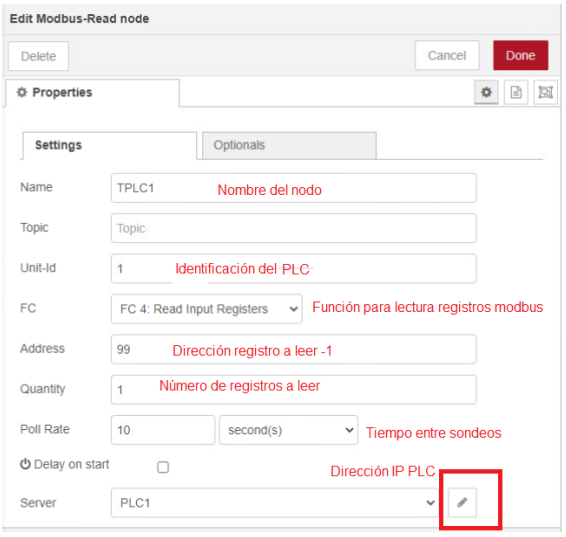
Comprobamos que tenemos acceso a los nuevos nodos desde el menu lateral izquierdo

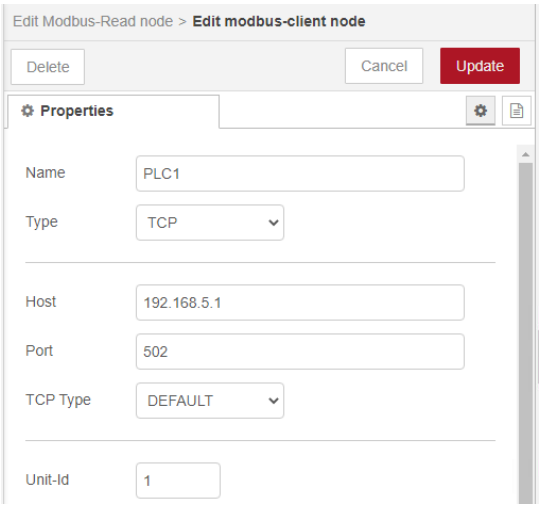


Lectura de los registros del PLC a través de MODBUS

Arrastramos el nodo **Modbus-Read** y editamos sus propiedades haciendo doble click

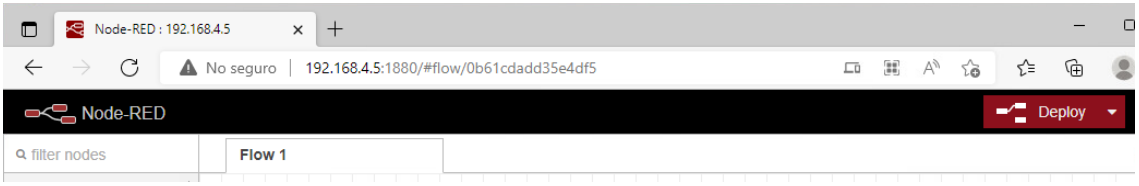




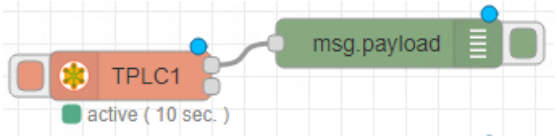


Añadimos un nodo “debug” para visualizar la lectura y lo conectamos a la salida superior del nodo anterior (TPLC1).

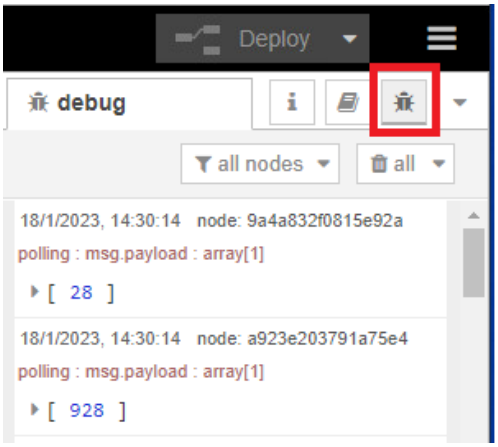
Pulsamos sobre DEPLOY



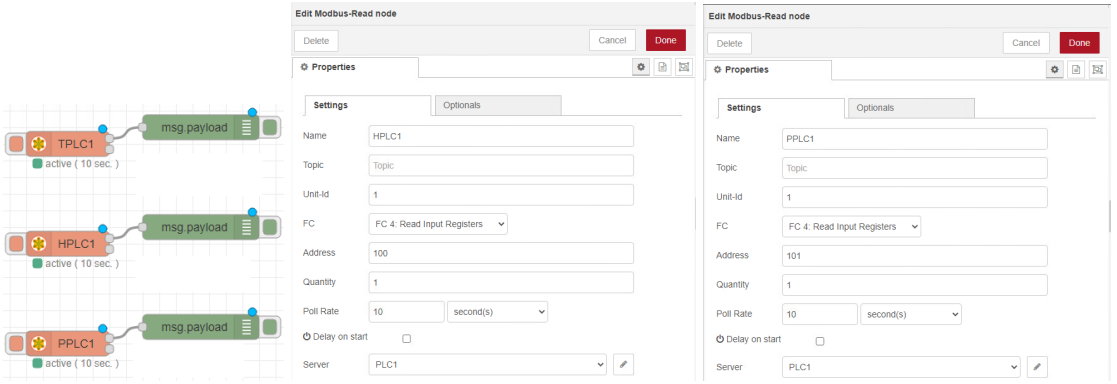
Si la conexión se establece correctamente se muestra el mensaje “active”



Pulsamos sobre el icono “debug” y se van mostrando los datos de lectura del PLC

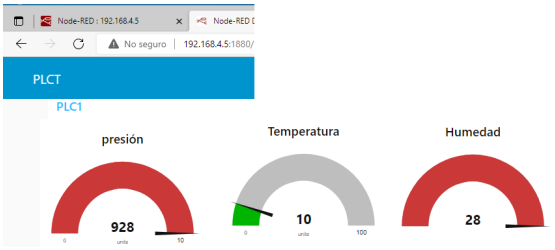


Procedemos de forma similar para la lectura de los registros siguientes, modificando el registro a leer del mismo PLC1



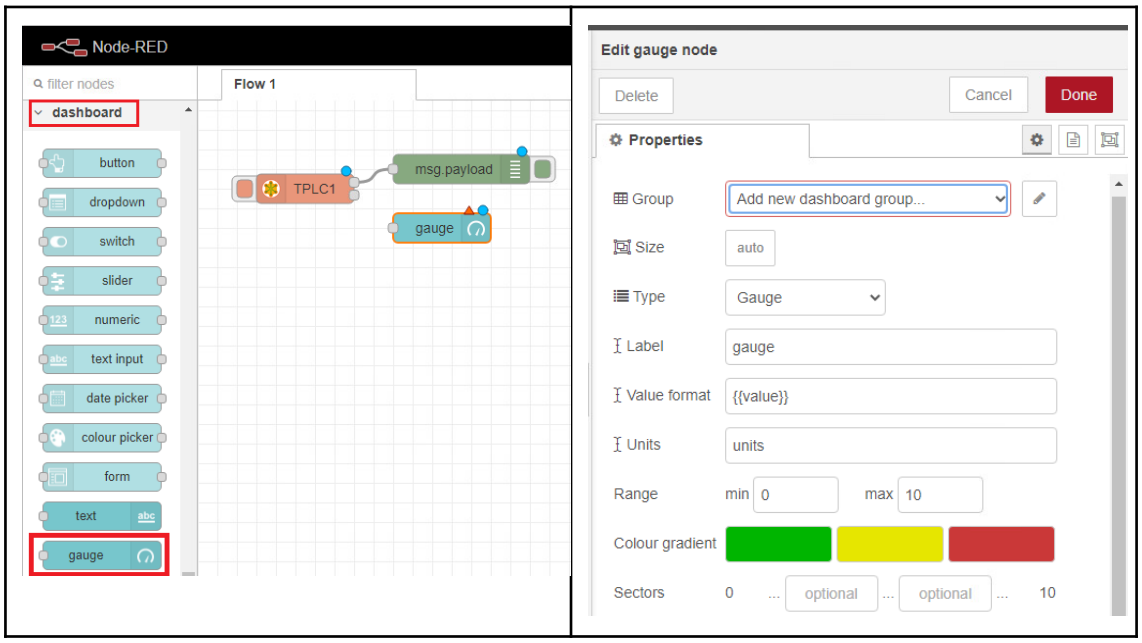
Creación de los “gauges” (HMI)

El objetivo ahora es mostrar los datos recogidos de los registros del PLC1 y mostrarlos en gráficos similares a esta:



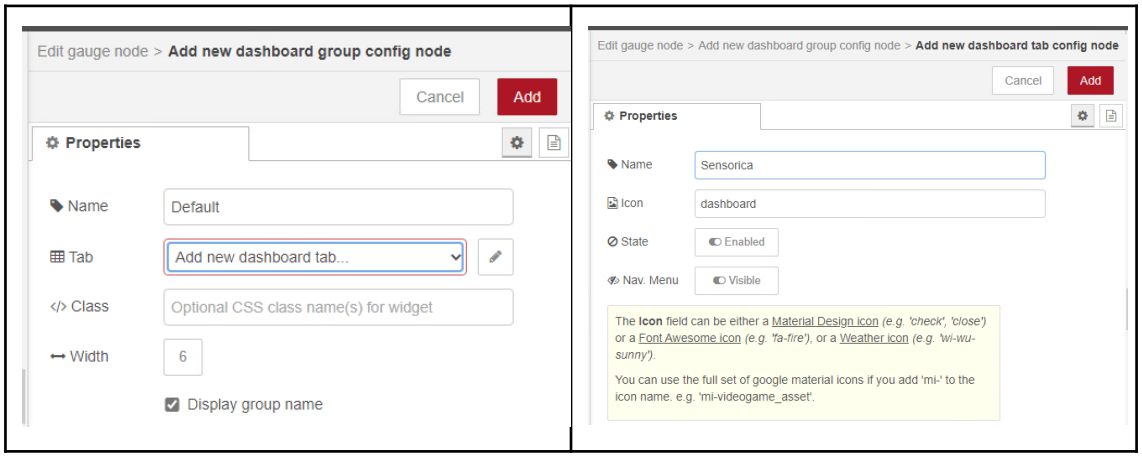
Creación del panel y subpaneles HMI

Desde el panel dashboard seleccionamos el nodo “gauge” y configuramos.

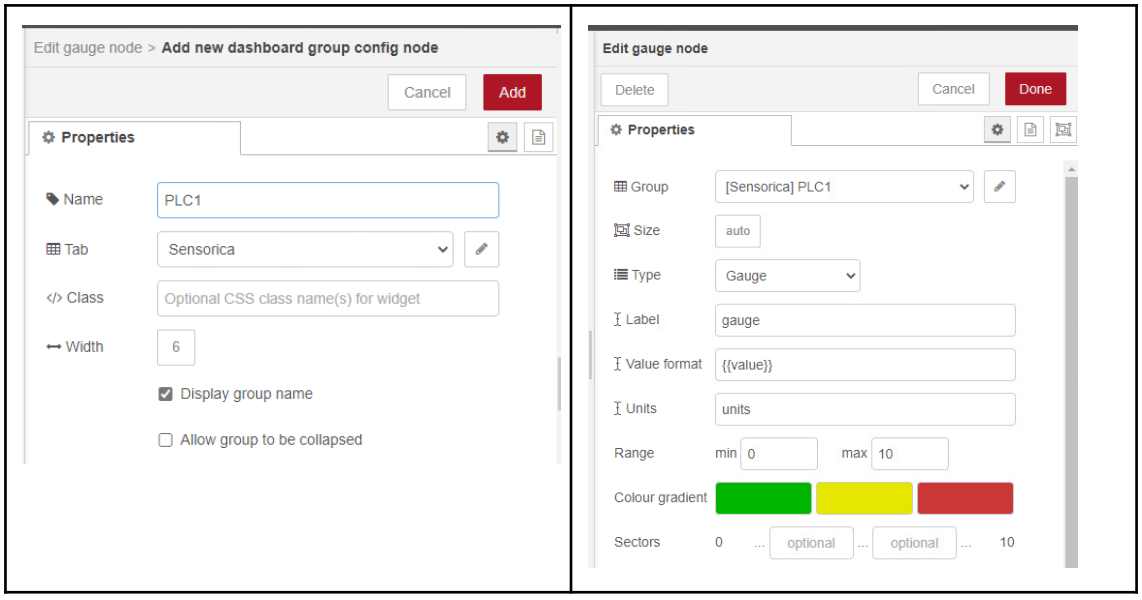


Para la creación del primer “gauge” es necesario crear primero un “dashboard tab” (tablero o panel principal que contendrá todos nuestros gauges)” y dentro de este tablero definir “grupos de gauges” (por ejemplo uno por cada PLC). Para ello debemos proceder como se indica a continuación, teniendo en cuenta que primero debe definirse el “primer grupo” que se ubicara en el “tablero” (es decir en orden inverso), asi:

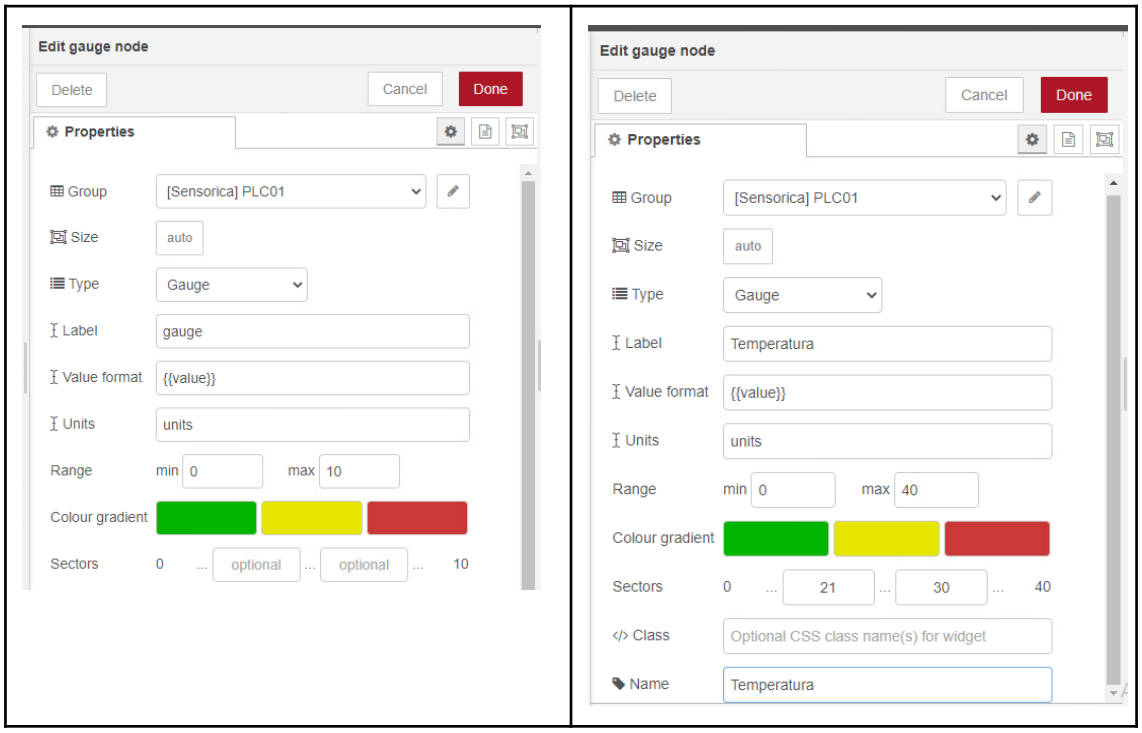
En primer lugar seleccionamos un “nuevo dashboard **grupo**” (su nombre final será “PLC1”) y pulsamos sobre el lapiz (edición) y continuamos seleccionando “nuevo dashboard **tab**” (su nombre será “Sensorica”)



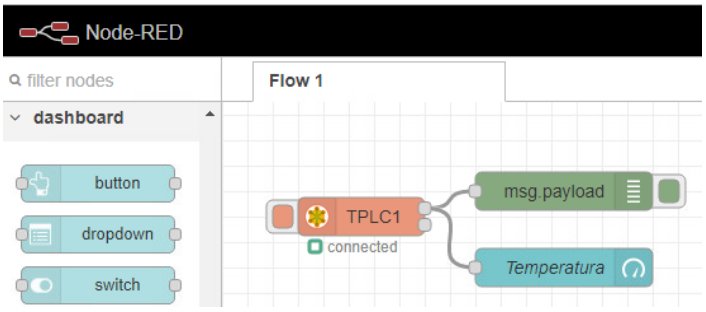
Indicamos el nombre del primer grupo de gauges (PLC01), pulsamos **Add** y **Done**



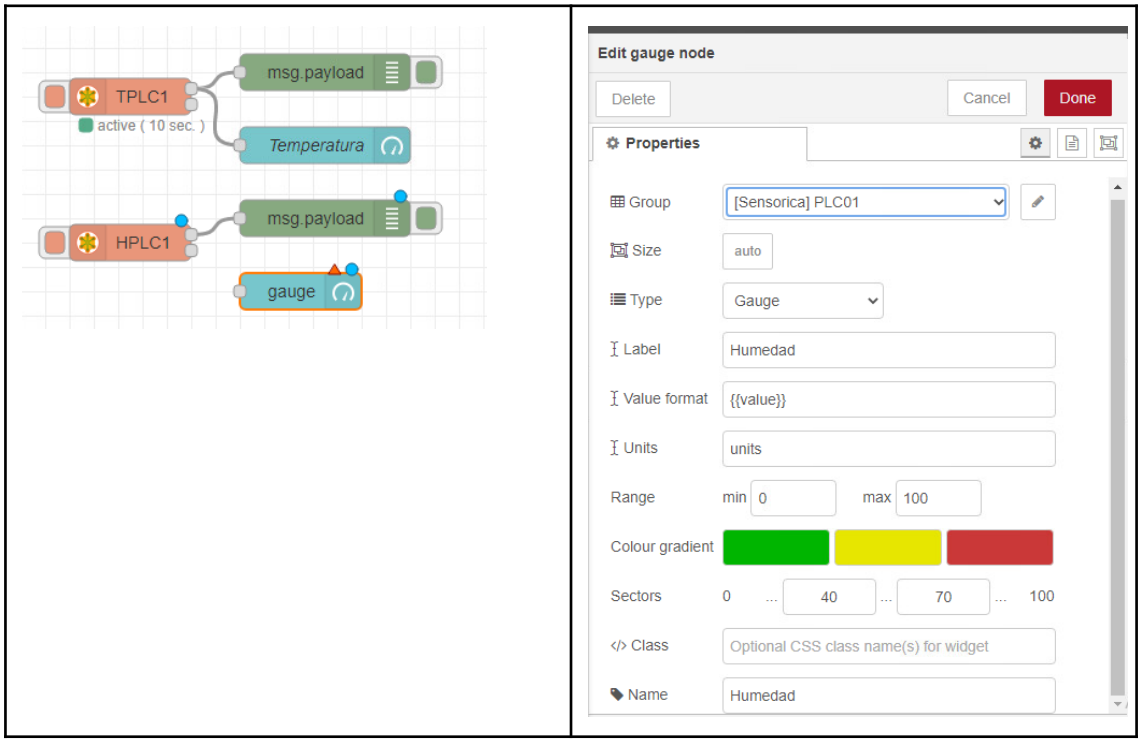
una vez definido, configuramos sus características específicas al sensor



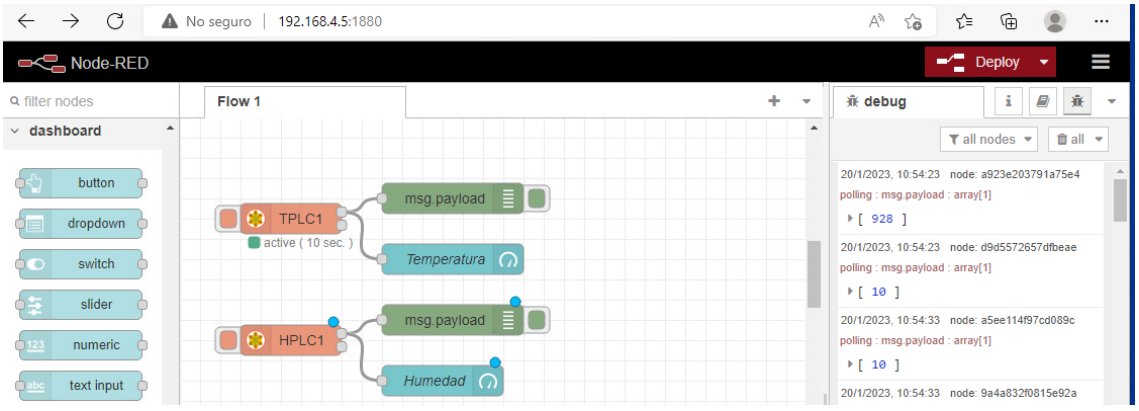
Conectamos el gauge con el nodo modbus asociado al PLC y registro correspondiente al sensor de temperatura (registro 100 del PLC1) creado anteriormente



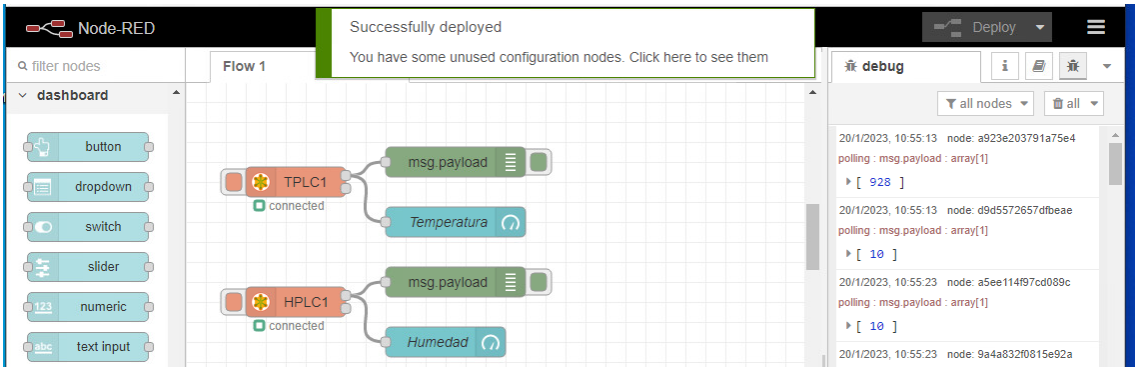
Para el resto de los sensores simulados (humedad, presión atmosférica) se procede de la misma manera, añadiendo un “gauge” para cada uno de ellos.
La diferencia es que a partir de ahora ya tenemos creado el “dashboard tab” (sensorica) y el “dashboard group”(PLC01) donde ubicarlos.



Conectamos el gauge con el node modbus y pulsamos en “Deploy”

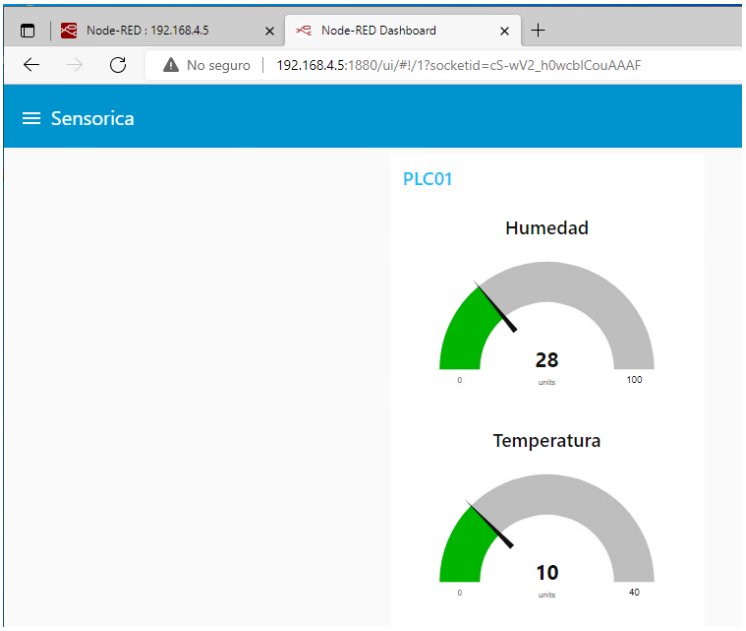


Comprobamos el estado de connected/active



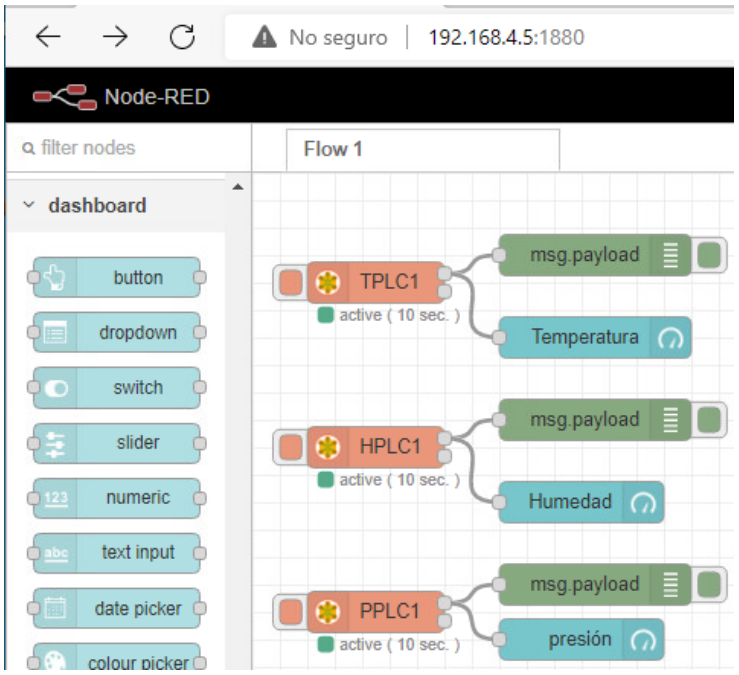
Visualizando el dashboard (HMI)

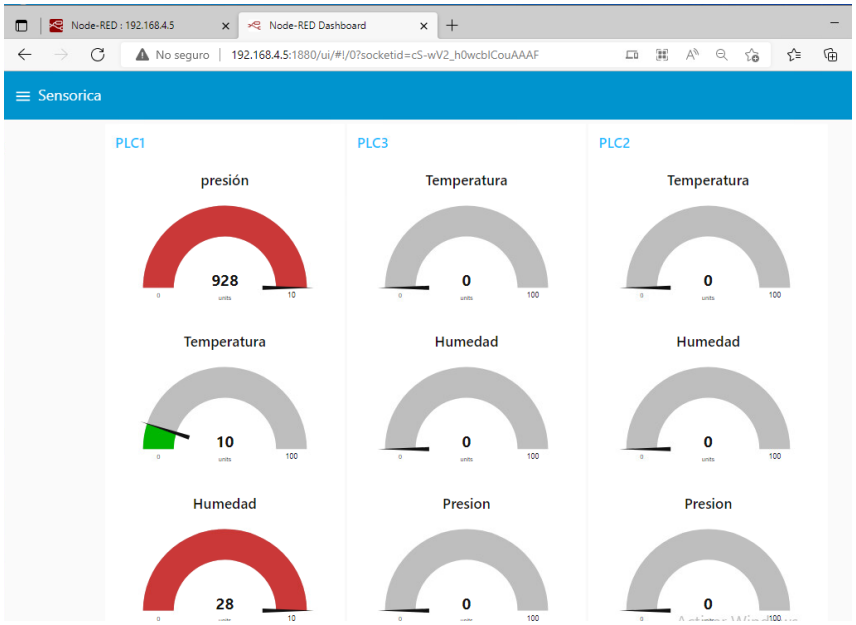
Para visualizar el HMI accedemos a la URL del equipo HMI añadiendo /ui tras el puerto 1880 << **http://192.168.4.5:1880/ui>>** mostrando en tiempo real los valores de ambos sensores



Para añadir información de otros sensores se procedería de la misma manera:

1. Añadir nuevos nodos “modbus read”
2. Vincular los nuevos nodos a un nuevo PLC (otra dirección IP)
3. especificar para cada nodo el registro a leer (desde el 99 al 101)
4. Añadir nuevos gauges, creando un nuevo “dashboard group” (PLC02) dentro del “dashboard tab” (Sensórica) ya creado

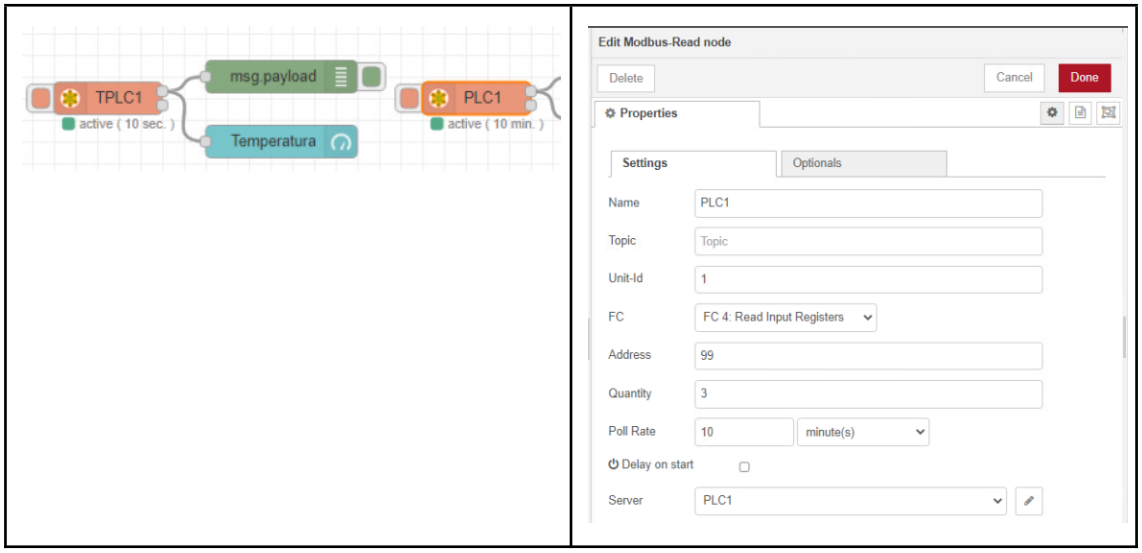




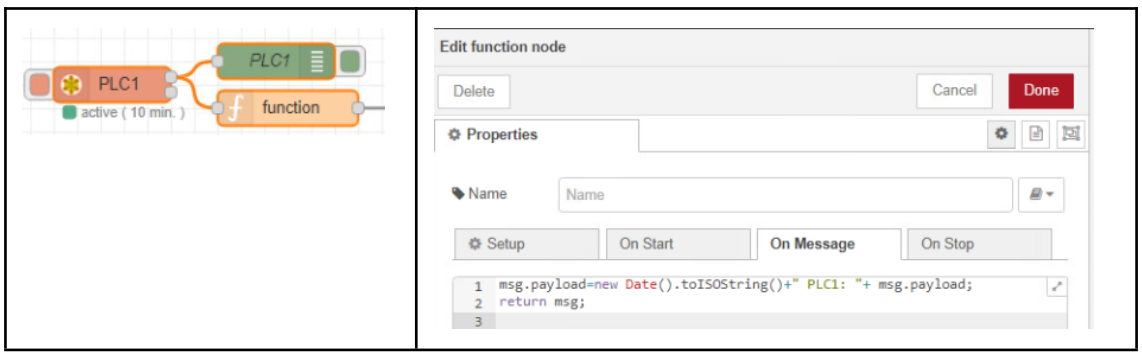
Histórico

Para realizar la función de registro de datos como fichero histórico vamos a programar la recogida simultánea de los 3 sensores (en cada PLC) formateando la salida para que forme una única línea de datos que posteriormente pueda ser grabada secuencialmente sobre un fichero mediante el uso del nodo “write file”.
El proceso a seguir es el siguiente:

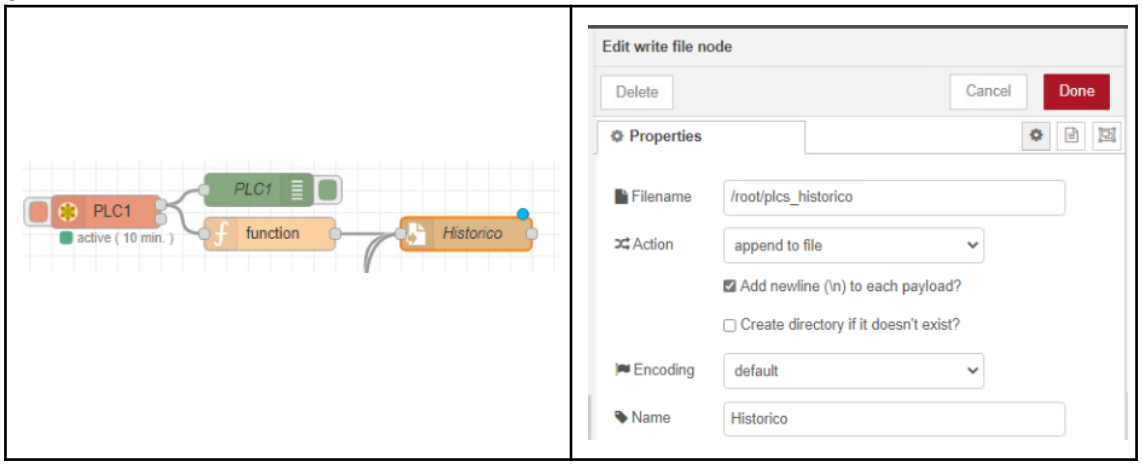
1.Añadimos un nuevo nodo “MODBUS READ” vinculado al PLC1 definido anteriormente sobre el que programamos la lectura de 3 registros (a partir de la posición 99)



2.Añadimos un nodo “function” donde preparamos el formateo de los datos leídos antes de ser grabados sobre el fichero histórico, concatenado la fecha del evento convertida a formato “string” (new Date().toISOString()) con el nombre del PLC (PLC1) y los datos recogidos (msg.payload())



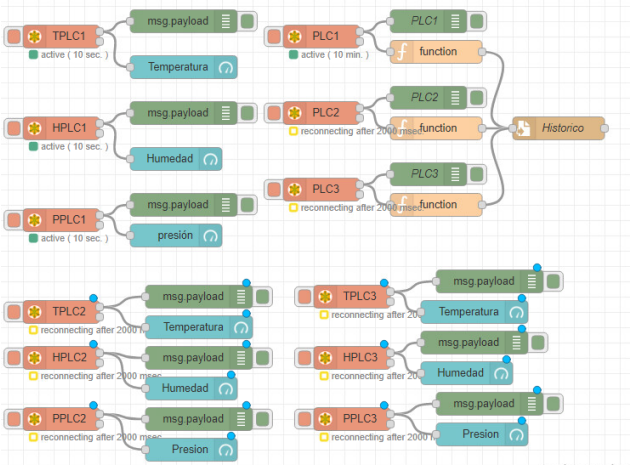
3. Añadimos el nodo “write file” indicando la ruta y nombre del fichero en el que se grabaran los datos así como el formato del proceso (“append to file”)



4.Comprobamos la grabación de los registros visualizando el contenido del fichero

```
C:\Users\W10_Ingeniero>ssh root@192.168.4.5
The authenticity of host '192.168.4.5 (192.168.4.5)' can't be established.
ECDSA key fingerprint is SHA256:OPglAPfFDWyjTNwdbaVDkdxmDY+rdeuY+jkK0O4qnNU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.4.5' (ECDSA) to the list of known hosts.
root@192.168.4.5's password:
Linux hmihistorico 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1+deb10u1 (2020-04-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jan 13 21:50:48 2023
root@hmihistorico:~# tail /root/plcs_historico
2023-01-20T18:00:43.959Z PLC1: 10,28,928
2023-01-20T18:10:43.960Z PLC1: 10,28,928
2023-01-20T18:20:43.960Z PLC1: 10,28,928
2023-01-20T18:30:43.962Z PLC1: 10,28,928
2023-01-20T18:40:43.964Z PLC1: 10,28,928
2023-01-20T18:50:43.964Z PLC1: 10,28,928
2023-01-20T19:00:43.965Z PLC1: 10,28,928
2023-01-20T19:10:43.967Z PLC1: 10,28,928
2023-01-20T19:20:43.967Z PLC1: 10,28,928
2023-01-20T19:30:43.968Z PLC1: 10,28,928
root@hmihistorico:~#
```

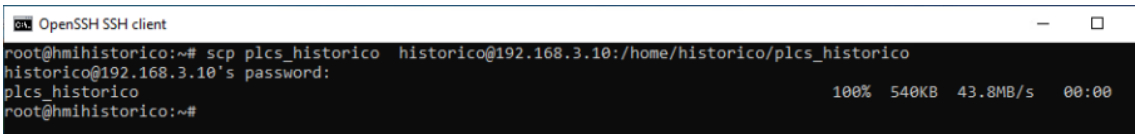
Realizamos el mismo procedimiento con el resto de PLC’s y conectamos la salida al nodo “histórico”



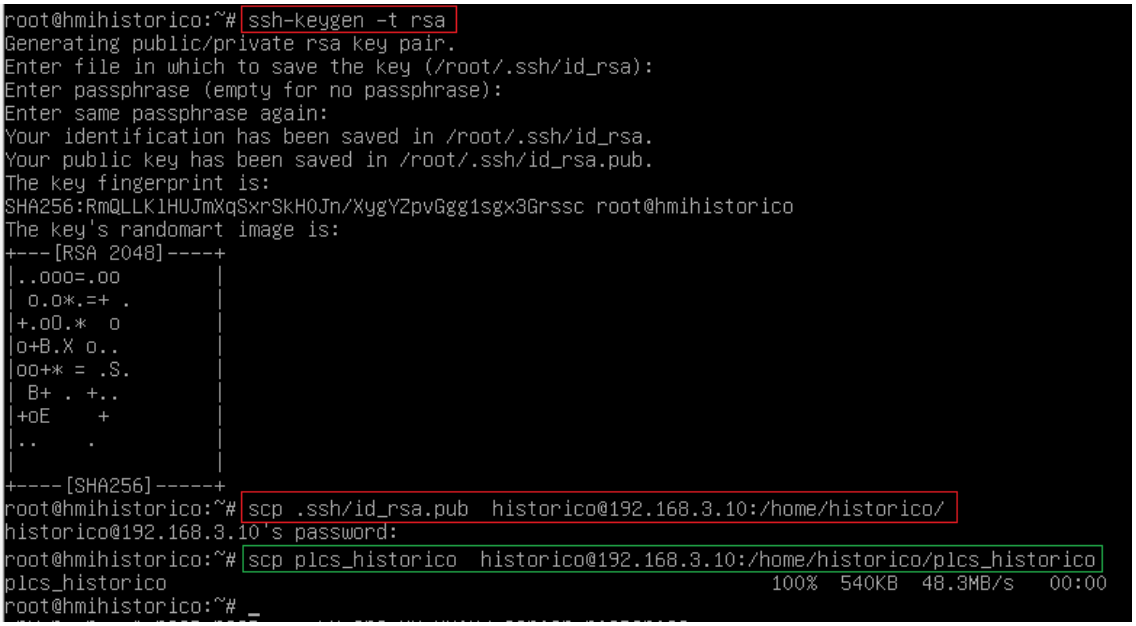
Equipos en la red INTERCAMBIO

Para realizar la función de **Histórico Replicado**, podemos basarnos en cualquier distribución Linux ya que tan solo será necesario habilitar la conexión por SSH para permitir la copia segura programada del fichero "**plcs histórico**" desde el servidor HISTÓRICO mediante el comando "scp"

En el servidor creamos un usuario (en nuestro caso de nombre "histórico").
Desde el equipo HISTÓRICO comprobamos que podemos copiar el fichero con el comando scp al servidor histórico replicado (192.168.3.5)

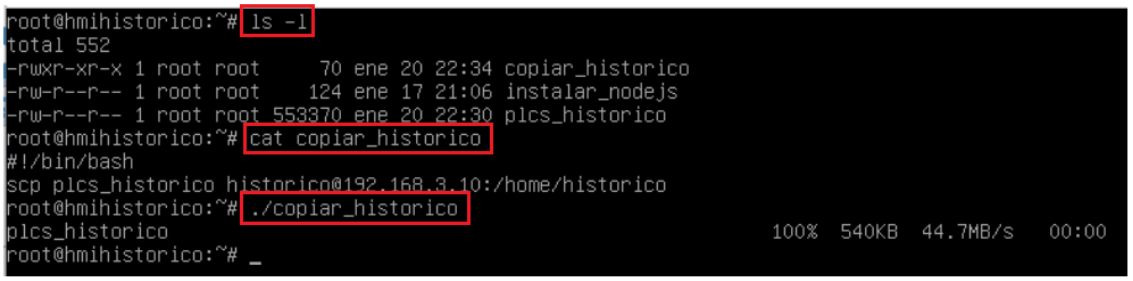


Para evitar el uso de una contraseña en el proceso de copia podemos crear un par de llaves pública/privada para el usuario root del servidor HISTORICO y copiar la llave publica al fichero authorized_keys en el directorio **/home/historico/.ssh** del servidor HISTORICO_REPLICADO

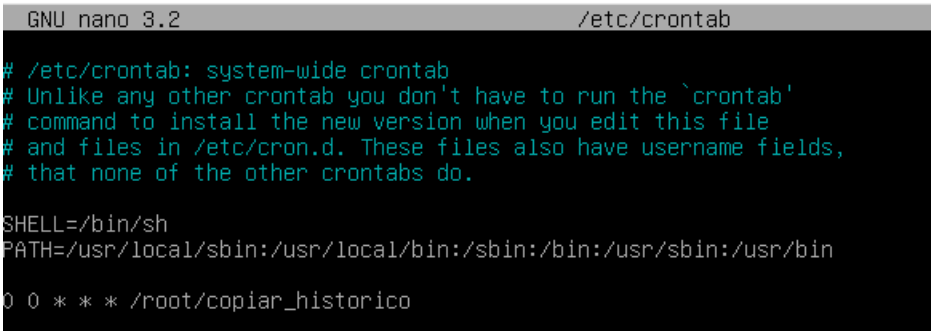


Queda ahora únicamente programar un script para la ejecución del comando “scp anterior” por ejemplo cada hora

Creamos el script (copiar_historico) y comprobamos su funcionamiento



Programamos desde /etc/crontab la ejecución del script anterior cada hora de cada dia



Equipos en la red TI

Si bien en la red TI tenemos dos segmentos de red LAN y DMZ, de cara al objetivo de realizar la integración de las redes de TI/OT en principio solo necesitamos contar con una máquina cliente (por simplificar puede ser la máquina que usa el administrador de TI) para verificar que podemos recibir el fichero plcs_histórico del servidor HISTORICO_REPLICADO ubicado en la red de INTERCAMBIO.
Para el acceso a este fichero podemos proceder de igual manera que la explicada en el caso de la comunicación desde el HMI/Histórico, esto es:

- Crear un par de llaves RSA,(privada y pública)
- Copiar el archivo id_Rsa.pub a la cuenta del usuario del servidor remoto
- Volcar el contenido del archivo id_rsa.pub al fichero authorized_keys del usuario remoto en el servidor de la red INTERCAMBIO donde se encuentra el fichero.

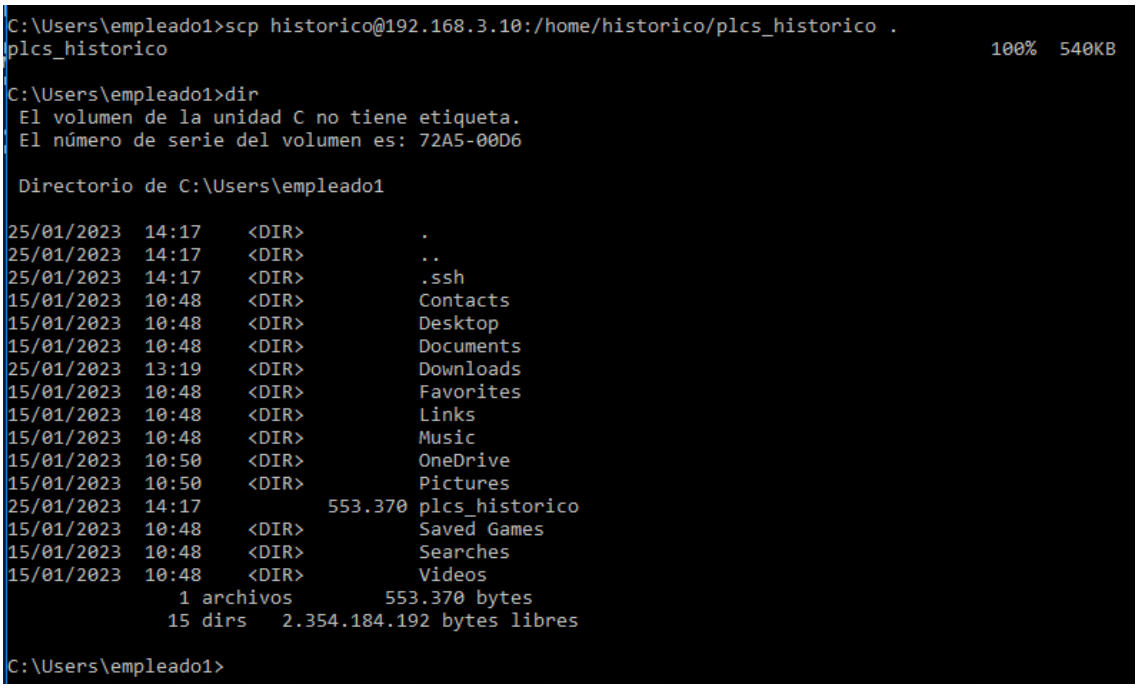
```
C:\Users\empleado1>ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\empleado1/.ssh/id_rsa):
Created directory 'C:\\Users\\empleado1/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\empleado1/.ssh/id_rsa
Your public key has been saved in C:\Users\empleado1/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:IztNPR5NJaC2wYZUT+NXby0KJIjkn3axUCiOu1/4GDA empresas\empleado1@DESKTOP-84PLURO
The key's randomart image is:
+---[RSA 3072]----+
|    ....++ =.. o  |
|    .o.o+ B . + ..|
|    o..o B + o . +|
|   . .. = * = . o |
|  E.  = S + o     |
|  .o o * o o      |
|   .o + . .       |
|  .  = .          |
|   .o .           |
+----[SHA256]-----+
```

```
C:\Users\empleado1\.ssh>scp id_rsa.pub historico@192.168.3.10:/home/historico/id_rsa.pub
historico@192.168.3.10's password:
id_rsa.pub                                                    100%

C:\Users\empleado1\.ssh>
```

HISTORICOreplicado

```
root@historicoreplicado:/home/historico# ls -l
total 548
-rw-r--r-- 1 historico historico    589 ene 25 15:07 id_rsa.pub
-rw-r--r-- 1 historico historico 553370 ene 20 22:33 plcs_historico
root@historicoreplicado:/home/historico# cat id_rsa.pub >> .ssh/authorized_keys
root@historicoreplicado:/home/historico#
```

Una vez realizado el proceso anterior probamos a recoger el fichero plcs_historico



Podemos comprobar como podemos acceder al fichero plcs_historico sin necesidad de identificarnos con usuario y password una vez que hemos creado y copiado nuestra clave pública en el servidor.

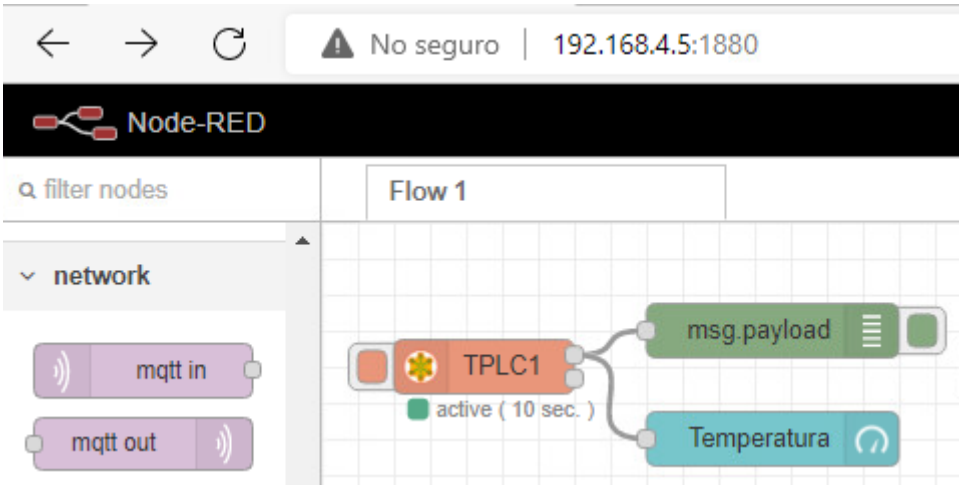
Volcado de las lecturas de los sensores a servidor MQTT

La utilización del protocolo MQTT (Message Queue Telemetry Transport) permite publicar en un servidor (local o en la nueve) los datos emitidos por los sensores y recogidos por el equipo HMI.

Su ventaja es la flexibilidad para poder acceder a las lecturas de los sensores sin la necesidad de tener que estar conectado a la red local donde se están generando. Para ello tan solo es necesario contar con un “cliente MQTT” disponible para todo tipo de plataformas de PC y smartphones y realizar la conexión e identificación contra el servidor en la nube.

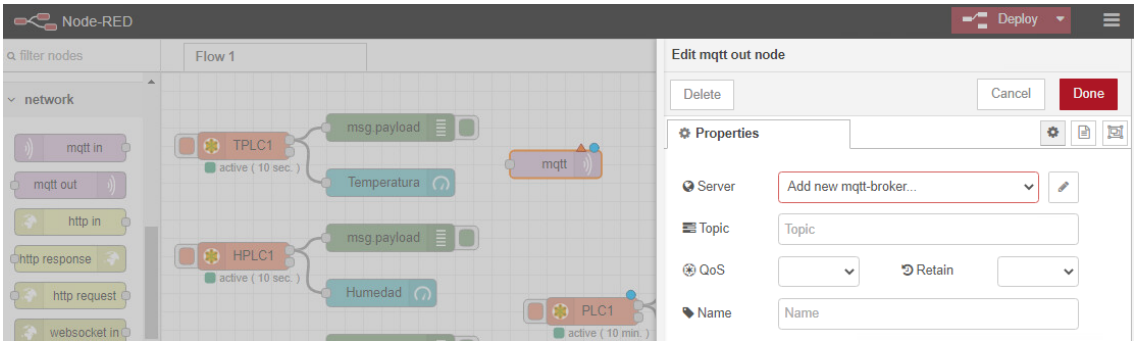
Configuración node-red acceso MQTT

Consultamos los nodos disponibles para MQTT

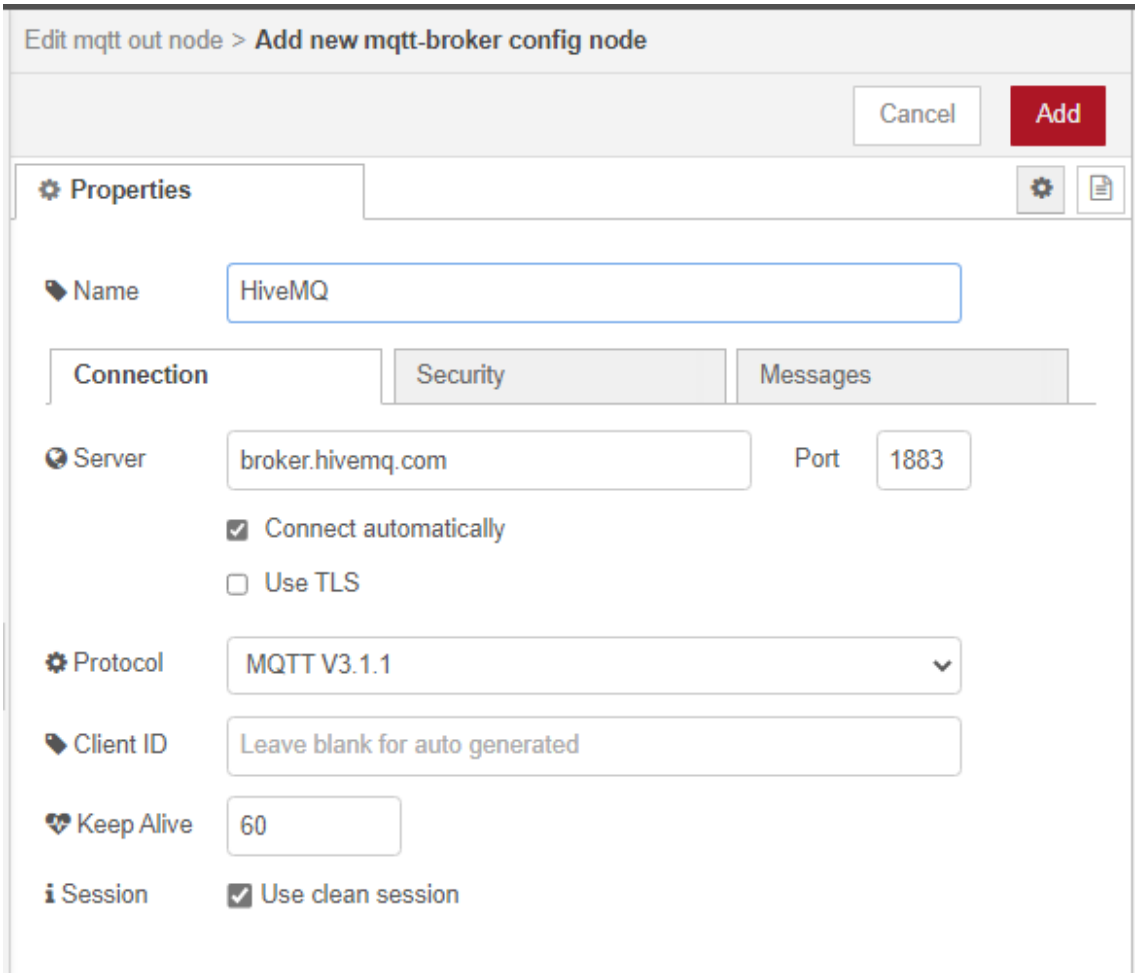


Con el nodo “mqtt out” procedemos a grabar los datos y con el nodo “mqtt in” podemos leer los datos registrados en el servidor.

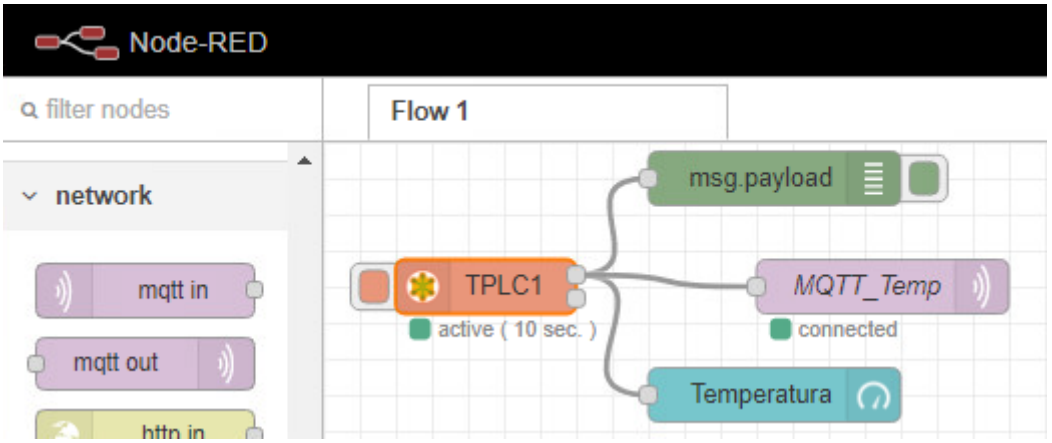
Añadimos un nodo mqtt out y configuramos



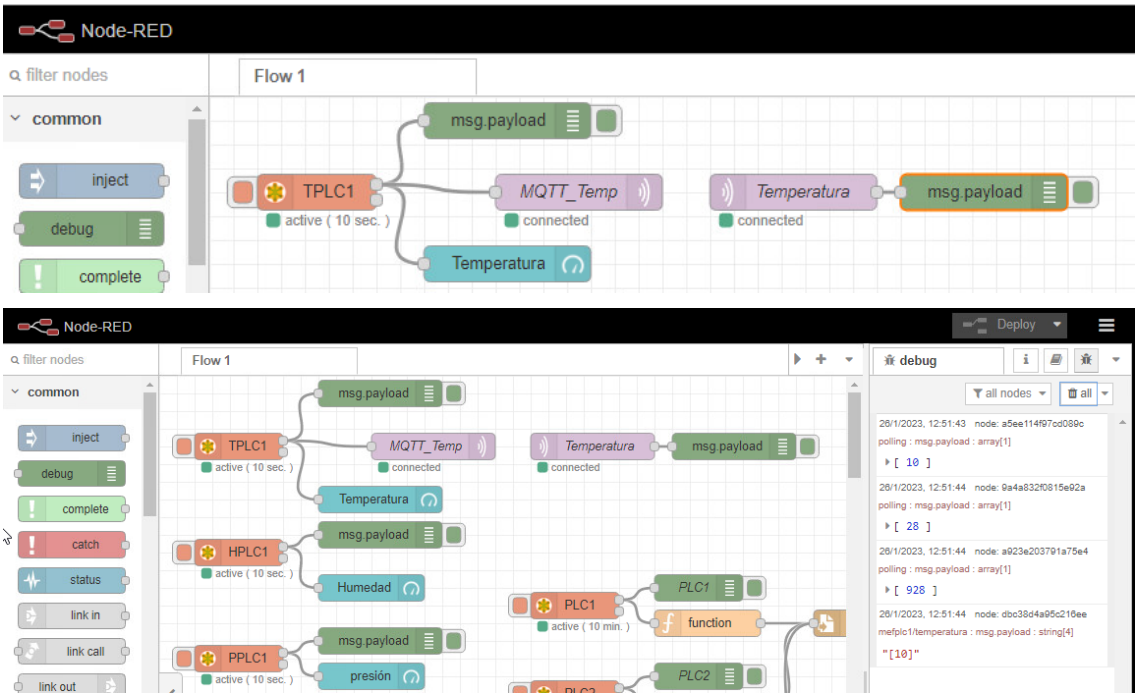
Añadimos la información del broker (en nuestro caso usaremos el broker público “broker.hivemq.com”



Conectamos el nodo a la salida del nodo “temperatura” del TPLC1”



Una vez verificado que hay conectividad (mensaje “connected”) podemos comprobar primero con el nodo “mqtt in” si está enviando los datos correctamente y si es posible su consulta.



Se observa en la última línea de Deploy como la temperatura [10] se muestra tanto en la salida del primer msg.payload cómo en el último que indica que se está obteniendo desde el servidor MQTT con el “topic” → mefplc1/temperatura

Si configuramos cualquier smartphone con un cliente MQTT (como (IotMQTT) podemos acceder igualmente a este dato.

Guía didáctica creada en el marco del Proyecto Industria 4.0

Socios del proyecto:

Centro de estudios AEG ARROKA S.L

Muévete Gestión Integral S.L.

CES S. Ramón y Cajal

Titanium Industrial Security

HORINTEG Soluciones Tecnológicas, S.L.

"Financiado por el Ministerio de Educación y Formación Profesional – U.E. – Next Generation"