Diagnóstico de vulnerabilidades de seguridad en un prototipo de red OT

Luis Fernando Miranda Ordoñez

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Ingeniería en Automática industrial
Popayán, septiembre de 2019

Diagnóstico de vulnerabilidades de seguridad en un prototipo de red OT

Luis Fernando Miranda Ordoñez

Trabajo de grado como requisito para optar al título de Ingeniero en Automática Industrial

Asesor de la empresa: Ing. Iván Darío Arenas Mejía
Director: Msc. Andrea Enríquez Zúñiga
Co-director: Msc. Oscar Amaury Rojas

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Ingeniería en Automática industrial
Popayán, septiembre de 2019

PÁGINA DE ACEPTACIÓN

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____

_____

FIRMA DEL ASESOR ACADEMICO

_____

FIRMA DEL ASESOR DEL PASANTE

Tabla de contenido

Capítulo I 1
1. Introducción 1
1.1. Objetivo general 2
1.2. Objetivos específicos 2
1.3. Contenido 3
Capítulo II 4
2. Marco teórico 4
2.1. Red IT 4
2.2. Red OT 10
2.3. Integración IT y OT 13
2.4. Estándares para seguridad en sistemas de control y automatización industrial 14
2.5. Herramientas para seguridad IT 21
2.6. Herramientas para seguridad OT 22
Capítulo III 24
3. Proceso de desarrollo 24
3.1. Diseño de prototipo de red OT 24
3.2. Implementación de prototipo de red OT 27
Capítulo IV 39
4. Análisis de vulnerabilidades en el prototipo de red OT implementado 39
4.1. Ejecución del funcionamiento normal del sistema 39
4.2. Verificar aprendizaje 40
4.3. Configuración de NOZOMI en modo protección 41
4.4. Realizar cambios sobre el proceso 42
4.5. Herramientas de hacking para analizar vulnerabilidades 42
4.6. Verificar detección de anomalías 45
4.7. Conexiones externas nuevas 48
Capítulo V 51
5. Conclusiones y futuros trabajos 51
5.1. Conclusiones 51
5.2. Trabajos futuros 52
Anexos 54
6. Configuración de LADDER 54
6.1. Configuración de dirección IP del PLC mediante BOOTP/DHCP Server 54

6.2. Configuración del Driver en RSLinx Classic 56
6.3. Programación del PLC 58
7. Configuración y puesta en marcha de HMI 61
8. Conexión y configuración de prototipo de red OT 69
8.1. Configuración firewall FORTIGATERUGGED 30D 69
8.2. Configuración de VLAN 72
8.3. Configuración de FortiSwitch 73
9. Pruebas de comunicación en red OT 75
9.1. Gestión de NOZOMI P500 desde Fortigate 75
9.2. Asignación de VLAN a puertos del FortiSwitch 76
9.3. Configuración de políticas IPV4 77
9.4. Configuración Mirror Span 84

Índice de figuras

Figura 1: Ejemplo de red IT. Fuente: propia 4
Figura 2:Modelo OSI. Fuente propia 7
Figura 3: Solución de red OT [21]. 12
Figura 4: Problemas de red OT [25]. 14
Figura 5: Arquitectura de prototipo de red OT a implementar. Fuente propia 25
Figura 6: Metodología para diagnósticos de vulnerabilidades. Fuente propia 27
Figura 7: P&ID del proceso de nivel 28
Figura 8: Esquema de conexiones eléctricas 29
Figura 9: Modelo planta de nivel. Fuente propia 30
Figura 10: Construcción final maqueta. Fuente Propia 32
Figura 11:Programa en código LADDER. Fuente propia 33
Figura 12: interfaz HMI. Fuente propia 34
Figura 13: Estado de los instrumentos. Fuente propia 34
Figura 14: Activos de red OT. Fuente propia 36
Figura 15: Visualización de Red OT. Fuente propia 37
Figura 16: Seguimiento de activos. Fuente propia 38
Figura 17: Fase de aprendizaje de NOZOMI. Fuente propia 39
Figura 18: Selección de tiempo de Aprendizaje. Fuente propia 40
Figura 19: Aprendizaje Nozomi. Fuente propia 41
Figura 20: Configuración modo aprendizaje. Fuente propia 42
Figura 21:Escaneo de puertos con Zenmap. Fuente propia 43
Figura 22:Inicio de Script DoS al servidor Web. Fuente propia 44
Figura 23: Intento de conexiones al servidor Web a través del puerto 80. Fuente propia 44
Figura 24: Antes del ataque DoS. Fuente propia 45
Figura 25: Después del ataque DoS. Fuente propia 45
Figura 26: Entorno de alarmas y vulnerabilidades. Fuente propia 46
Figura 27: respuesta de Nozomi al ataque DoS. Fuente propia 47
Figura 28 Reconocimiento de nueva conexión vulnerable. Fuente propia 47
Figura 29: Panel de alertas NOZOMI P500. Fuente propia 48
Figura 30: Alerta de detección de puertos. Fuente propia 48
Figura 31 : Aparición de nuevos nodos. Fuente propia 49
Figura 32: Inicio software BOOTP/DHCP Server. Fuente propia 54
Figura 33: Seleccionar MAC y Dirección IP. Fuente propia 55
Figura 34: Asignar dirección IP a PLC. Fuente propia 55
Figura 35: PLC configurado con dirección IP. Fuente propia 56
Figura 36: Inicio de Software RSLinx Classic. Fuente propia 56
Figura 37: Configurar nuevo Driver. Fuente propia 57
Figura 38:Selección de Driver. Fuente propia 57
Figura 39: Nombre para el Driver. Fuente propia 58
Figura 40:Configuración IP para el Driver. Fuente propia 58
Figura 41: Inicio software RSLogix 500. Fuente propia 59
Figura 42: Abrir código LADDER. Fuente propia 59
Figura 43: Código de acceso. Fuente propia 60
Figura 44: Descarga de código LADDER al PLC. Fuente propia 60
Figura 45: Descarga de código LADDER al PLC. Fuente propia 61
Figura 46: Código LADDER descargado a PLC. Fuente propia 61
Figura 47: Inicio: Software Factory Talk View. Fuente propia 62
Figura 48:Entorno Machine Edition. Fuente propia 62
Figura 49:Proyecto Machine Edition. Fuente propia 63
Figura 50: Crear servidor OPC Data Server. Fuente propia 63
Figura 51:Nombre y tipo de servidor OPC. Fuente propia 64

Figura 52:Nuevo servidor OPC creado. Fuente propia 65
Figura 53: Configuración OPC. Fuente propia 65
Figura 54: Asociar servidor OPC al código LADDER. Fuente propia 66
Figura 55: Ejecución Interfaz HMI. Fuente propia 66
Figura 56: Autenticación de usuario en la interfaz. Fuente propia 67
Figura 57 Usuario autenticado. Fuente propia 67
Figura 58: Inicio y parada del Proceso. Fuente propia 68
Figura 59: Estado de los instrumentos. Fuente propia 68
Figura 60: Configuración Firewall. Fuente propia 69
Figura 61: configuración de red. Fuente propia 70
Figura 62: Login. Fuente propia 70
Figura 63: configuración LAN 4. Fuente propia 71
Figura 64: Crear zona. Fuente propia 71
Figura 65: Conexión ISP. Fuente propia 72
Figura 66: Segmento de VLAN 88 (Red de Control). Fuente propia 72
Figura 67: Segmento de VLAN 20 (Red de Operación). Fuente propia 73
Figura 68: integración del FortiSwitch. Fuente propia 73
Figura 69: control remoto del Switch. Fuente propia 74
Figura 70: ingreso a consola del Fortigate. Fuente propia 74
Figura 71: Habilitar control de Switch desde consola. Fuente propia 75
Figura 72: Control del FortiSwitch. Fuente propia 75
Figura 73: Configuración de puerto gestión de NOZOMI. Fuente propia 76
Figura 74: Configuración de puertos del FortiSwitch. Fuente propia 76
Figura 75: Asignar VLAN al puerto del FortiSwitch. Fuente propia 77
Figura 76: Red de control- Internet. Fuente propia 78
Figura 77: Red de control-NOZOMI P500. Fuente propia 78
Figura 78:Red de control-Red de operación. Fuente propia 79
Figura 79:Red de operación-Internet. Fuente propia 79
Figura 80: Red de operación-gestión NOZOMI P500. Fuente propia 80
Figura 81:Red de operación-red de control. Fuente propia 80
Figura 82: Cambiar configuración de Adaptador. Fuente propia 81
Figura 83: Adaptador Ethernet. Fuente propia 81
Figura 84: TCP/IPv4. Fuente propia 82
Figura 85: IP estática. Fuente propia 82
Figura 86: Nuevo acceso a interfaz del FortiGate. Fuente propia 83
Figura 87: Acceso a NOZOMI P500. Fuente propia 83
Figura 88: Ingreso a consola FortiGate. Fuente propia 84
Figura 89: Configuración mirror Span. Fuente propia 85
Figura 90: Comprobar configuración mirror span. Fuente propia 85

Índice de tablas

Tabla 1: Requerimientos para Prototipo de red OT. Fuente propia 24
Tabla 2: Descripción de dispositivos de red OT. Fuente propia 26
Tabla 3: construcción de prototipo. Fuente propia 31

Capítulo I

1. Introducción

Actualmente, las organizaciones industriales requieren que las tecnologías IT (Information Technology) y OT (Operation Technology) adopten un modelo acorde con las necesidades reales del mercado, se tienen clientes más exigentes, una demanda oscilante y un mayor número de competidores. Por tanto, se requiere un modelo de trabajo ágil, que incremente el conocimiento, la comunicación, la colaboración y la coordinación entre IT y OT [1].

Las IT pueden ser definidas como aquellas tecnologías usadas para organizar, procesar y difundir información que será usada en aplicaciones específicas. Como ejemplos de IT se tienen las redes MAN, LAN, WAN, computadoras, dispositivos móviles, entre otros [2]. A nivel empresarial, una organización debe actualizar constantemente su infraestructura de red IT porque esto va a repercutir en su desempeño, a través del manejo de herramientas que logran disminuir costos operativos de la empresa, entregar productos en menor tiempo y brindar a los clientes un servicio de calidad con resultados óptimos [3].

Las tecnologías operacionales relacionan un conjunto de hardware y software, utilizado para detectar o causar un cambio a través del monitoreo directo y/o control de dispositivos físicos, procesos y eventos en empresas centradas en activos, en particular en producción y operaciones. Estas tecnologías se utilizan en el control de equipos y procesos industriales, teniendo como su principal área de interés los sistemas de control supervisorio y adquisición de datos (SCADA), de control distribuido (DCS), controladores lógicos programables (PLC), unidades terminales remotas (RTU), y más recientemente, comparten mucho con lo que denominamos Internet de las Cosas (IoT) [4].

Hace algunos años las IT y OT no estaban muy relacionadas, sin embargo, con el uso extendido del Internet de las cosas (IoT), las empresas empezaron a darse cuenta de la necesidad de coordinar y comunicar las IT con las OT, con el fin de encontrar y analizar patrones que permitieran crear soluciones eficientes a los problemas [2]. Hoy en día, las redes OT y las redes IT suelen estar integradas, ambos entornos necesitan compartir información entre ellos y en muchas ocasiones, se requiere que esa información, así como algunas aplicaciones de supervisión y control de proceso sean accesibles desde el exterior de la planta de control de procesos industriales. Esto permite dotar de flexibilidad y rapidez de actuación a una organización, pero también puede convertirse en un problema si no se adoptan

medidas que aseguren que el tránsito de la información se lleve a cabo de forma segura [5].
La integración de redes OT y redes IT conlleva a que el mundo OT se enfrente a problemas absolutamente desconocidos en su ámbito, principalmente en la seguridad de toda su infraestructura. La convergencia IT/OT y ciberseguridad deben ir de la mano, lo que implica más necesidad y desarrollo de ciberseguridad y más complejidad de los sistemas tecnológicos. En IT han existido procesos de desarrollo y gestión de aplicaciones, despliegue y administración, que estaban tradicionalmente planificados de acuerdo con un ciclo de vida de software o de hardware. En las redes OT, los sistemas son desplegados de manera poco estructurada y sin coordinación con las redes IT. Esto impide su soporte y mantenimiento eficiente, con lo cual se incrementan los costes a largo plazo. Por lo general, la gestión de incidencias y peticiones en OT tiende a ser escasamente consistente, no existe inventario ni gestión de configuración y es habitual carecer de una estrategia y gestión de proveedores OT [6].

Gamma Ingenieros es una empresa con amplia experiencia en seguridad de redes IT, que a través de su larga experiencia comercial ha identificado la necesidad de muchas empresas en el sector industrial de integrar sus redes OT con redes IT de forma segura. Por tal motivo, la empresa pretende estar a la vanguardia en seguridad tecnológica, a través de soluciones y herramientas que permitan brindar seguridad en redes OT. Consecuentemente, el presente proyecto busca brindar apoyo en el proceso de diagnóstico de vulnerabilidades en entornos de red OT, utilizando herramientas hardware y software proporcionadas por partner de la empresa Gamma Ingenieros como FORTINET y NOZOMI NETWORKS, para cumplir los propósitos de la empresa se plantean los siguientes objetivos:

1.1. Objetivo general

Diagnosticar vulnerabilidades de seguridad informática en un prototipo de red OT

1.2. Objetivos específicos

- Implementar un prototipo de red OT, de acuerdo a requerimientos y especificaciones de Gamma Ingenieros.

- Realizar diagnóstico de vulnerabilidades de seguridad en el prototipo de red OT implementado, usando las herramientas de NOZOMI Networks.

1.3. Contenido

Este documento se ha organizado en 5 capítulos:

Capitulo I. Proporciona una visión general de la necesidad de integrar redes IT, OT, y presenta el problema de seguridad en la integración de estas redes.

Capítulo II. Describe las principales características de las redes IT, OT y de su integración; al tiempo que presenta algunas herramientas para seguridad de las mismas. Además, muestra conceptos de seguridad en el ámbito industrial proporcionados por el estándar ISA 99.00.01.

Capítulo III. Define el proceso de construcción e implementación del prototipo de red OT.

Capítulo IV. Presenta el análisis de vulnerabilidades del prototipo de red OT desarrollado, de acuerdo a la metodología definida por Gamma Ingenieros.

Capítulo V. Muestra las conclusiones de la práctica profesional y el control de vulnerabilidades en una red OT.

Capítulo II

2. Marco teórico

2.1. Red IT

Hace algunos años, la informática estaba limitada a grandes empresas e instituciones que disponían de enormes centros de cálculo. Sin embargo, con la aparición del ordenador personal, la informática entró en todos los lugares: hogares (informática personal), puestos de trabajo, comercios, grandes vehículos, etc. De modo que, logró influir en todas las facetas personales y profesionales de los seres humanos y se convirtió en algo más amplio y potente: las redes de tecnologías de la información (TI) [7]. Una red IT se puede definir como, un conjunto de herramientas hardware y software que se complementan para prestar un servicio en particular. A continuación, en la figura 1 se observa un ejemplo de red IT y luego se definen sus componentes.

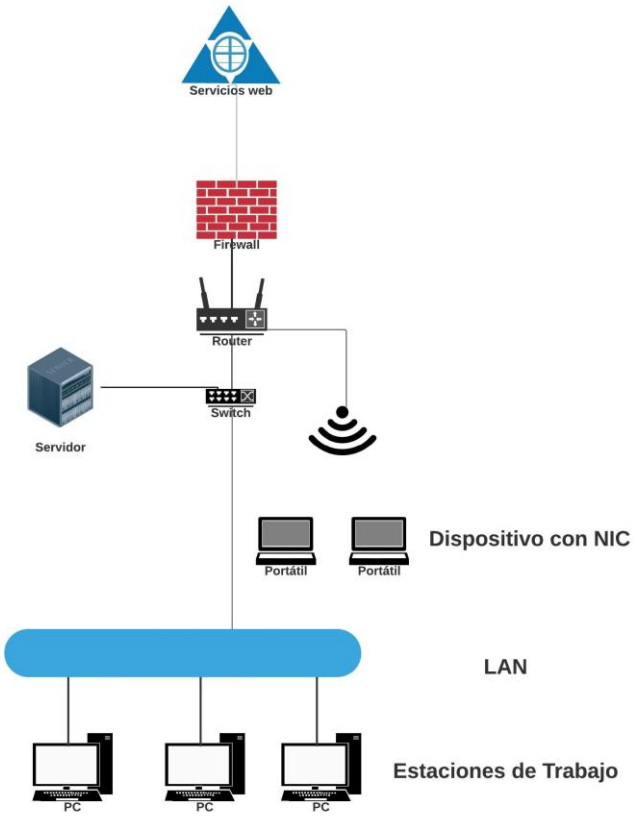


Figura 1: Ejemplo de red IT. Fuente: propia

2.1.1. Componentes de una red IT.

Una red IT puede estar compuesta por estaciones de trabajo, tarjetas de conexión a la red, servidores, dispositivos de interconexión como switch y routers, dispositivos de seguridad como firewall y por el cableado en general.

- **Cableado:** Los tipos de cableado más utilizados en las redes IT son par trenzado, cable coaxial y fibra óptica. Además, se pueden realizar conexiones a través de radio o microondas, dependiendo el tipo de red y los requerimientos de la misma, velocidad y longitud se debe considerar el tipo de cable a utilizar.

- **Estación de Trabajo:** es un ordenador que facilita a los usuarios el acceso a servidores y periféricos de la red. A diferencia de un ordenador aislado, tiene una tarjeta de red y está físicamente conectada por medio de cables u otros medios no guiados con los servidores. Las estaciones de trabajo usualmente ofrecen más alto rendimiento que las computadoras personales, especialmente en lo que respecta a gráficos, poder de procesamiento y habilidades multitareas [8].

- **Tarjeta de conexión a la red:** conocida como NIC (Network Interface Card), es el elemento que conectamos al computador para proporcionar el soporte y conexión a la de red. Puede venir en formato de arquitectura Industrial estándar (Industry Standard Architecture) o PCI (Peripheral Component Interconnect); para Ethernet estándar resulta suficiente el ancho de banda de la primera, pero para Fast Ethernet merece la pena utilizar PCI.

- **Servidor:** es un ordenador u otro equipo informático encargado de suministrar información a una serie de clientes, que pueden ser personas u otros dispositivos conectados a él. La información que puede transmitir es múltiple y variada, desde archivos de texto, imágenes, vídeos, hasta programas informáticos, bases de datos, etc. [9].

- **Switch:** es un dispositivo de interconexión que opera en la capa 2 (nivel de enlace) del modelo OSI y reenvía las tramas de datos de acuerdo a la dirección MAC (Media Access Control)) de los dispositivos de origen y destino. Están diseñados para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. Segmenta la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final.

- **Router:** es un dispositivo de interconexión de redes que opera en la capa 3 (nivel de red) del modelo OSI. Interconecta segmentos de red o redes

enteras, haciendo pasar paquetes de datos entre ellas. Se encarga del enrutamiento y direccionamiento de paquetes[10].

- **Firewall:** es un dispositivo de seguridad en redes IT, controla el tráfico de la red entrante y saliente, pero también decide si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad. Los firewalls han sido una primera línea de defensa en seguridad de redes por más de veinticinco años, establecen una barrera entre las redes internas seguras y controladas en las que se puede confiar y las redes externas no confiables, como Internet. Un firewall puede ser hardware, software o ambos [11]. Existen diferentes tipos de firewall, entre ellos se pueden mencionar los siguientes:

- **Servidor de seguridad proxy:** firewall proxy sirve como puerta de enlace de una red a otra para una aplicación específica. Los servidores proxy pueden proporcionar una funcionalidad adicional, como el almacenamiento en caché de contenido y la seguridad, impidiendo las conexiones directas desde fuera de la red. Sin embargo, esto también puede afectar las capacidades de rendimiento y las aplicaciones que pueden admitir [11].

- **Firewall de inspección de estado:** permite o bloquea el tráfico según el estado, el puerto y el protocolo. Supervisa toda la actividad desde la apertura de una conexión hasta que se cierra. Las decisiones de filtrado se toman con base tanto a las reglas definidas por el administrador como al contexto, que se refiere al uso de información de conexiones anteriores y paquetes que pertenecen a la misma conexión [11].

- **Firewall de gestión de amenazas unificadas (UTM):** un dispositivo UTM generalmente combina las funciones de un firewall de inspección de estado, previniendo la autenticación de intrusos a través de un antivirus. También puede incluir servicios adicionales y, a menudo la gestión de la nube. Los UTM se centran en la simplicidad y la facilidad de uso [11].

- **Firewall de última generación (NGFW): l**os firewalls han evolucionado más allá del simple filtrado de paquetes y la inspección de estado. La mayoría de las empresas están implementando firewalls de próxima generación para bloquear amenazas modernas, como malware avanzado y ataques de capa de aplicación [11]. Un firewall de próxima generación debe incluir capacidades de cortafuegos estándar como inspección de estado, prevención integral de intrusiones, conocimiento y control de aplicaciones para ver y bloquear aplicaciones de riesgo, actualizar rutas para incluir futuros feeds de información y técnicas para hacer frente a las amenazas de seguridad en evolución.

2.1.2. Comunicación de una red IT.

La interconexión de redes se basa en el modelo de referencia OSI (interconexión de sistemas abiertos), que permite estandarizar la comunicación a través de siete niveles que describen como se realiza una comunicación de principio a fin. Cada uno de estos niveles tiene sus propias funciones y protocolos para comunicarse con otros niveles, de modo que, cada nivel trabaja de forma independiente de los demás, sin necesidad de conocer el funcionamiento del resto de niveles. Los protocolos de cada nivel se comunican con sus homólogos, es decir, su mismo protocolo situado en el otro extremo de la comunicación. De esta forma, no tendrán influencia sobre protocolos de otros niveles.

La Figura 2 indica como se establece el flujo de información según el modelo OSI, la estación de trabajo de origen envía información desde la capa siete (aplicación) hasta la capa uno (física). Luego, en la estación de destino el flujo llegará a la capa física y subirá hasta la capa de aplicación.

Figura 2:Modelo OSI. Fuente propia

La capa física del modelo OSI se encarga de los elementos físicos de la conexión. Gestiona los procedimientos a nivel electrónico para que la cadena de bits de información viaje desde el transmisor al receptor sin alteración alguna. Define el medio físico de transmisión (cables de pares trenzados, cable coaxial, ondas y/o fibra óptica), maneja las señales eléctricas y transmite el flujo de bits y delimita las características de los materiales, como conectores y niveles de tensión [12].

La capa de enlace del modelo de referencia OSI, proporciona los medios funcionales para establecer la comunicación de los elementos físicos. Se ocupa del direccionamiento físico de los datos, el acceso al medio y especialmente de la detección de errores en la transmisión. Esta capa construye tramas de bits con la información y controla que la transmisión se haga de forma correcta. Los protocolos más conocidos de este enlace son los IEEE 802 para las conexiones LAN y IEEE 802.11 para las conexiones Wifi [12].

La capa de red se encarga del enrutamiento entre dos o más redes conectadas. Este nivel garantiza que los datos puedan llegar desde el transmisor al receptor, realizando las conmutaciones y encaminamientos necesarios. Por ello, se requiere que ésta capa conozca la topología de la red en la que opera [12].

La cuarta capa es la de transporte, y es la responsable de la regulación del flujo de información desde el origen hasta el destino de forma confiable y precisa; se encarga de dividir los datos recibidos desde la aplicación en segmentos, a los cuales agrega un encabezado para identificarlos (incluyendo los números de puerto origen y destino) y poder reensamblarlos. Además, transmite los datos ensamblados a la aplicación correcta (lo hace mediante los números de puertos) y determina el protocolo que garantiza el envío del mensaje [13].

El nivel de sesión controla y mantiene activo el enlace entre las máquinas que están transmitiendo información, asegura que se establezca y se mantenga la conexión hasta finalizar la transmisión. Por su parte, el nivel de presentación se encarga de la representación de la información transmitida, asegura que los datos sean entendibles a los usuarios, a pesar de los distintos protocolos utilizados tanto en un receptor como en el transmisor. Finalmente, el nivel de aplicación permite a los usuarios acceder a los servicios de las demás capas [12].

2.1.3. Seguridad en redes IT.

Es el proceso de tomar medidas físicas y preventivas para proteger la red subyacente de uso indebido, mal uso, mal funcionamiento, modificación, destrucción o divulgación incorrecta, funciones críticas dentro de un entorno seguro. A continuación se definen algunos conceptos importantes para poder tener conocimiento acerca de la seguridad en una red IT [14].

- I**nformación de seguridad y gestión de eventos (SIEM Security Information and Event Management):** estos productos pretenden reunir información de una variedad de herramientas de red, con el fin de proporcionar los datos necesarios para identificar y responder a las amenazas, tienen como objetivo otorgar a las organizaciones información útil sobre potenciales amenazas de seguridad de sus redes críticas de negocio, a través de la estandarización de datos y priorización de amenazas. Esto es posible mediante un análisis centralizado de datos de seguridad, obtenidos desde múltiples sistemas, que incluyen aplicaciones antivirus, firewalls y soluciones de prevención de intrusiones [15].

- **VPN (Red privada Virtual):** es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet, las empresas suelen utilizar estas redes para conectarse desde otros lugares a sus recursos corporativos para proteger su información. Parte de la protección de la información que viaja por una VPN es el cifrado, no obstante, verificar que la misma se mantenga íntegra es igual de trascendental. Para lograr esto, IPsec emplea un mecanismo que cuando detecta alguna modificación dentro de un paquete procede a descartarlo. Proteger la confidencialidad e integridad de la información utilizando una VPN es una buena medida para navegar en sitios Wi-Fi públicos e inseguros incluso si no se desea acceder a un recurso corporativo [16].

- **Seguridad de la red y la nube:** para manejar los aspectos de seguridad, muchos proveedores de servicios en la nube establecen políticas centralizadas de control de seguridad en su propia plataforma. Sin embargo, el truco aquí es que esos sistemas de seguridad de la nube, no siempre coinciden con las políticas y procedimientos para las redes internas de una empresa, y esa falta de coincidencia puede aumentar la carga de trabajo para los profesionales de seguridad de redes. Hay una variedad de herramientas y técnicas disponibles que pueden ayudar a aliviar parte de esta preocupación, pero la verdad es que esta área todavía está en desarrollo y la conveniencia de la nube puede significar problemas de seguridad para la red [14].

- **Software de seguridad de red:** existen diferentes soluciones de software para brindar seguridad en la red, algunas de estas herramientas son productos corporativos de grandes proveedores, mientras que otras vienen en la forma de utilidades gratuitas y de código abierto. Las categorías principales incluyen: analizadores de paquetes, que ofrecen una visión profunda del tráfico de datos, exploradores de vulnerabilidades como el software de detección y prevención de intrusos. En un entorno donde necesita obtener muchas herramientas para trabajar, es posible que también se desee implementar software SIEM. Los productos SIEM evolucionaron a

partir del software de registro y analizan los datos de red recopilados por varias herramientas diferentes para detectar comportamientos sospechosos en las redes IT [14].

2.2. Red OT

Una red OT se refiere al conjunto de tecnologías que se utilizan para controlar y monitorear los procesos industriales, es una integración entre software y hardware que detecta o causa un cambio a través de la monitorización y control directo de dispositivos físicos o eventos relacionados a un proceso [17]. Las redes OT se implementan para diferentes procesos de producción y cada uno de ellos tiene requisitos concretos que deben personalizarse. Sin embargo, se puede afirmar que, el objetivo general de esas infraestructuras es tener acceso y control remoto de la maquinaria; además, deben soportar condiciones ambientales agresivas como vibraciones, choques y altas temperaturas; son diseñadas para tener un ciclo de vida mínimo de 15 a 20 años; deben estar siempre disponibles MTDP (Maximun tolerable period of disruption< 300 ms) y presentan elementos críticos de seguridad por encima de la red [18].

2.2.1. Niveles de red OT.

Cuando se habla de niveles de red OT se referencia en el modelo de Purdue, siendo este adoptado del modelo de Arquitectura de referencia de empresa de Purdue (PERA) por ISA-99 y se usó como un modelo conceptual para la segmentación de la red de ICS (Sistema de Control Industrial). Es un modelo de referencia adoptado por la industria que muestra las interconexiones e interdependencias de todos los componentes principales de un ICS típico, divididos en 5 niveles:

Nivel 0 – Proceso: el nivel 0 es donde está el equipo de proceso o instrumentación que estamos controlando y monitoreando desde los niveles más altos. También conocido como equipo bajo control, en este nivel podemos encontrar dispositivos como motores, bombas, válvulas y sensores que miden la velocidad, la temperatura o la presión. Como el nivel 0 es donde se realiza el proceso real y donde se fabrica el producto, es imperativo que las cosas funcionen sin problemas y sin interrupciones. La interrupción más leve en un solo dispositivo puede causar un caos en todas las operaciones [19].

Nivel 1 - Control básico: El nivel 1 es donde está todo el equipo de control. El propósito principal de los dispositivos en este nivel es abrir válvulas, mover actuadores, arrancar motores, etc. Típicamente, se encuentran los PLC, las unidades de frecuencia variable (VFD), los controladores dedicados de

proporcional-integral (PID). Aunque puede encontrar un PLC en el nivel 2, su función es de naturaleza de supervisión en lugar de control [19].

Nivel 2 - Control de supervisión de área: Muchas de las funciones y sistemas en el nivel 2 son las mismas que para el nivel 3, pero están más orientadas a una parte o área más pequeña del sistema en general. En este nivel, partes específicas del sistema son monitoreadas y administradas con sistemas HMI [19].

Nivel 3 - Operaciones del sitio: es donde residen los sistemas que soportan las funciones de control y monitoreo en toda la planta. En este nivel, el operador está interactuando con los sistemas de producción en general, en salas de control centralizadas con HMI y terminales de operador que brindan una descripción general de todos los sistemas que ejecutan los procesos en una planta o instalación. El operador utiliza estos sistemas HMI para realizar tareas tales como controles de calidad, administración del tiempo de actividad y monitoreo de alarmas, eventos y tendencias [19].

Nivel 4 - Planificación y logística del negocio del sitio: es el hogar de todos los sistemas de tecnología de la información que respaldan el proceso de producción en una planta de una instalación. Estos sistemas informan estadísticas de producción, como el tiempo de actividad y las unidades producidas para los sistemas corporativos, y toman pedidos y datos comerciales de los sistemas corporativos que se distribuirán entre los sistemas de OT o ICS [19].

Teniendo en cuenta el modelo de Purdue y la clasificación de los niveles OT, se puede desglosar un sistema de control industrial lo que permite visualizar y organizar mejor una infraestructura de red OT, para que así aparezcan dos conceptos en el ámbito de la ciberseguridad como son SOC y SIEM.

2.2.2. Estructura SOC y su integración con SIEM.

Un SOC (Security Operations Center) es un equipo de analistas de seguridad (con herramientas, tácticas, técnicas y procedimientos de ciberseguridad) organizados con el objetivo de detectar, analizar responder, informar y prevenir ciber-incidentes y proporcionar servicios a un conjunto de usuarios, sitios, activos IT/OT, redes, organizaciones, etc. Todo SOC utiliza sistemas SIEM para monitorizar y gestionar de forma continua el estado de seguridad de una organización, puede interconectarse con otros SOC externos. Un SOC integra un equipo de especialistas que defienden una empresa de toda actividad no autorizada dentro de sus redes y equipos de computadores, implantando monitorización, detección anticipada, análisis (tendencias y análisis de patrones) y respuesta y restauración de las actividades [20].

El SOC ayuda a las organizaciones a reducir el tiempo de estar infectado por alguna ciber-amenaza o ciber-arma, a través de monitoreo constante y búsqueda de indicadores específicos de actividad de APTs (Advanced Persistent Threats). Su principal misión es supervisar continuamente las redes, sistemas de computación, dispositivos IoT, etc., para detectar vulnerabilidades, intentos de intrusión, ciber-ataques o signos de actividad anómala o maliciosa y desplegar la respuesta apropiada de forma rápida. También, un SOC permite una mejor detección e investigación de ciber-incidentes, incluyendo capacidades de respuesta con datos procedentes de todo tipo de dispositivos (servidores DNS, software de aplicación, firewalls, logs, sistemas de seguridad y flujos de red) [20].

En la figura 3 se observa una solución de infraestructura de red OT a través del modelo de Purdue con cada uno de los niveles, permitiendo desglosar un ICS para realizar de forma adecuada una arquitectura de seguridad OT con los equipos de NOZOMI NETWORKS. La función principal o aporte es que centraliza toda la información que llega desde los equipos de nivel 2 y 3, así obtiene toda la información centralizada de todas las redes existentes, realizando un control de activos y posibles vulnerabilidades a las que se enfrenta una red OT, además de simplificar las tareas de un equipo SOC.

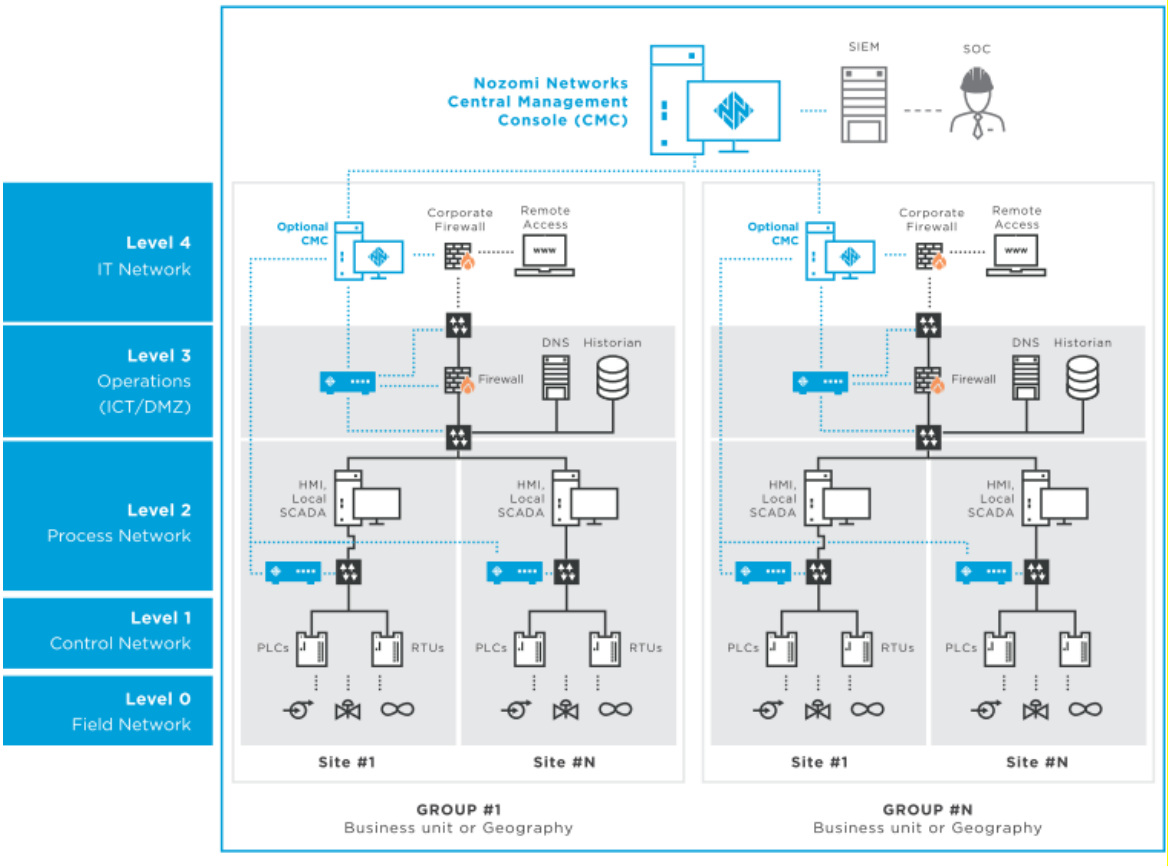


Figura 3: Solución de red OT [21].

El modo de funcionamiento de la consola de administración centralizada de NOZOMI en el modelo de Purdue, se basa en la identificación y captura de tráfico en los SWICHES de administración de equipos de la red OT, así de esta manera en la figura 3 se observan sondas en los niveles 2 y 3, para capturar e interpretar la información que viaja encapsulada sobre el protocolo TCP/IP.
Con la interpretación de esta información se pueden tomar medidas correctivas ante eventuales vulnerabilidades encontradas en la red OT y proveer un mejor panorama al equipo SOC.

2.3. Integración IT y OT

Los sistemas de automatización y control industrial operan en un entorno complejo, las organizaciones comparten cada vez más información entre el sistema de automatización industrial (red OT) y la parte administrativa de negocios (red IT). Esto hace que, la seguridad informática en la parte industrial y de negocios tome un papel importante, ya que muchos daños pueden ser ocasionados, por ejemplo: pérdida de secretos comerciales, interrupción en el flujo de información, posible pérdida de vidas humanas, violación de regulación a normas de control, daños en la producción y daños al medio ambiente. Todos estas fallas pueden ser consecuencias del inapropiado manejo de la seguridad informática, por tal motivo el compromiso con la seguridad operacional debe ser muy grande [22].

Tradicionalmente, los equipos de OT que llevan más de veinte años funcionando sin necesidad de recurrir a un refuerzo de seguridad, ahora se ven afectados por los ataques que llegan con facilidad a los dispositivos de IT. En la medida en que OT e IT se integren por completo, dejando de existir por separado, será obligatoria una tecnología de ciberseguridad más potente que la que se conoce actualmente, para poder proteger las redes de todos los posibles ataques y violaciones a la seguridad. La seguridad es un problema que debe abordarse a fondo para evitar todo tipo de ataques [23]

Durante los últimos años, los ICS (sistemas de control industrial) han sido objeto de ciberataques cada vez más frecuentes y sofisticados. En gran parte, esto es una consecuencia de la inevitable convergencia de IT con OT. Como sucede en todas las esferas de la informática, las ventajas de mayor conectividad en red a través de estándares de código abierto como Ethernet y TCP/IP, así como el ahorro derivado de la sustitución de los equipos registrados dedicados por hardware y software comercial, deben pagar el coste de una mayor vulnerabilidad [24].

Los sistemas industriales (industrias de gas, petrolíferas, sanidad, hidroeléctricas etc.) están cada vez más conectados a las redes IT, por tanto, se han convertido en el objetivo de ciberdelincuentes. Los ataques no solo van dirigidos al software, sino

también al hardware, estas vulnerabilidades no son nuevas o de última generación, solo se asumía que no serían exploradas en las redes OT, ya que estas redes sólo trabajaban bajo sus protocolos propietarios y no se autenticaban en las redes de IT, de ahí el porqué de los principales problemas en una red OT.

Figura 4: Problemas de red OT [25].

2.4. Estándares para seguridad en sistemas de control y automatización industrial

Actualmente, existen estándares que abordan el tema de seguridad en sistemas de control y automatización industrial. Entre ellos el estándar ANSI/ISA-62443-1-1 (99.01.01)-2007, Manufacturing and Control Systems Security (99.00.01) y el reporte técnico ANSI / ISA-TR99.00.01-2004 ANSI / ISA-TR99.00.01-2.

2.4.1. ANSI/ISA-62443-1-1 (99.01.01).

El estándar ANSI/ISA-62443-1-1 (99.01.01)-2007 es el primero de una serie de estándares ISA que abordan el tema de seguridad para sistemas de control y automatización industrial. La atención está centrada en la seguridad electrónica de estos sistemas, comúnmente conocida como seguridad cibernética. Esta primera parte del estándar describe conceptos y modelos básicos relacionados con la seguridad cibernética.

La meta en la aplicación de la serie 62443 es mejorar la seguridad, la disponibilidad, integridad y la confidencialidad de los componentes o sistemas utilizados para la automatización industrial, así como proporcionar criterios para adquisición e implementación de sistemas de control industrial. Este estándar plantea una serie de requisitos destinados a mejorar la seguridad electrónica y a ayudar en la identificación de vulnerabilidades, En su primera parte, el estándar ANSI/ISA-62443-1-1 (99.01.01) establece las siguientes definiciones [26].

- **Amenaza**: es una potencial violación a la seguridad de la red, que existe cuando hay una circunstancia, capacidad, acción o evento que podría violar parámetros y como consecuencia causar daños.

- **Vulnerabilidad:** es un error o debilidad en un sistema de diseño, ejecución o funcionamiento de gestión que podría ser explotada para violar la política de integridad o la seguridad del sistema.

- **Riesgo residual:** se define como el resto de riesgo después de aplicar los controles de seguridad o contramedidas.

- **Evaluación de riesgos**: es el proceso que identifica sistemáticamente vulnerabilidades potenciales a valiosos recursos del sistema y las amenazas a esos recursos, cuantifica las exposiciones de pérdida y consecuencias basada en la probabilidad de ocurrencia, y (opcionalmente) recomienda cómo asignar los recursos a las contramedidas para reducir al mínimo la exposición total.

- **Gestión de riesgos:** es el proceso de identificación y aplicación de contramedidas proporcional al valor de los bienes protegidos, se basa en una evaluación del riesgo [27].

2.4.2. Manufacturing and Control Systems Security (99.00.01)

El objeto del estándar es la seguridad en la fabricación[1] y sistemas de control. El término “Manufacturing and Control Systems Security” se aplica en el sentido práctico más amplio, que abarca todos los tipos de plantas e instalaciones, así como otras operaciones de procesamiento tales como los servicios (es decir, eléctrica, gas y agua), fabricación, tuberías y sistemas de transporte u otras industrias que utilizan activos automatizados o controlados a distancia [28]. El estándar presenta algunos términos, definiciones y abreviaturas utilizadas en esta referidos especialmente a la seguridad:

2.4.2.1. *Niveles de seguridad*

RFC 2828 [2] define el nivel de seguridad de la información y el grado de sensibilidad que se califica como: Baja, Media y Alta. Teniendo cinco niveles de seguridad, que son independientes de la técnica utilizada para realizar la evaluación de riesgos, divididos de la siguiente manera:

[1] Fabricación: Elaborar un producto a partir de la combinación de varios componentes, especialmente en serie y por medios mecánicos.
[2] **RFC (solicitud de comentarios) 2828:** conjunto de abreviaciones, términos y recomendaciones para el uso de una terminología relacionada a la seguridad de los sistemas de información.

- **Nivel 0:** no hay seguridad, la información fluye libremente dentro y entre todas las zonas. El acceso y uso de los datos no son controlados. No hay ninguna garantía de integridad, confidencialidad, la restricción de flujo de datos, y no hay detección, notificación y respuesta a violaciones.

- **Nivel 1:** función de control de acceso basado en roles (RBAC[3]), para el intercambio de información de dos vías. Este nivel se asegura de que los atributos de los archivos del sistema se establecen en valores de liberación estándar. En este nivel, no se toman medidas, y los servicios del sistema no se ven afectados.

- **Nivel 2:** este nivel ofrece una seguridad adecuada de control para la mayoría de entornos. Algunos de los ajustes de los archivos y los parámetros del sistema se modifican, lo que restringe el acceso al sistema para reducir los riesgos de ataques a la seguridad. Se reportan las debilidades de seguridad y las modificaciones realizadas para restringir el acceso.

- **Nivel 3:** los archivos del sistema y los parámetros se ajustan para minimizar los permisos de acceso. La mayoría de las aplicaciones y comandos del sistema funcionan con normalidad, pero a este nivel, las consideraciones de seguridad tienen prioridad sobre cualquier otro comportamiento del sistema.

- **Nivel 4:** no existen canales de comunicación entre cualquiera de las zonas. La seguridad de la comunicación y la seguridad de la información es un asunto local.

2.4.2.2. *Vulnerabilidades.*

Las vulnerabilidades son debilidades inherentes a los sistemas, componentes o las organizaciones; pueden ser el resultado de opciones de diseño intencional o pueden ser accidentales, como resultado de la falta de comprensión del entorno operativo. La comprensión de la interacción entre la vulnerabilidad física y cibernética es fundamental para establecer una seguridad efectiva [28].

Las vulnerabilidades más comunes en un sistema de control son cambios en el entorno, cambio de la tecnología, falla de los componentes del sistema, falta de disponibilidad de los componentes de repuesto, rotación de personal, mayor inteligencia de amenazas, entre otros. Una cuidadosa adaptación de las vulnerabilidades a las amenazas proporcionará una jerarquía de oportunidades para mejorar la seguridad del sistema de fabricación y de control [28].

[3] **RBAC (El control de acceso basado en roles)**: Es una función de seguridad para controlar el acceso de usuarios a tareas que normalmente están restringidas al superusuario.

2.4.2.3. *Ataques.*

Las amenazas que se convierten en acciones, se conocen como ataques (a veces conocido como una intrusión). Ya sea con el diseño de componentes y sistemas, o la implementación de un programa de seguridad dentro de un sitio o en la misma organización, es necesario modelar los ataques con el fin de garantizar que las contramedidas están en su lugar para identificar y disuadir de ellos. Herramientas como los árboles de ataque (a veces conocido como ataque gráfico), proporcionan un medio estructurado de representar múltiples eventos hostiles que ocurren típicamente [28]. A continuación, se describen los ataques más comunes:

- **Pasivo:** reciben su nombre debido a que el atacante (o perpetrador u oponente o persona que se entromete) no altera en ningún momento la información, es decir, únicamente la observa, escucha, obtiene o monitorea mientras está siendo transmitida. Con los ataques pasivos se obtiene información que puede consistir en obtener datos sobre el origen y destino de la comunicación, con ello se determina la localización y la identidad de los anfitriones (emisor, receptor), además del control de volumen de tráfico intercambiado entre las entidades monitoreadas, de esta forma se obtienen todos los datos necesarios para percatarse de la actividad o inactividad inusuales [29].

- **Activo:** los ataques activos implican algún tipo de modificación del flujo de datos transmitido modificación de los mismos, o la creación de un falso flujo de datos. El enmascaramiento o suplantación de identidad, el intruso se hace pasar por una entidad diferente, por ejemplo, las secuencias de autenticación pueden ser capturadas y repetidas después de que una secuencia válida haya sido capturada con éxito [29].

- **Sniffing (olfateando):** este ataque recolecta datos e información sobre todo lo que ocurre dentro de una red. Existen dispositivos disponibles al público para olfatear datos sobre diversas redes de comunicación, aunque estos dispositivos son comúnmente utilizados para la solución de problemas de redes y análisis de tráfico de datos, también pueden ser utilizados para recoger datos específicos acerca de cualquier transacción que tenga lugar a través de la red. Los sniffers son muy difíciles de detectar, ya que sólo leen la información de movimiento a través de los medios de comunicación conectados y no proporcionan señales en la ruta de señalización [28].

  Los sniffers pueden ser detectados con dispositivos de comunicación modernos, tales como conmutadores de red inteligente de datos, pero cuando se realiza de forma inalámbrica es casi imposible de detectar incluso con equipos de telecomunicaciones por radio muy sofisticados. Para prevenir estos ataques se debe reducir el acceso de control a puertos de datos no utilizados en la planta y proporcionar inteligencia con equipos de control de la comunicación [28].

- **Inyección:** una forma de ataque activo, que busca infiltrar código intruso para que sea interpretado/ejecutado por alguna aplicación del sistema atacado. Entre ellos, se encuentran los ataques de inyección SQL, usados para robar información de una base de datos que normalmente no estarían disponible y/o para obtener acceso a los equipos host de una organización a través del equipo que aloja la base de datos [28].

- **Repetición:** una forma de ataque pasivo, en la que las señales pueden ser capturadas a partir de trayectos de comunicaciones y reproducirse más tarde para proporcionar acceso a los sistemas de control, o para falsificar datos en el sistema de fabricación y de control. Intrusos potenciales pueden reproducir señales de control de acceso, señales biométricas y señales del sistema de control para obtener acceso no autorizado a zonas o sistemas asegurados, ocultando actividades ilegítimas y proporcionar falsas distracciones. Un correcto diseño del sistema de control debe combinar múltiples caminos para adquisición de datos, señalización y control, evitando así, que un solo toque pueda ser capturar toda la información. Dispositivos de detección de intrusiones pueden alarmar potenciales ubicaciones de tomas y las subrutinas aplicación pueden proporcionar validación de los datos recogidos[28].

- **Suplantación:** tipo de ataque pasivo generalmente conocido como spoofing, este término se utiliza para describir una variedad de maneras en que el hardware y el software pueden ser engañados. Por ejemplo, en IP spoofing el atacante sustituye la dirección IP de la víctima por otra, se puede suplantar la dirección IP de un servidor de correo. Cuando un usuario envíe su nombre de usuario y contraseña, la enviaría al equipo del atacante y no al de la empresa que aloja su correo electrónico[28].

- **Ingeniería social:** es una de las formas en las que los cibercriminales usan las interacciones entre personas para que el usuario comparta información confidencial. En este caso, un cibercriminal puede dejar un dispositivo USB infectado con software malicioso a la vista en un espacio público, alguien recogerá ese dispositivo y lo conectará a su equipo para ver qué contiene y en ese momento, el software malicioso se introducirá en el equipo. Existen muchos otros ejemplos como spear phishing, vishing, quid pro quo, etc [28].

2.4.3. ANSI / ISA-TR99.00.01-2004 ANSI / ISA-TR99.00.01-2.

Este reporte técnico proporciona una evaluación de herramientas y tecnologías de seguridad, que se aplican al entorno de fabricación y sistemas de control. Describe categorías de tecnologías de seguridad, los tipos de productos disponibles en esas categorías, los pros y contras de utilizar estos productos en la fabricación y sistemas de control, con relación a amenazas y vulnerabilidades conocidas[30].

2.4.3.1. *Tecnologías de autenticación y autorización.*

Autorización y autenticación son fundamentales para el control de acceso. Son conceptos distintos, que a menudo se confunden debido a la estrecha relación entre los dos. La autorización es el proceso para determinar quién y qué se debe permitir entrar o salir del sistema. Una vez determinada esta información, las medidas de control de acceso pueden implementarse, para verificar que las personas y los dispositivos autorizados en realidad son los que pueden acceder al sistema. La primera medida es generalmente la autenticación de la persona o dispositivo que está intentando acceder al sistema [30].

La autenticación describe el proceso de identificar positivamente a los usuarios potenciales de la red, hosts, aplicaciones, servicios y recursos que utilizan una combinación de factores de identificación o de credenciales. Existen dos tipos de autenticación, la tradicional y la de red. La autenticación de usuario tradicional se encarga de autenticar equipos, por ejemplo, al iniciar sesión en un ordenador o al activar una interfaz hombre-máquina (HMI) para ajustar un proceso. Por su parte, el servicio de autenticación de red, da capacidad a los dispositivos de red para distinguir entre las peticiones remotas autorizadas y no autorizadas de datos o para realizar acciones [30].

2.4.3.1.1 *Vulnerabilidades de seguridad.*

El enfoque tradicional para controlar el acceso a los recursos de información y de la red es establecer permisos específicos para cada usuario. Los permisos se configuran en los mecanismos de seguridad compatibles con los dispositivos inteligentes individuales. Un sistema de control industrial puede tener miles de dispositivos, tales como DCS (sistemas de control distribuido), HMI, historiadores de proceso, PLC (Controlador lógico programable), centros de control de motor, sensores inteligentes, y concentradores de datos específicos de la aplicación. Aunque son eficaces en un entorno estático, este enfoque es difícil de manejar en entornos dinámicos, donde los usuarios entran y salen del empleo, hay contratistas, fabricantes de equipos, integradores de sistemas y los proveedores van y vienen.

El flujo constante de cambios requiere actualizaciones frecuentes a los permisos de acceso, un tiempo de proceso lento y propenso a errores [30]. Un error de seguridad común con este enfoque es la falta de actualización de permisos oportuna, pues usuarios no autorizados como empleados despedidos o viejos contratistas, podrían acceder a las funciones restringidas.

2.4.3.1.2 *Autenticación física con token.*

La autenticación física determina la autenticidad para un dispositivo o token, la persona que solicita el acceso debe tener en su posesión el token de seguridad que

en su caso puede ser una tarjeta inteligente. Cada vez más, las claves de llave pública (PKI) están siendo incorporadas en dispositivos físicos tales como bus serie universal (USB dongle). Algunas fichas admiten la autenticación de un solo factor, de manera al tener en posesión el testigo es suficiente para ser autenticado. Otros admiten la autenticación de doble factor que requiere el conocimiento de un código (PIN) o contraseña, además de poseer el testigo con el fin de ser autenticado.

2.4.3.1.3 *Vulnerabilidades de seguridad de autenticación con token.*

Para la autenticación física de un solo factor, la mayor debilidad es que la posesión material del símbolo significa que el acceso se concede (por ejemplo, cualquiera de encontrar un conjunto de llaves perdidas ahora tiene acceso a lo que abren). La autenticación con token es más segura cuando se combina con una segunda forma de autenticación, tal como un PIN memorizado. Además, los tokens requieren apoyo logístico y financiero para distribuir y administrar lo que conlleva a requerir de servidores adicionales para admitir la autenticación, lo que complicaría aún más la seguridad de una red de control.

2.4.3.2. ***Autenticación de tarjetas inteligentes.***

Las tarjetas inteligentes son similares al token de autenticación, pero pueden proporcionar funcionalidad adicional. Las tarjetas inteligentes se pueden configurar para ejecutar varias aplicaciones (de doble factor o de tres factores diferentes de autenticación), como acceder al edificio y realizar compras sin efectivo en una sola tarjeta, mientras actúa como identificación en la compañía para el individuo.

2.4.3.2.1 *Vulnerabilidades de seguridad de tarjetas inteligentes.*

La mayoría de desventajas son respecto a temas logísticos relacionados con la emisión de nuevas tarjetas, sobre todo para reemplazar tarjetas pérdidas o robadas. Por ejemplo, una tarjeta pérdida o robada proporciona cierto nivel de acceso por el buscador, también las tarjetas pérdidas o dañadas crean un bloqueo temporal para el acceso al sistema de control, lo que puede ser crítico para el funcionamiento normal de las operaciones generales. Por otro lado, la información de las tarjetas inteligentes puede ser duplicada en segundos por dispositivos electrónicos utilizados con ese fin, lo que produce una vulnerabilidad muy grande [30].

2.4.3.3. ***Autenticación biométrica.***

Determina la autenticidad mediante las características biológicas, presumiblemente únicas de quien solicita el acceso humano, las características biométricas utilizables

incluyen huellas dactilares, geometría facial, la retina y el iris, patrones de voz, patrones de mecanografía, y geometría de la mano.

2.4.3.3.1 *Vulnerabilidades de seguridad de autenticación biométrica.*

No todos los dispositivos biométricos son capaces de detectar un objeto real de una posible falsificación; por ejemplo, distinguir un verdadero dedo humano de un molde de silicona-caucho o una voz humana real de una grabación. Además, todos los dispositivos biométricos están sujetos a errores tipo I y tipo II, la probabilidad de rechazar una imagen biométrica válida y la probabilidad de aceptar una imagen biométrica no válida, respectivamente. La incapacidad temporal del dispositivo de detección para reconocer un usuario legítimo puede impedir el acceso necesario a los del sistema de control.

2.5. Herramientas para seguridad IT

Las herramientas para seguridad IT sirven para garantizar privacidad de la información y continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas y de la información contenida en ellos, así como de las redes privadas y sus recursos. Una herramienta para seguridad IT debe vigilar la privacidad, integridad, disponibilidad, seguridad física, lógica y seguridad en redes .

Garantizar privacidad significa que la información debe ser vista y manipulada solo por quien o quienes tengan el derecho de hacerlo. Asegurar integridad, implica que la información deber ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataques a la integridad es la modificación no autorizada de saldos en un sistema bancario, es decir, la modificación de números en un banco que provoca un caos en el ente financiero[31].

La información debe estar en el momento que el usuario requiera de ella, esto es disponibilidad. Un ataque a la disponibilidad es la negación de servicio (Denial of Service o DoS), que es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

La seguridad física comprende el aspecto de hardware, la manipulación del mismo, así como también del ambiente en el cual se va a instalar el equipo. La seguridad lógica, comprende tanto los sistemas operativos como las aplicaciones, y principalmente la información del usuario. Por su parte, la seguridad en redes, incluye todo lo que hace referencia a la seguridad en todas sus formas de comunicación [32]. Existen muchas herramientas para seguridad IT, aquí se mencionan, FortiNet y FortiGate, que son algunas soluciones que utiliza la empresa Gamma Ingenieros.

- **Fortinet:** esta herramienta software ofrece una seguridad amplia, verdaderamente integrada y de alto rendimiento en toda la infraestructura de TI. Proporciona seguridad de contenido y red de primera categoría, así como productos de acceso seguro que comparten inteligencia. Brinda una plataforma de firewall empresarial llamada *FortiGate,* disponible en una amplia gama de tamaños y factores que se adapta a cualquier entorno y proporciona funciones de red y seguridad de próxima generación [33].

- **FortiGate:** permite una infraestructura de seguridad de extremo a extremo simplificada que cubre seguridad de la red, seguridad multi-nube, seguridad de aplicaciones web, seguridad del correo, protección avanzada contra amenazas, acceso unificado seguro, puesto final de seguridad, gestión y análisis.

2.6. Herramientas para seguridad OT

Existen diferentes herramientas para seguridad OT, aquí se mencionan Nozomi Network, Nesus, Indegy y carbón black, que son soluciones utilizadas por la empresa Gamma Ingenieros.

- **NOZOMI NETWORKS**: visualiza redes industriales en tiempo real y realiza inventarios de activos y supervisión de la red, además de administrar rápidamente las amenazas cibernéticas y los riesgos del proceso con una solución que correlaciona múltiples técnicas avanzadas de detección [34]. Esta herramienta solo se ofrece en modo licenciado, lo que quiere decir que cuando se termina el contrato con la empresa, así se tenga el hardware del equipo de nozomi, el software no trabajará para la detección de alertas y no actualizara la base de firmas.

- **Nessus**: es la solución de evaluación de vulnerabilidades estándar de la industria para identificar y reparar vulnerabilidades con rapidez y facilidad, incluso fallas de software, parches faltantes, malware y configuraciones erróneas, en una gran variedad de sistemas operativos, dispositivos y aplicaciones[35]. Esta solución se puede encontrar en modo licenciado y no licenciado, en el modo pago tienen acceso a más herramientas, por ejemplo, a un pool con todo el contenido para entornos OT.

- **Indegy**: protege la infraestructura crítica de las amenazas cibernéticas, informantes maliciosos y los errores humanos, ofreciendo un conjunto completo de capacidades de seguridad OT de clase empresarial, con una flexibilidad y escalabilidad, garantizando la seguridad y confiabilidad de los entornos complejos de sistemas de control industrial [36]. Esta herramienta se ofrece en

una versión gratuita, donde se realiza un cheque de actividades de la red OT y se genera una información que luego es enviada a los laboratorios de indegy para realizar un diagnóstico del estado de la red OT, adicionalmente se ofrece la parte licenciada donde se cuenta con el diagnóstico de en tiempo real y con firmas actualizadas automáticamente.

- **Carbon black**: realiza un análisis sofisticado de poder y agilidad computacional en la nube. Con la plataforma CB Predictive Security Cloud, transforma la ciberseguridad con una nueva generación de soluciones en la nube diseñadas para protegerse contra las amenazas más avanzadas. Aprovecha plantillas, herramientas y mejora las prácticas establecidas en miles de implementaciones para guiar de manera eficiente en la configuración necesaria para abordar requisitos específicos de seguridad.

  Asegura sistemas críticos, protegiendo los dispositivos corporativos, los servidores críticos y los dispositivos de función fija, como los ICS, de ataques de malware y no malware. Realiza control de entorno, evitando la ejecución no autorizada de software para supervisar y controlar los cambios de archivos/sistemas, garantiza las configuraciones de aplicación adecuadas en los sistemas SCADA, incluso en aquellos que están al final de su vida útil. Además, realiza funciones de detección y respuesta, aprovechando las capacidades de detección en la industria para descubrir brechas en las defensas y evitar futuros ataques [37]

Capítulo III

3. Proceso de desarrollo

La empresa Gamma Ingenieros planteó la necesidad de implementar un prototipo de red OT, que permitiera realizar diagnóstico de vulnerabilidades de seguridad usando las herramientas de Nozomi Network. Para dar cumplimiento a este requerimiento, se plantearon dos fases: el diseño del prototipo de red OT y la implementación del prototipo de red OT.

3.1. Diseño de prototipo de red OT

Para realizar el diseño del prototipo de red OT, se llevaron a cabo reuniones tanto presenciales como virtuales con los ingenieros encargados del proyecto en la empresa Gamma Ingenieros, con el objetivo de definir sus requerimientos respecto al prototipo. Los requerimientos definidos por la empresa, incluyendo tipo de instrumentación a usar, el protocolo de comunicación, equipos de infraestructura de red OT y equipos para detección de anomalías en la Tabla 1.

Requerimiento	Especificación
Características del prototipo	El prototipo debe ser portable para diagnosticar fallas en vivo
Tipo de proceso industrial a controlar	No se requiere un proceso complejo, se define un control de nivel.
Tipos de sensores/actuadores	Sensores y actuadores digitales
Tipo de controlador	PLC de Allen Bradley (micrologix1100)
Protocolo de comunicación	Ethernet
Alimentación	AC o DC
Equipos de infraestructura de red OT	FORTINET
Equipo para detección de anomalías	NOZOMI NETWORKS

Tabla 1: Requerimientos para Prototipo de red OT. Fuente propia

Teniendo en cuenta los requerimientos planteados, se define el diseño planteado en la Figura 5. El prototipo estará compuesto por un controlador micrologix 1100 de Allen Bradley, un ordenador, un switch 112D de FORTINET, un firewall FortiGate 30D de FORTINET y un dispositivo para análisis de tráfico, NOZOMI P500.

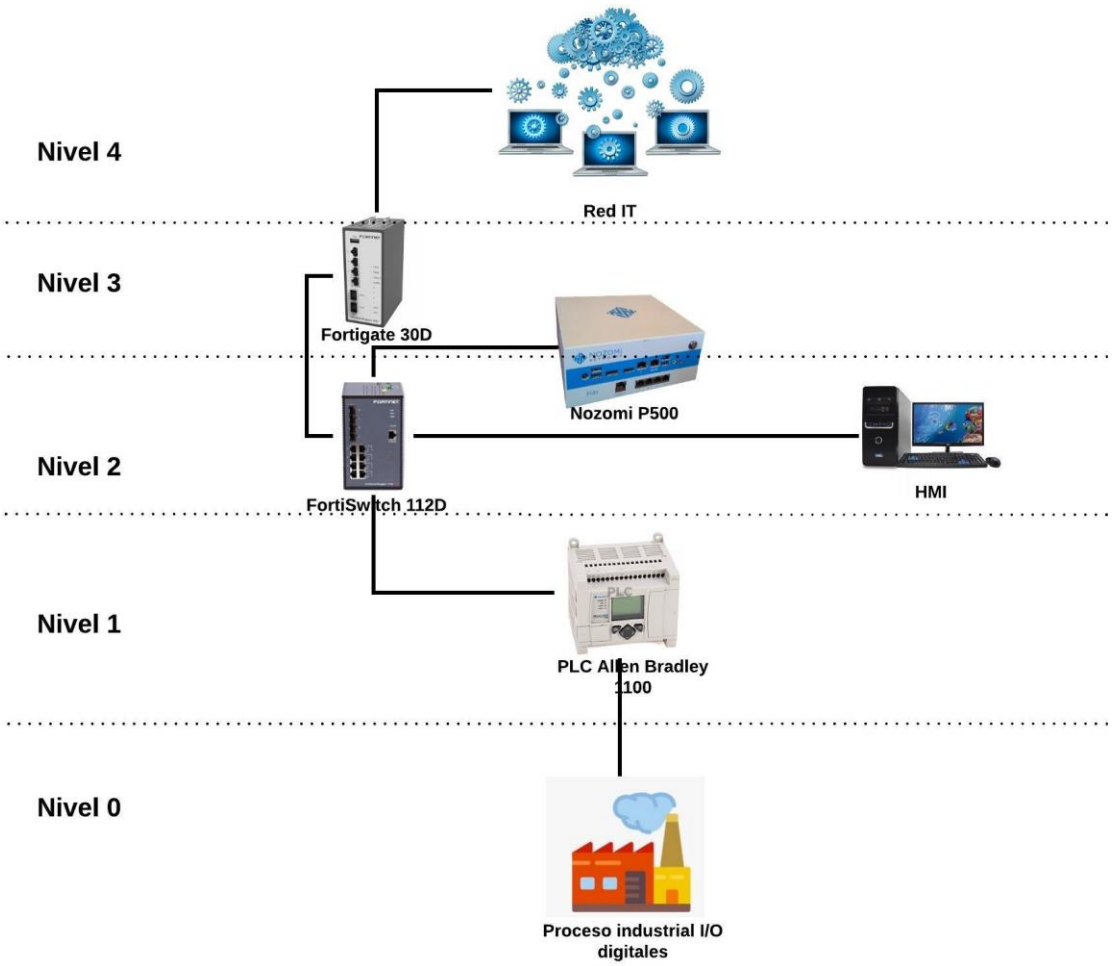


Figura 5: Arquitectura de prototipo de red OT a implementar. Fuente propia

3.1.1. Componentes de la arquitectura de red OT.

Los componentes usados en esta arquitectura se seleccionaron de acuerdo a los partner y proveedores que tiene la empresa Gamma ingenieros. Se utilizaron equipos de Fortinet y Nozomi networks, ambos son grandes fabricantes de equipos para seguridad IT y OT que se complementan para implementar arquitecturas de red seguras e integradas. Por otra parte, la empresa Gamma ingenieros está incursionando en el ámbito de OT y ha realizado una alianza con el proveedor Allen Bradley, se definió entonces un controlador de micro Logix 1100 de Allen Bradley que cumplía a los requerimientos definidos para el prototipo de red OT, en cuanto a memoria, velocidad de procesamiento, y cantidad de entradas y salidas digitales para controlar el proceso de nivel.

Los equipos mencionados anteriormente integran una red OT, formando una arquitectura de seguridad para el control de las vulnerabilidades entre la red de control y la red operación, se crearán dos redes en el Switch en forma de Vlans con el propósito de diferenciar el control del proceso y la adquisición de datos. La función del equipo de Nozomi en esta arquitectura es de escuchar todo este tráfico entre las dos Vlans para determinar si en el trascurso de ese tráfico hay paquetes maliciosos o vulnerabilidades de seguridad. Todo este proceso lo realiza de forma pasiva, lo que quiere decir que no afecta al proceso ni pone retrasos en el tráfico que está capturando. La Tabla 2 resume la funcionalidad de cada componente del prototipo de red OT.

Dispositivo	Función
Fortigate 30D	Es un firewall del fabricante FORTINET, es el encargado de proteger la red y poder realizar filtros, pero además corregir vulnerabilidades de la red OT
FortiSwitch 112D	Es un switch del fabricante FORTINET, se conectará los dispositivos finales o host y se crearan dos redes tipo VLAN para administrar la red de control y la red de operación
NOZOMI P500	Dispositivo para analizar el tráfico o información con el fin de realizar un diagnóstico de las vulnerabilidades presentadas en toda la red OT
PLC Allen Bradley 1100	Dispositivo electrónico programable que llevará el control de las variables digitales del proceso, en este caso son 3 entradas y 5 salidas
PC	En este ordenador se programará el HMI que administrará el proceso industrial de la red OT.

Tabla 2: Descripción de dispositivos de red OT. Fuente propia

3.1.2. Metodología utilizada para el análisis de vulnerabilidades.

Durante la fase de diseño, también se definió en reuniones con Gamma Ingenieros, la metodología para diagnosticar las vulnerabilidades del prototipo de red OT planteado. La metodología definida consiste en seis fases descritas en la Figura 6, éstas se basan en planteamientos del fabricante Nozomi Networks, el producto (NOZOMO P500) usado está diseñado con inteligencia artificial para que pueda determinar cuándo un equipo anormal o algún tipo de vulnerabilidad existe y así poder alertar para dar atención inmediata al caso.

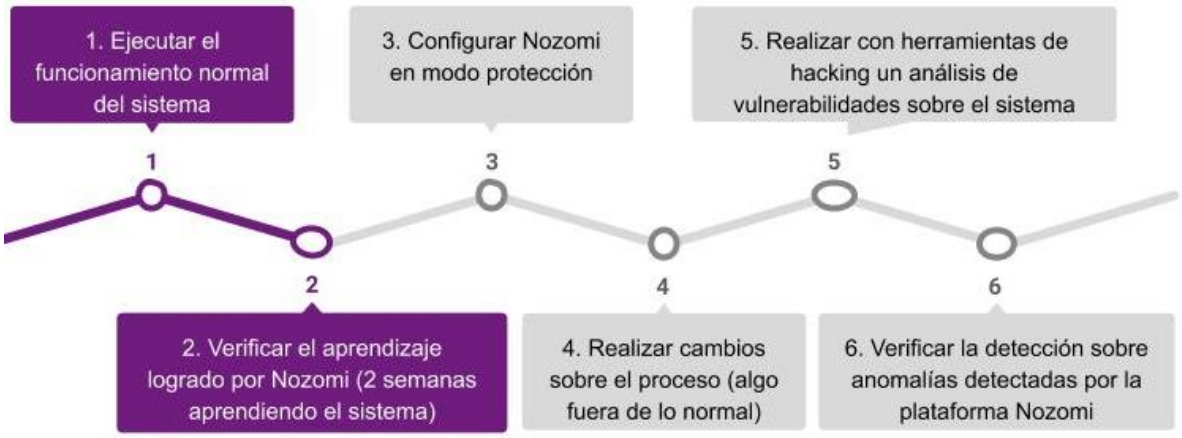


Figura 6: Metodología para diagnósticos de vulnerabilidades. Fuente propia

3.2. Implementación de prototipo de red OT

Para desarrollar el prototipo de red OT definido en la fase de diseño, se procede a implementar el prototipo de planta industrial a controlar, realizar el programa de Ladder para el control de prototipo de planta, programar la interfaz hombre-máquina (HMI), conectar y configurar los equipos de infraestructura de red (PC, PLC, Switch, firewall y dispositivo de análisis de tráfico) y realizar las pruebas de comunicación en la red OT.

En la figura 7 se presenta el diagrama P&ID del proceso de nivel a implementar, el cual se realiza en los siguientes pasos: extracción de líquido desde los tanques de almacenamiento, dosificación de los tanques y para finalizar el mezclado del producto.
La instrumentación utilizada en el nivel 0 para la extracción de las variables físicas, se utilizó 3 sensores de nivel, dos válvulas solenoides y dos motobombas.

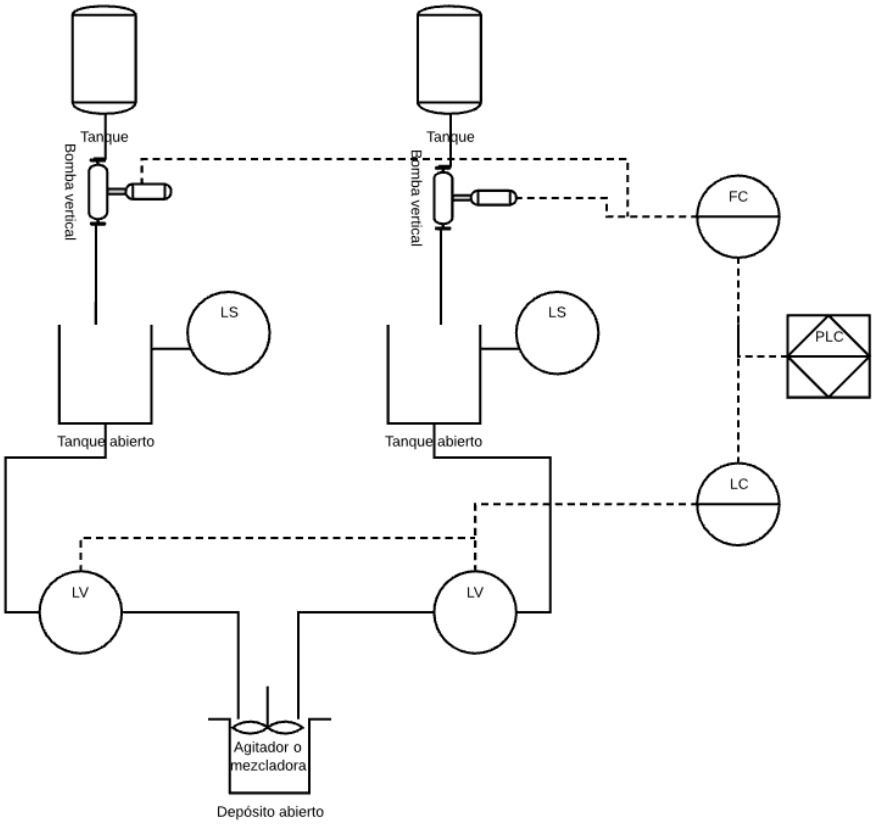


Figura 7: P&ID del proceso de nivel

En la figura 8 se observa el diagrama de conexiones eléctricas el cual se llevó a cabo para la instalación y conexiones físicas de todos los equipos mencionados en el proceso de nivel, todos los dispositivos fueron adicionados al PLC Allen Bradley para luego en fases previas realizar la configuración y funcionamiento del proceso de nivel

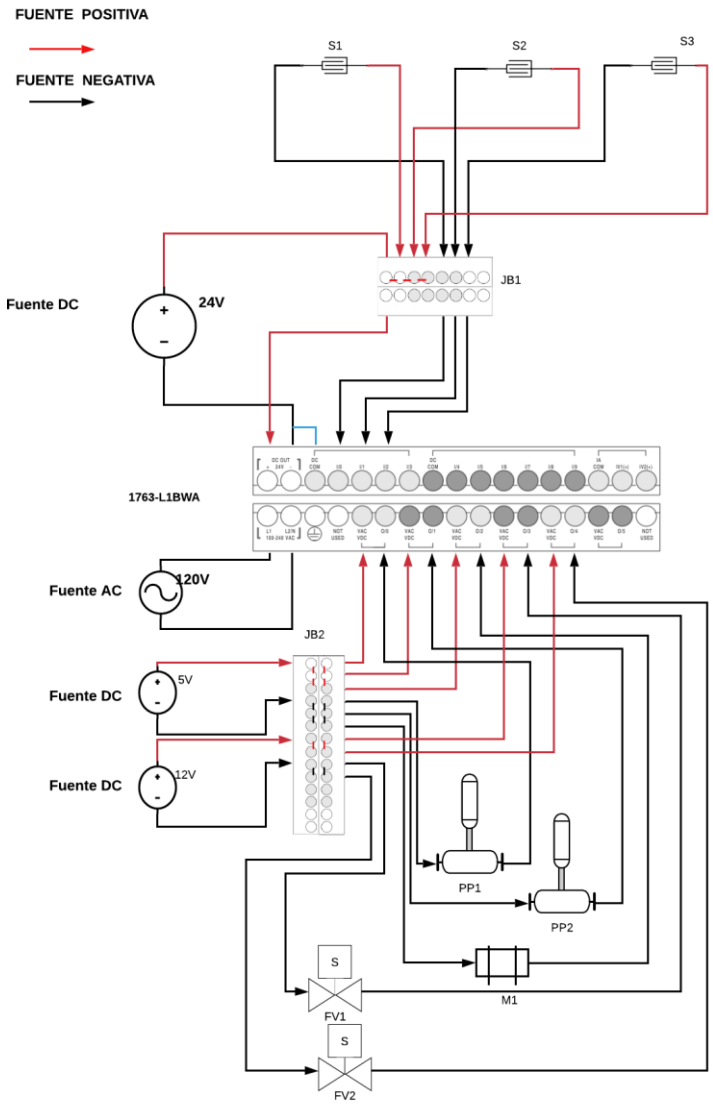


Figura 8: Esquema de conexiones eléctricas

3.2.1. Construcción maqueta de planta de nivel.

Se realiza el cableado del prototipo de planta de control de nivel. Esta consta de dos tanques de almacenamiento del producto, el cual es llevado por dos bombas verticales hasta dos tanques de dosificación. Luego, el líquido es vaciado a través de dos válvulas solenoides (accionadas por dos interruptores de nivel) hacia un tanque más grande equipado con un motor eléctrico, que se encarga de agitar la mezcla. El modelo de la planta se presenta en la Figura 9, los materiales usados en la Tabla 2 y la construcción final de la planta en la Figura 10.

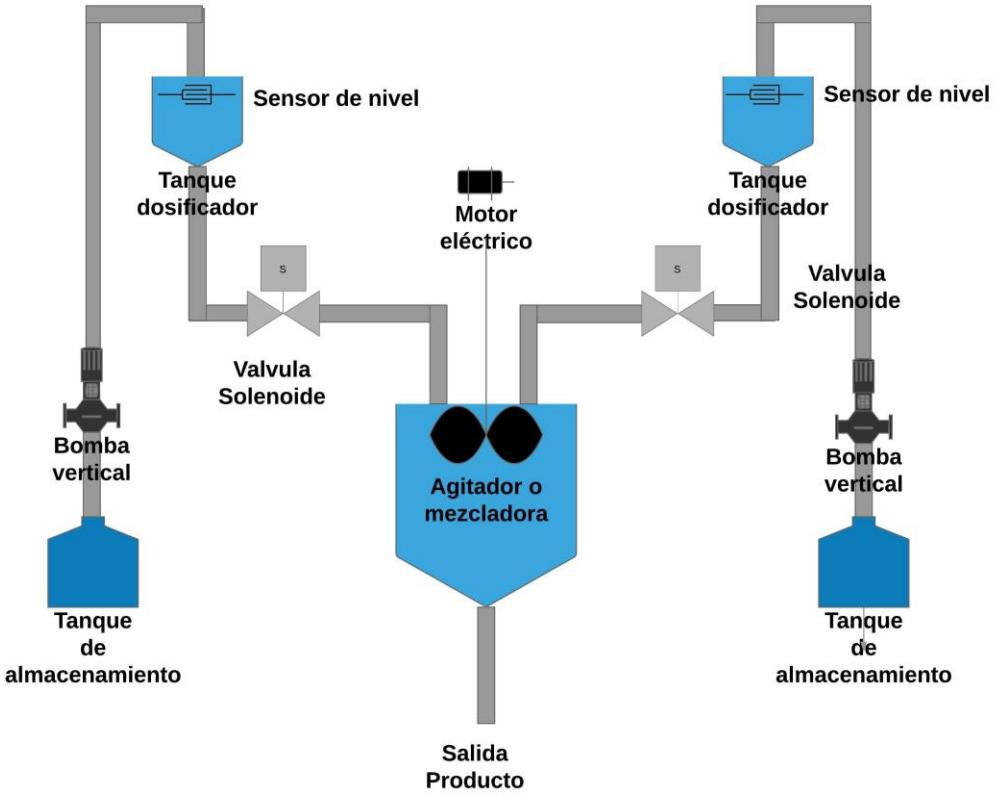
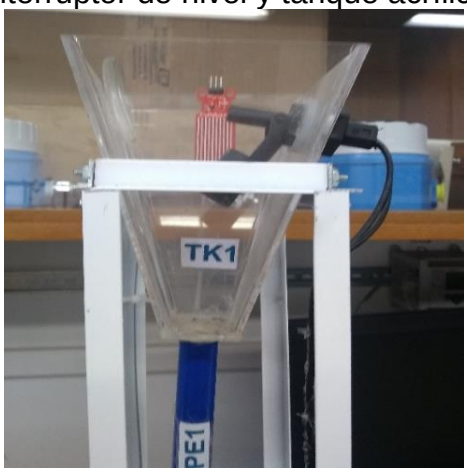


Figura 9: Modelo planta de nivel. Fuente propia

Válvula solenoide 12VDC	Interruptor de nivel y tanque acrílico
	

Motobombas 5V DC 	Motor 5v DC 
PLC Allen Bradley 1100 serie A 	Mezclador 

Tabla 3: construcción de prototipo. Fuente propia

Figura 10: Construcción final maqueta. Fuente Propia

3.2.2. Programa de control de la planta de nivel.

En la fase de diseño se definió emplear un PLC Micrologix 1100 para realizar el control de la planta de nivel. Por tanto, se requiere de la suite de software de Rockwell Automation equipada con RSLinx Classic Gateway, RSLogix 500 y BOOTP/DHCP Server.

- RSLinx Classic Gateway: este software permite crear el driver de conexión al PLC según se requiera. En este caso se usó un driver Ethernet, para realizar la descarga del código Ladder al PLC.
- RSLogix 500: es el software de programación de lenguaje LADDER que posteriormente se carga al PLC
- BOOTP/DHCP Server: este software permite configurar una dirección IP al PLC a través de la dirección MAC del dispositivo.

Es necesario configurar una dirección IP al PLC mediante el software BOOTP/DHCP SERVER y establecer una red punto a punto a través de ethernet con el ordenador. El programa LADDER inicia y realiza un paro de emergencia a través de contactos normalmente abierto y normalmente cerrado, respectivamente. Luego de iniciar el proceso, se activan las dos motobombas que llevan el contenido de los tanques de almacenamiento (TK1 y TK2) hacia el tanque mezclador (TK3), a través de la activación de los sensores de nivel (nivel alto) y la desactivación de las válvulas solenoides; finalmente, el contenido del tanque mezclador es agitado con la activación del motor. (ver configuración en anexo I, numeral 1). La Figura 11 muestra una vista general del programa Ladder realizado en RsLogix500 para el control del prototipo de planta realizado.

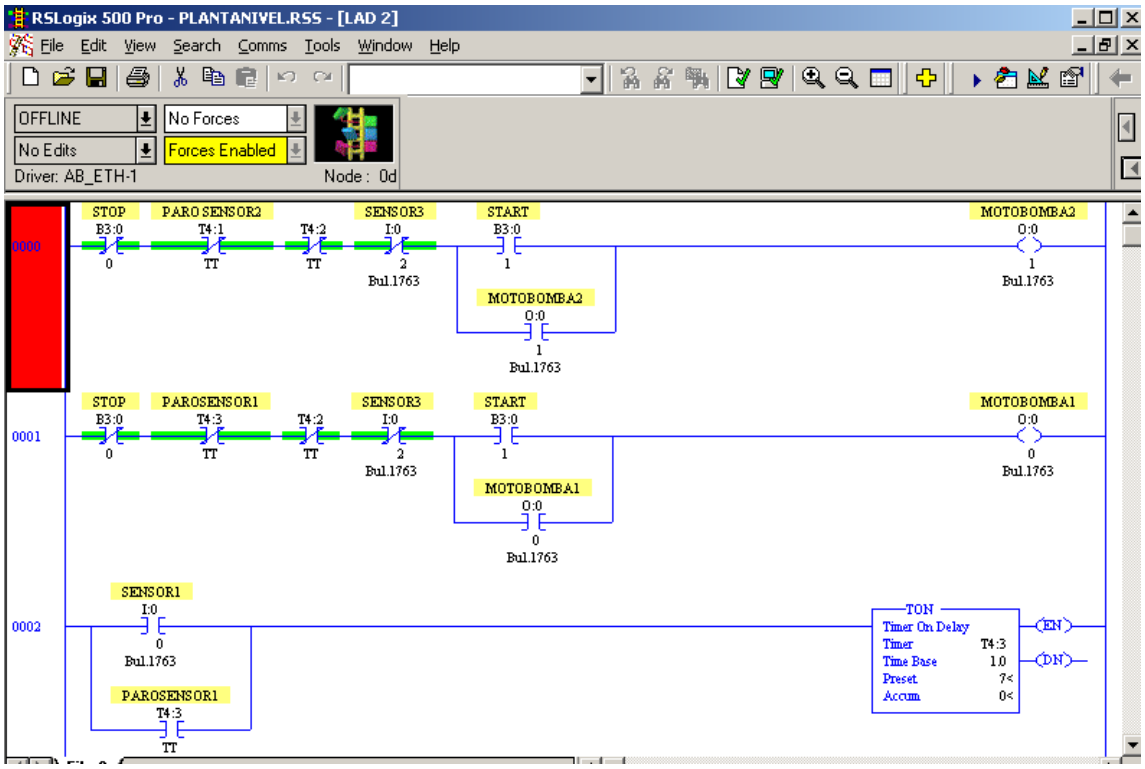


Figura 11:Programa en código LADDER. Fuente propia

3.2.3. Interfaz hombre máquina para la planta de control de nivel.

Para desarrollar la interfaz hombre máquina de la planta de control de nivel, se utilizó el software Factory Talk View ME de la suite de Rockwell Automation. Factory Talk View ME permite crear interfaces hombre máquina (HMI) para supervisar y controlar procesos industriales. En el HMI de la planta se requiere iniciar y parar el proceso, visualizar el estado del proceso y el funcionamiento de la instrumentación, teniendo en cuenta el perfil del tipo de usuario que ingresa al sistema: si es operario

solo podrá supervisar el funcionamiento del proceso, pero si es controlador podrá iniciar, parar y manipular el proceso.

La Figura 12 muestra el inicio de sesión de un usuario tipo controlador, como indica el recuadro rojo; este usuario tiene todos los permisos, por tanto, inicia y para el proceso e ingresa a la visualización de los instrumentos, para saber la actividad de los mismos como se muestra en la Figura 13.

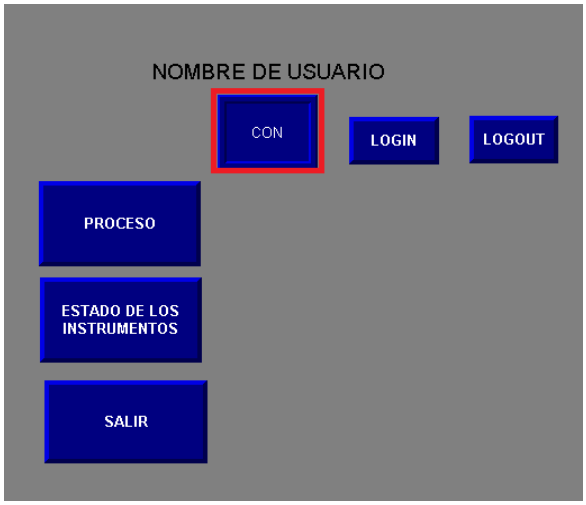


Figura 12: interfaz HMI. Fuente propia

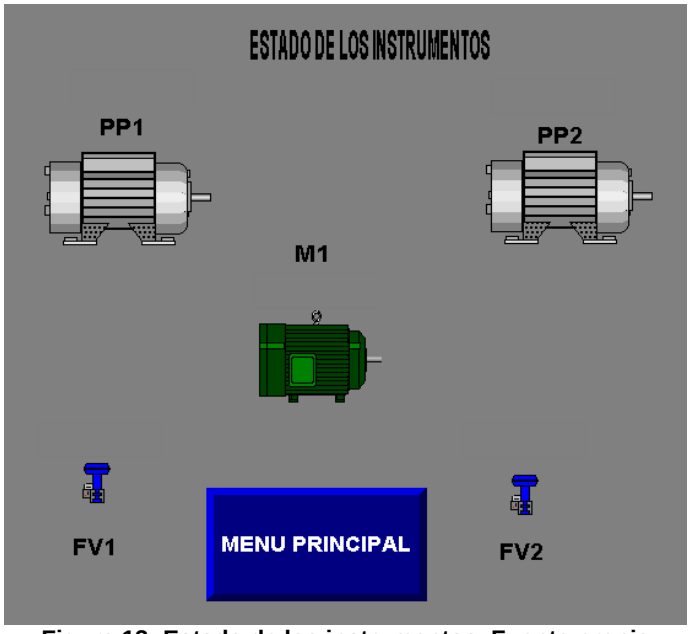


Figura 13: Estado de los instrumentos. Fuente propia

Para la integración del programa de control del PLC realizado en RSLogix y la interfaz hombre-máquina se realizó una conexión OPC Data Server a través del software RSLinx. (Ver esta configuración en anexo I, numeral 2)

3.2.4. Conexión y configuración de prototipo de red OT.

Para la conexión y configuración del prototipo de red se conectan todos componentes ya mencionados de la red OT (ver Figura 5) y se configura el FortiGate 30D, activando cada uno de los puertos donde se van a realizar conexiones. También, se realiza la configuración de la interconexión entre Switch y el FortiGate con el fin de gestionar toda la red desde el FortiGate. Para la segmentación de la red SCADA se crean dos Vlans para gestionar el control (Vlan 1, en la cual se encuentra el PLC y su equipo para realizar su descargar el código Ladder) y la operación (Vlan 2, en la cual se encuentra el equipo para operar el proceso a través de la HMI) con el fin de capturar el tráfico entre las dos redes. (Ver esta configuración en anexo II, numeral 1).

3.2.5. Pruebas de comunicación en red OT.

En las pruebas de comunicación se realizó la gestión del equipo NOZOMI P500 a través del FortiGate, luego de tener la gestión de todos los equipos de la red OT a través de la asignación de los segmentos lógicos de Vlans a los puertos físicos, y para finalizar se crearon todas las políticas de comunicación de la red OT, entre las comunicaciones de la red de operación y red de control. (Ver esta configuración en anexo II, numeral 2).

Las políticas de comunicación se realizan para gestionar toda la red OT a través del equipo FORTIGATE, así se puede gestionar la red independientemente de la ubicación geográfica de los dispositivos. Con la creación de las Vlans, se segmenta la red y su vez se divide para proteger la red control y la red de operación de la red IT que puede comunicarse a internet, así con esa intención se segmenta la red con otro tipo de direccionamiento para que estas redes solo permitan el acceso a operarios o controladores de la red.

3.2.6. Funcionalidades de Nozomi networks.

Se realizaron pruebas sobre las funcionalidades de las herramientas de NOZOMI NETWORKS, entre ellas se encuentran el inventario, visualización y seguimiento de activos. Estas herramientas son de gran ayuda para los administradores de red y prestan un servicio muy importante para las empresas del sector industrial, a continuación, se describe cada una de ellas.

3.2.6.1. *Inventario de activos de red OT.*

Desarrolla y mantiene un inventario centralizado del sistema de red OT. Nozomi a través de su herramienta SCADAguardian aborda la identificación de los activos de manera no intrusiva, manteniéndolos hasta a la fecha; además, de realizar todo el seguimiento en tiempo real. En la Figura 14 se identifica el PLC MicroLogix 1100, en la parte derecha de la imagen se observa todo lo relacionado a información del equipo como: fabricante, dirección MAC, dirección IP y la Vlan a la cual pertenece. En la parte izquierda de la imagen se observa el PLC y todas las conexiones salientes de todos los equipos con los que intercambia información o paquetes.

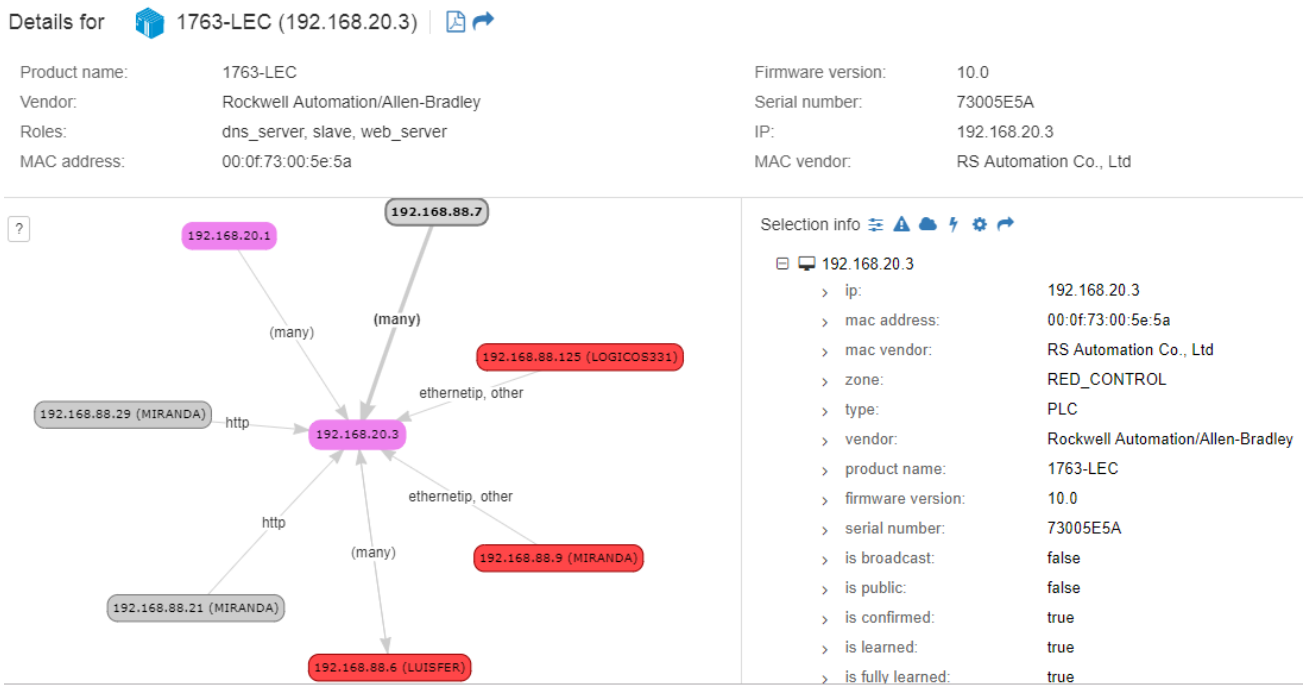


Figura 14: Activos de red OT. Fuente propia

3.2.6.2. *Visualización de red OT.*

El Nozomi P500 analiza el tráfico de red de un ICS y construye una visualización interactiva, en vivo de ella. Identifica todas las entidades que se comunican a través de la red, incluyendo las entidades con una dirección IP o MAC; dispositivos sin direcciones IP, como los que se comunican en la capa 2 del modelo OSI y dispositivos serie anidados detrás de equipos de redes, tales como puertas de enlace.

Nozomi P500 incluye otras capacidades de visualización de red: una pantalla que muestra los protocolos utilizados para la comunicación entre nodos y entre las

zonas; información de tráfico de red como el rendimiento y los protocolos de conexión TCP abierta; visualización de múltiples sitios distribuidos geográficamente, cuando se instala con la consola de administración central; versiones imprimibles y exportables de la estructura de la red y sus detalles, en múltiples formatos de archivo.

La figura 15 muestra la visualización del prototipo de red, explícitamente el nodo llamado LUISFER, con sus conexiones en toda la red OT y mostrando el protocolo utilizado en específico para la comunicación. Esta visualización se realiza en tiempo real, por tal motivo si alguna comunicación se termina el administrador de red podría darse cuenta de forma inmediata.

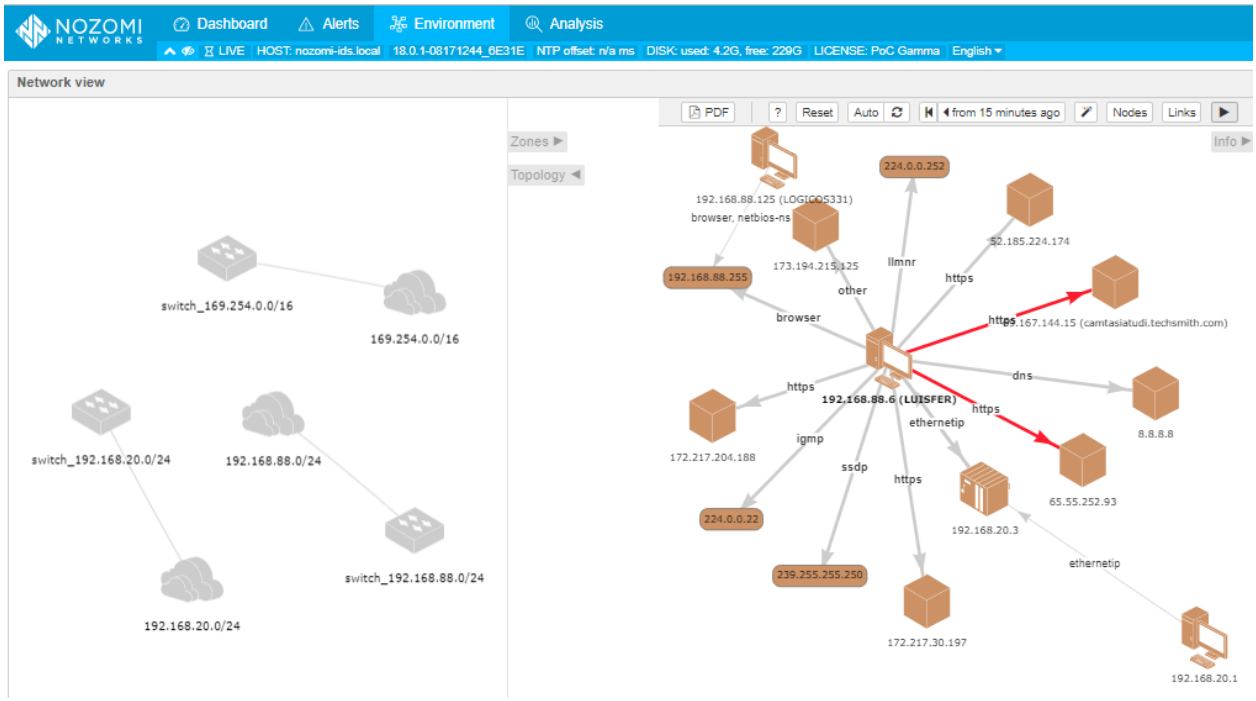


Figura 15: Visualización de Red OT. Fuente propia

3.2.6.3. *Seguimiento de todos los tipos de activos y redes.*

Nozomi Networks identifica los dispositivos de todos los fabricantes, incluyendo los activos heredados, asignando automáticamente los segmentos para cada nivel de red. La figura 16 muestra el diagrama de red en el modelo de Purdue, dividiendo la infraestructura de red OT en cada nivel: en el nivel 0 se muestra el FortiSwitch, en el nivel 1 se observa el PLC y la versión de su firmware, en nivel 2 se observan los equipos de la red de operación donde se encuentra el HMI y los equipos de prueba para realizar ataques a la red OT.

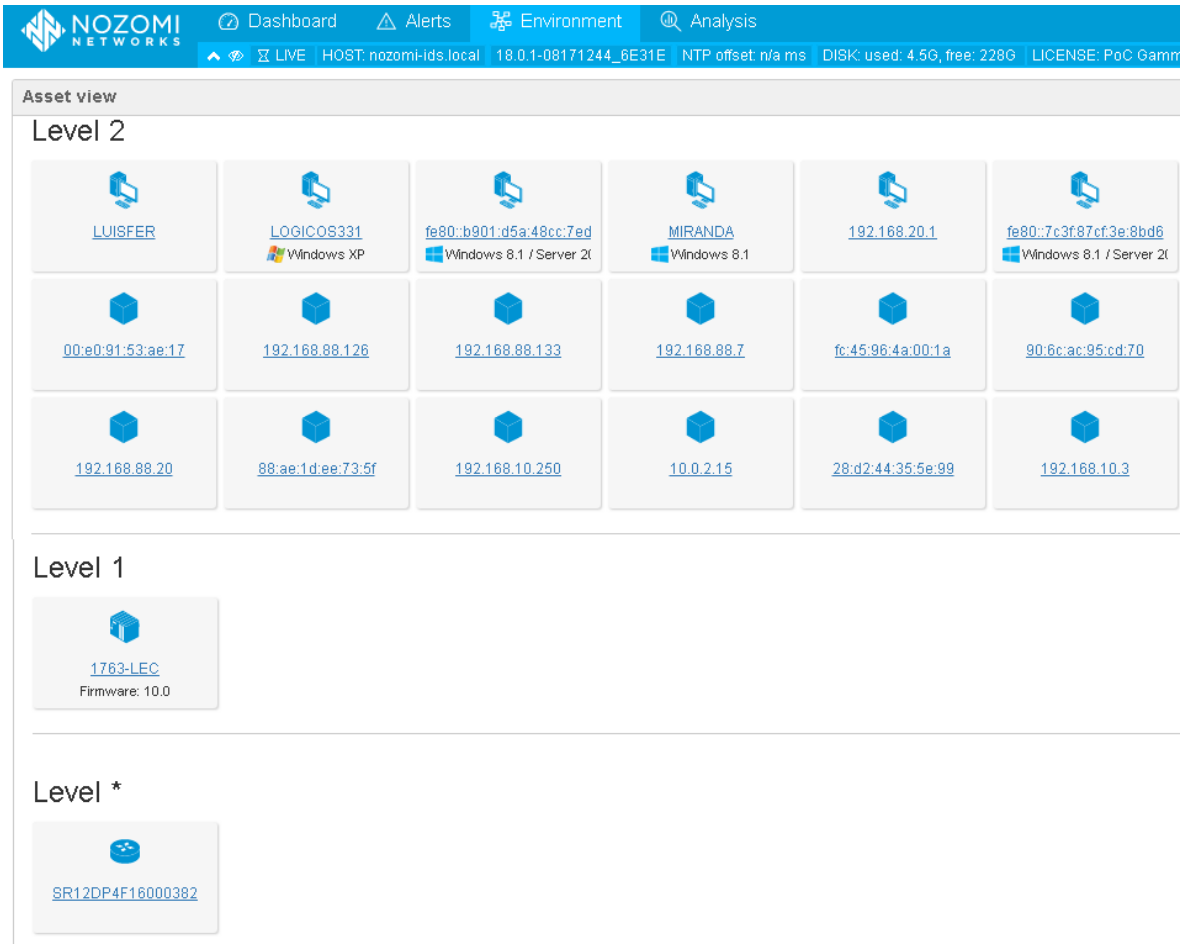


Figura 16: Seguimiento de activos. Fuente propia

Hasta aquí se ha realizado la implementación y configuración del prototipo de red, en el capítulo cuatro se realizará el análisis de vulnerabilidades en el prototipo de red OT implementado, para ello se utiliza la herramienta de NOZOMI NETWORKS y herramientas de hacking para realizar la detección de vulnerabilidades y anomalías.

Capítulo IV

4. Análisis de vulnerabilidades en el prototipo de red OT implementado

El análisis y diagnóstico de vulnerabilidades del prototipo de red OT, se realizó siguiendo la metodología definida previamente por la empresa Gamma Ingenieros (ver capítulo III numeral 3.1.2.).

4.1. Ejecución del funcionamiento normal del sistema

El funcionamiento normal del sistema se refiere al funcionamiento normal del proceso, en el cual todos los dispositivos necesarios para ejecutar el proceso de nivel se encuentran operando. Como por ejemplo el HMI, PLC, válvulas, motobomba, válvula solenoide y los sensores de nivel.
En este escenario el funcionamiento se produce durante un tiempo determinado, en este caso de estudio se estableció un período dos semanas. Para definir esta etapa de funcionamiento normal, se configuró el equipo de NOZOMI seleccionando */administration/learning/* como se muestra en la Figura 17 y luego, escribiendo el tiempo de aprendizaje que sería *2w (2 semanas),* tal como se indica en la Figura 18.

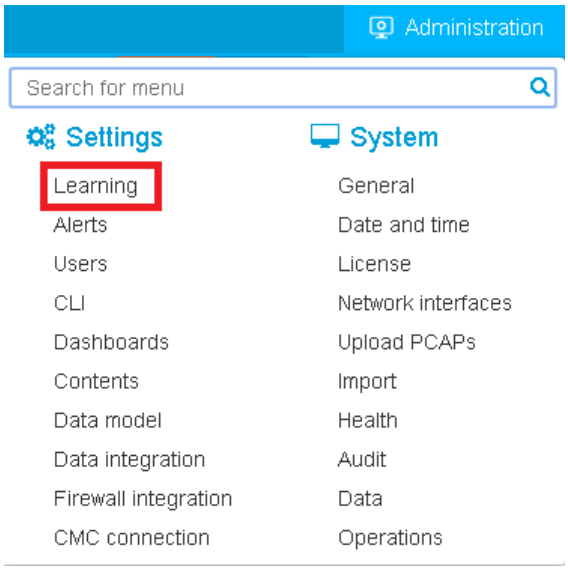


Figura 17: Fase de aprendizaje de NOZOMI. Fuente propia

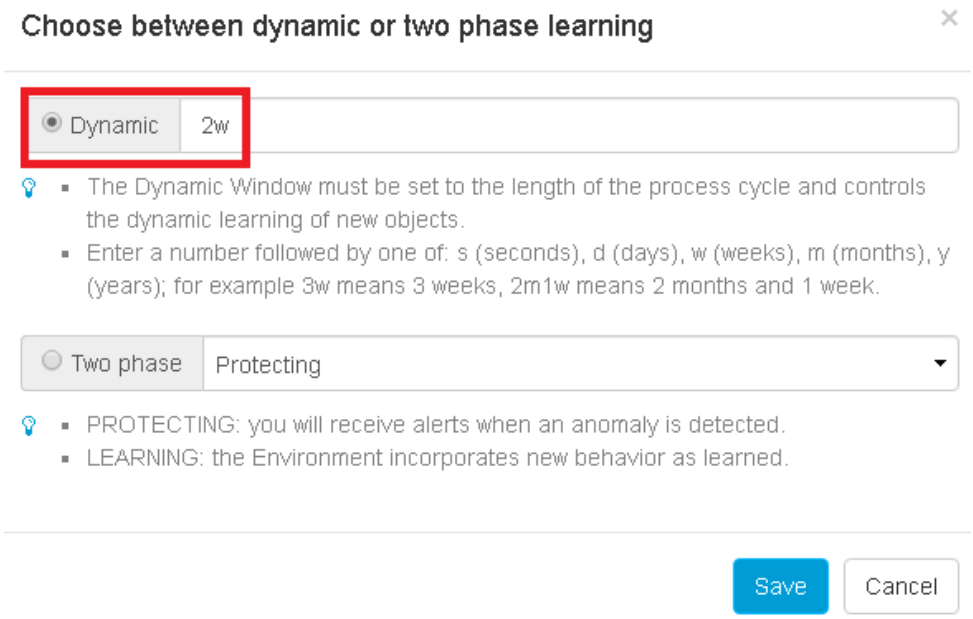


Figura 18: Selección de tiempo de Aprendizaje. Fuente propia

4.2. Verificar aprendizaje

Esta etapa es muy importante, ya que se confirma que las configuraciones y la ingesta de tráfico al dispositivo de NOZOMI NETWORKS es satisfactoria. La forma de saberlo es que al ingresar a la opción learning, se puede observar una línea de aprendizaje a través del software SCADA GUARDIAN, permitiendo ver la cantidad de nodos y conexiones entre los dispositivos.

En la Figura 19 se observa los nodos como “nodes” y las conexiones entre dispositivos como Links, para el caso de estudio se tenían 6 nodos y 2 links.

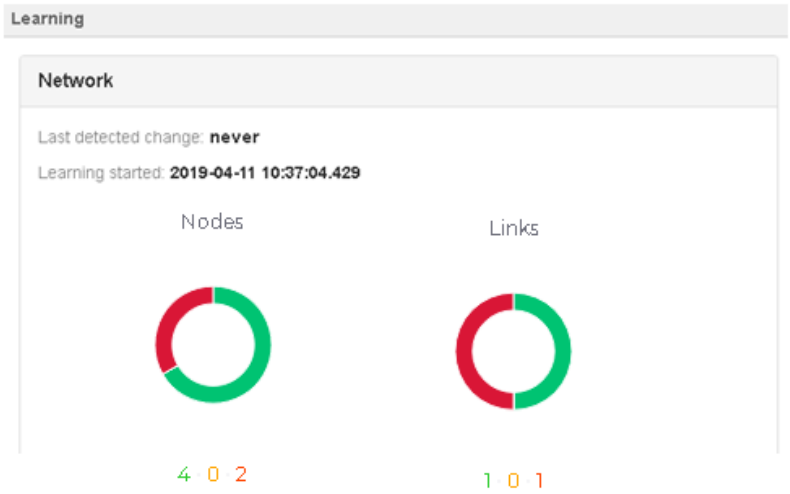


Figura 19: Aprendizaje Nozomi. Fuente propia

4.3. Configuración de NOZOMI en modo protección

Una vez concluido y verificado el período de aprendizaje del proceso configurado, ingresamos al modo de aprendizaje nuevamente (ver Figura 17), pero ahora se configura en modo protección, como se indica en la Figura 20. El objetivo de configurarlo en modo protección es poner a prueba toda la fase de aprendizaje en la que el equipo de NOZOMI, a través de inteligencia artificial realiza una predicción de las actividades que se denominan como “normales” durante el proceso de la red OT, luego si algo fuera de lo normal realizado durante la fase de protección, el equipo realizara la respectiva alerta sobre este suceso, para así tomar medidas respectivas al caso.

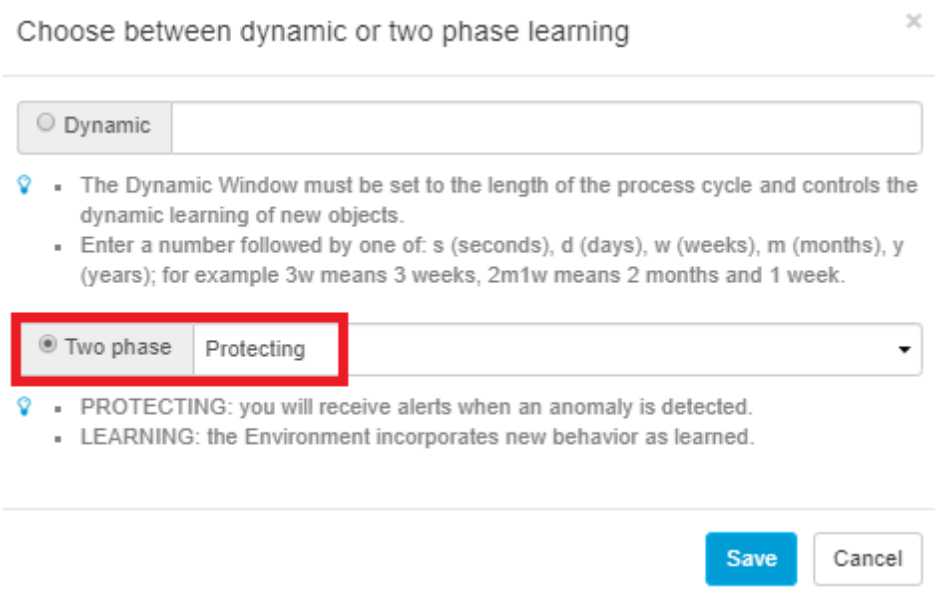


Figura 20: Configuración modo aprendizaje. Fuente propia

4.4. Realizar cambios sobre el proceso

El cambio realizado en el proceso se refiere a realizar conexiones de equipos que no estaban conectados a la red OT en la fase de aprendizaje, además, a realizar conexiones distintas de las habituales en el proceso que aprendió durante dos semanas. Para el caso de estudio los cambios realizados fueron: conexiones nuevas de dispositivos identificados con nuevas direcciones IP (en las VLAN red de control y red de operación), realizar descargas de programas LADDER desde un HMI diferente al utilizado anteriormente.

4.5. Herramientas de hacking para analizar vulnerabilidades

4.5.1. Escaneo de puertos abiertos con NMAP.

Nmap (Network Mapper) es un código libre y abierto, utilizado para el descubrimiento de redes y la auditoría de seguridad. Muchos administradores de sistemas y redes también lo encuentran útil para tareas como el inventario de la red, la administración de los horarios de actualización del servicio y la supervisión del tiempo de actividad del host o del servicio [38].

Como se observa en la Figura 19 el PLC MicroLogix 1100 tiene asignada la dirección IP 192.168.20.3. Además, tiene abiertos los puertos 80/TCP, 2000/TCP y el 5060/TCP. Lo que indica que es vulnerable al tener estos puertos abiertos, por

ejemplo, un ataque DoS se puede realizar en el puerto 80/TCP y así se caerá el servicio del servidor web del PLC.

Para analizar las vulnerabilidades del prototipo de red OT, se definió con el equipo de Gamma Ingenieros utilizar Nmap para realizar escáneo de puertos abiertos y además, realizar un ataque activo tipo denegación del servicio al servidor web del PLC micrologix 1100. El servidor web del PLC permite acceder remotamente a los datos del controlador utilizando una red con un navegador. Utilizar un navegador web para monitorear datos en tiempo real de un controlador es realmente una gran ventaja.

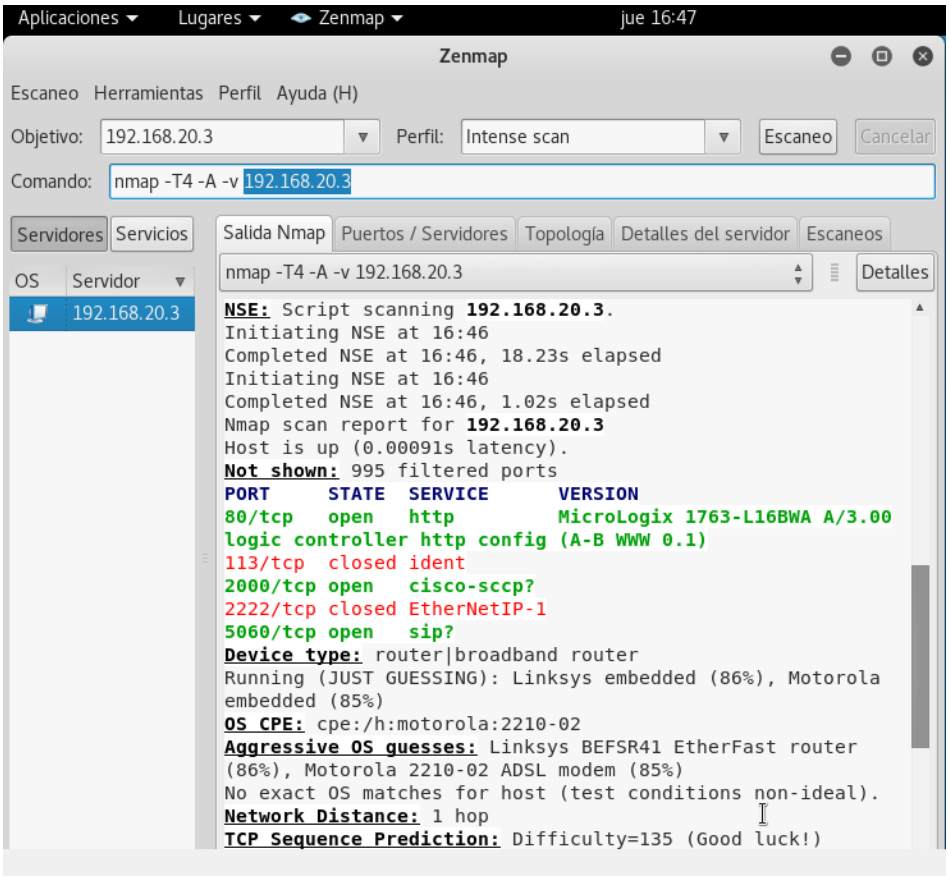


Figura 21:Escaneo de puertos con Zenmap. Fuente propia

4.5.2. Ataque DoS con kali-linux.

Se definió en conjunto con Gamma Ingenieros, realizar el ataque al servidor web del PLC mediante Dos con Kali-linux. En las figuras 22 y 23 se da inicio al script para el ataque DoS en el servidor web del PLC, en la figura 24 se observa el antes del ataque y en figura 25 el después del ataque. El resultado muestra que,

efectivamente con el ataque de denegación de servicio se cae el servicio del servidor web del controlador.

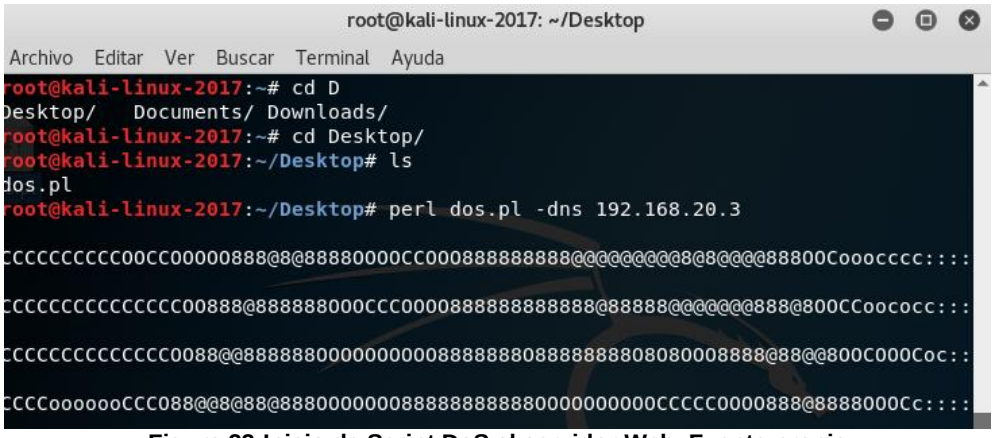


Figura 22:Inicio de Script DoS al servidor Web. Fuente propia

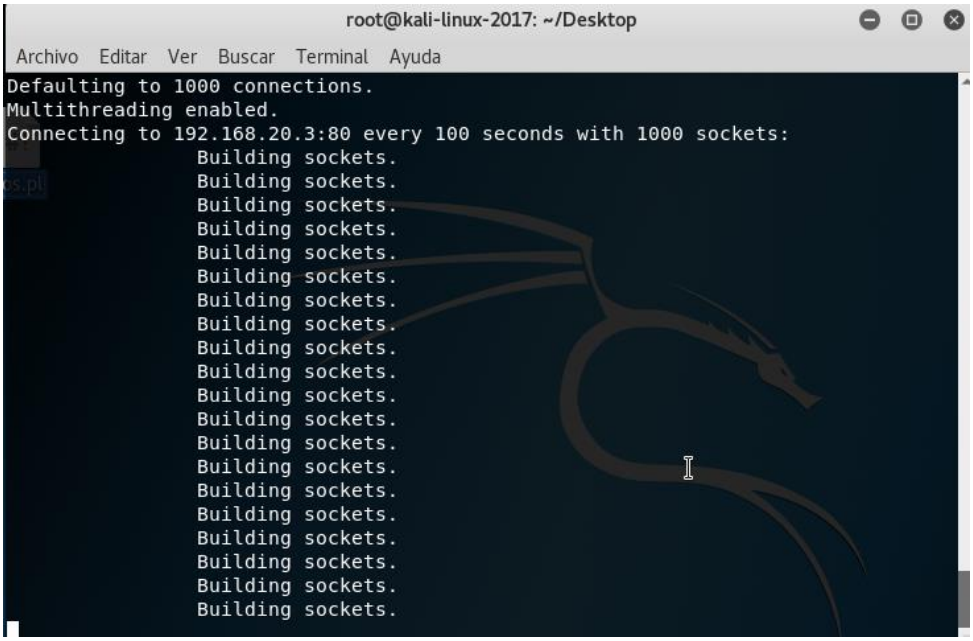


Figura 23: Intento de conexiones al servidor Web a través del puerto 80. Fuente propia

Figura 24: Antes del ataque DoS. Fuente propia

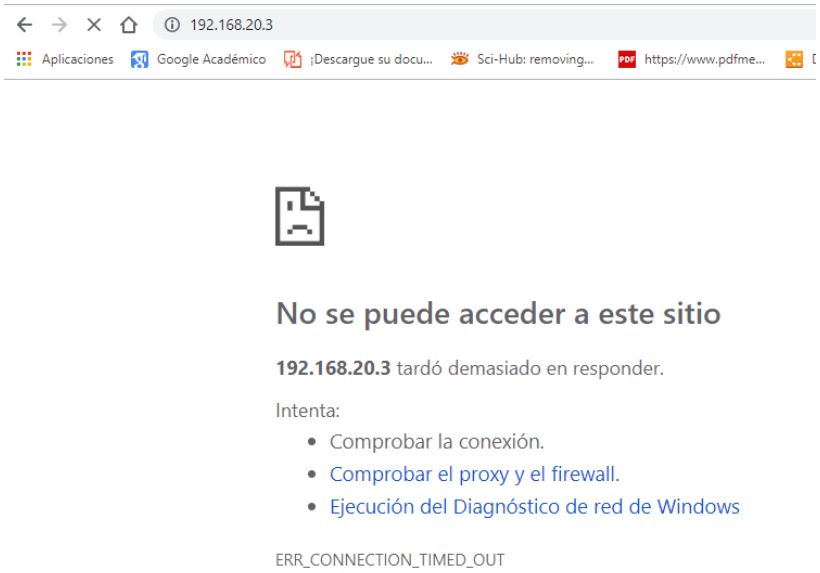


Figura 25: Después del ataque DoS. Fuente propia

4.6. Verificar detección de anomalías

Para realizar la verificación de anomalías se utiliza la interfaz de Nozomi, que contiene un panel de alarmas, que facilita la detección de ataques DoS, NMAP y detectar nuevas conexiones externas e identificar activos a través de su software llamado SCADA GUARDIAN.

4.6.1. Panel de alarmas.

La herramienta de Nozomi permite reconocer nuevas conexiones de dispositivos y muestra en tiempo real los riesgos y vulnerabilidades a los que se somete la red OT. En los círculos rojos encerrados en la Figura 26 se muestran los equipos y direcciones IP comprometidos en detecciones peligrosas para la red. Para la parte derecha se muestran todos los eventos y vulnerabilidades que ocurrieron en la red OT.

Los eventos que se observan de color rojo en la figura 26, no solo son nuevas conexiones o conexiones anormales fuera de la fase de aprendizaje, también nos muestra en alerta cada dispositivo en la red, el cual fue objeto de verificación por es parte de las firmas que tiene el software de NOZOMI, permitiendo alertar sobre posibles actualizaciones disponibles para sistemas operativos, aplicaciones y posibles vulnerabilidades que un atacante pueda explotar.

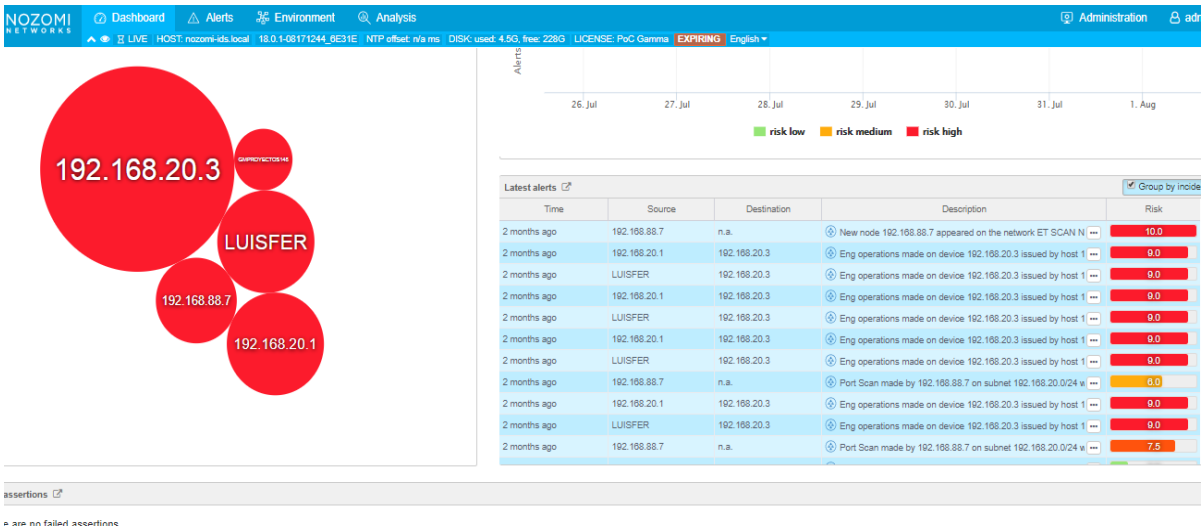


Figura 26: Entorno de alarmas y vulnerabilidades. Fuente propia

4.6.2. Detección de ataque DoS.

En la Figura 27 se observa la alerta de Nozomi ante un caso de ataque DoS, cuyo objetivo es atacar la dirección IP 192.168.20.3 recibiendo 301 intentos de conexiones en 30 segundos, recibir esa cantidad de conexiones en tan poco tiempo es algo anómalo y por tanto, la alarma del sistema de Nozomi lo muestra como una vulnerabilidad.

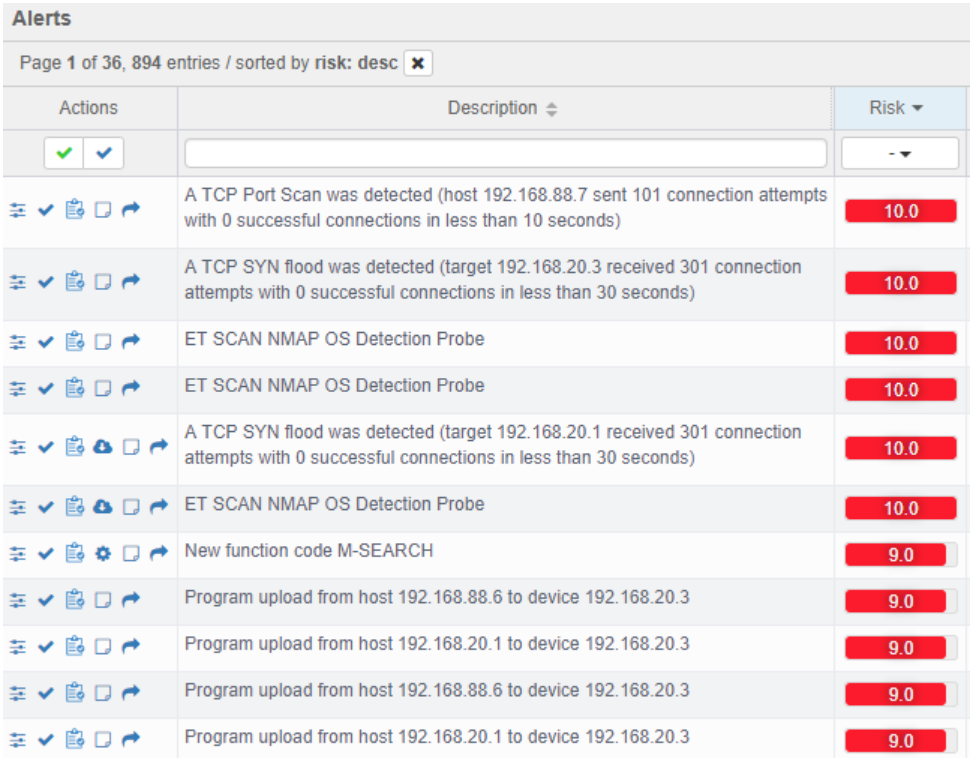


Figura 27: respuesta de Nozomi al ataque DoS. Fuente propia

4.6.3. Detección de ataque NMAP.

En la Figura 28 se observa los equipos conectados a la red OT, con sus vulnerabilidades y su grado de alerta, siendo rojo(mayor), naranja(medio), amarillo(bajo). Los equipos conectados son llamados: LUISFER con 332 alertas grado alto,121 grado medio y 1 grado bajo; LOGICOS331 con 168 alertas grado alto, 318 grado medio y 1 grado bajo; y un equipo no reconocido con la dirección IP 192.168.88.7 con 4 alertas grado alto, 20 medio y 2 grado bajo.

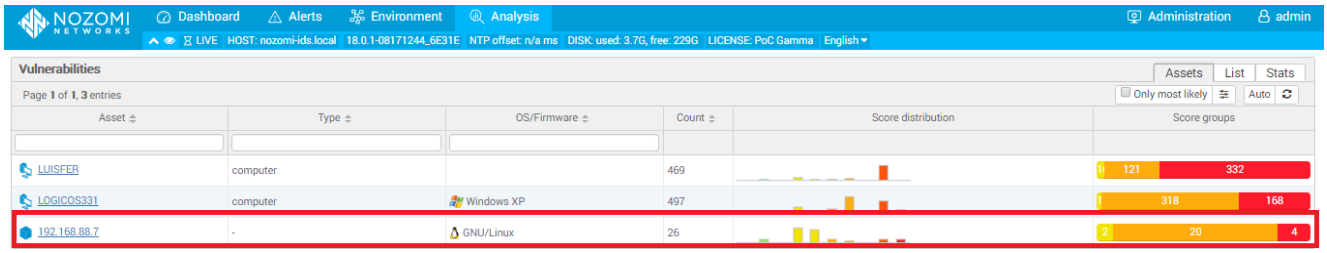


Figura 28 Reconocimiento de nueva conexión vulnerable. Fuente propia

En la Figura 29 se observa el panel de alertas generadas por el escaneo de la herramienta NMAP desde la dirección 192.168.88.7(Kali Linux) con un riesgo

máximo calificado como 10.0. Lo que indica que, la herramienta de Nozomi en efecto alera sobre posibles ataques Dos.

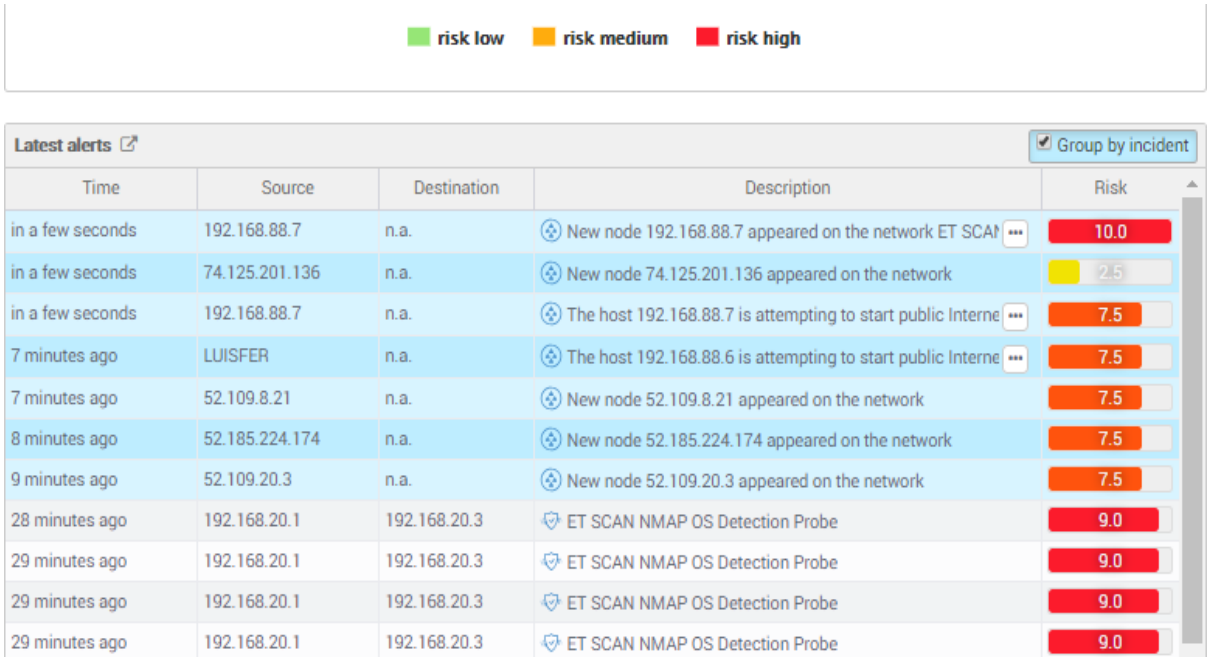


Figura 29: Panel de alertas NOZOMI P500. Fuente propia

En la Figura 30 se observa una alerta sobre la detección de puertos en la dirección 192.168.20.3, que para el caso es la dirección del PLC Allen Bradley 1100. En otras palabras, la herramienta de Nozomi indica que la dirección del PLC tiene puertos abiertos y esto es una vulnerabilidad de la red.

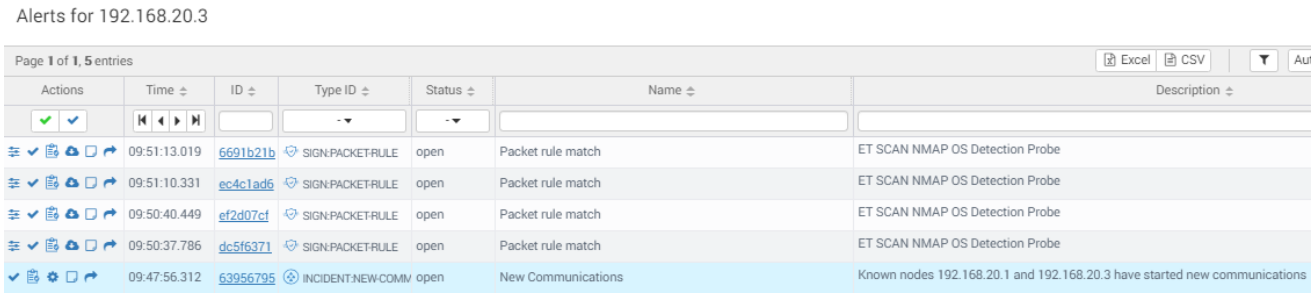


Figura 30: Alerta de detección de puertos. Fuente propia

4.7. Conexiones externas nuevas

Después de la fase de aprendizaje del NOZOMI P500, una nueva conexión se detectará inmediatamente como un intruso y enviará las respectivas alertas con la información de ese nuevo nodo, en la Figura 29 se observa el nuevo nodo llamado “MIRANDA” con una dirección IP 192.168.88.9.

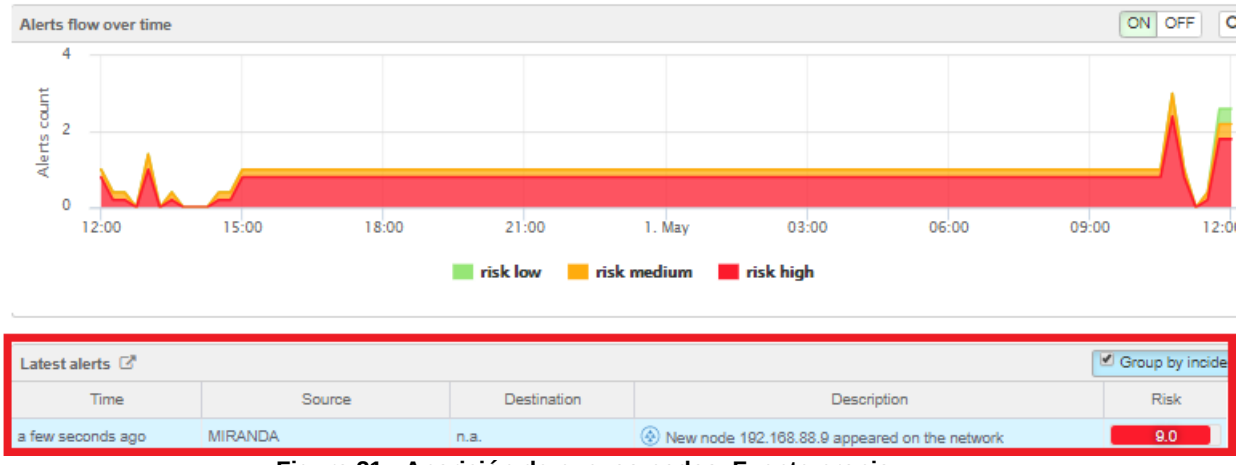


Figura 31 : Aparición de nuevos nodos. Fuente propia

4.7.1. Reporte de vulnerabilidades de SCADA GUARDIAN para cada equipo en la Red OT.

Se utilizó SCADA GUARDIAN con el fin de generar reportes de cada uno de los equipos comprometidos con vulnerabilidades en la red OT con su respectiva información del equipo como: dirección IP, dirección MAC, protocolos de comunicación, conexiones con otros dispositivos, software instalado, sistema operativo, además se genera un diagrama grafico en representación de las conexiones presentes del dispositivo en el momento en el cual se creó.

Los anexos de red de operación (anexos D y E) y control (anexos c) contienen información acerca de cada dispositivo que se encontró conectado a la red segmentada por medio de Vlans, permitiendo ver en detalle cada equipo con su información individual y sus respectivas vulnerabilidades encontradas por Nozomi Networks, a través de firmas alojadas en la nube que compara los datos adquiridos con sus datos alojados en la nube, para así poder determinar las posibles vulnerabilidades.

4.7.2. Red de control.

El anexo de la red de control (equipo identificado con la dirección 192.168.88.6 que contiene la HMI) contiene la información del HMI, como, por ejemplo: el sistema operativo en el cual está montado, la información de la red de operación y las conexiones con las transacciones de paquetes con los equipos que tiene comunicación. Además, se califica las vulnerabilidades en una escala de 1 a 10, siendo 10 la calificación máxima para una vulnerabilidad. Se muestran todas las debilidades que tiene este equipo en el momento que se generó el reporte. (Ver Anexo C).

4.7.3. Red de operación.

El anexo de la red de operación contiene la información del PLC y su ordenador encargado de programar su Ladder, como, por ejemplo, su versión de firmware, la información de la red de control y las conexiones con las transacciones de paquetes con los equipos que tiene comunicación. Además, indicar con una calificación máxima de 10 que sería la más alta de una vulnerabilidad para mostrar todas las debilidades que tiene es equipo en el momento que se generó el reporte (Ver Anexos D y E)

Capítulo V

5. Conclusiones y futuros trabajos

5.1. Conclusiones

Las herramientas y tecnologías para detección de vulnerabilidades en redes OT se encuentran en un desarrollo y fase de maduración, al igual que el concepto de protección en las empresas del sector industrial, se tiene muchos mitos y conceptos erróneos acerca de la ciberseguridad y se piensa que por no estar conectados a las redes IT no se pueden afectar los procesos y no tendrán ataques a su infraestructura.

Como vulnerabilidades de las redes OT e IT se pueden exponer errores humanos, entre los cuales se destacan los despistes, las negligencias, los fallos, tarde o temprano, van a suceder: una consigna mal introducida en un sistema, un mensaje de correo electrónico enviado al destinatario equivocado, un dato que se comparte con un tercero (cuando no debería haber sido así), un empleado que pierde su teléfono móvil, otro a quien “despistan” su ordenador portátil en una cafetería del aeropuerto, etc., son sólo algunos ejemplos de la citada fragilidad.

Las herramientas de Nozomi networks proporcionan una fase de protección inicial para ayudar a encontrar las vulnerabilidades de una red OT, realizando una organización de los niveles en el modelo de Purdue que ayuda al sector industrial no solo para ordenar su infraestructura, sino además de cumplir con normativas y requisitos de modelado.

En muchas ocasiones por la complejidad de las redes y el gran número de dispositivos o nodos, no se tiene un inventario de los activos en tiempo real, ya que en la mayoría de las empresas del sector industrial realizan todo este proceso de una forma manual. Este inventario puede ser obtenido con Nozomi de manera automática, además puede generarse y exportarse en formatos PDF y Excel, lo que representa una ventaja para los usuarios ya que esta tarea es tediosa al ser realizada manualmente.

En casos más específicos especialmente en las industrias eléctricas, la seguridad y el seguimiento de la infraestructura OT tiene un gran valor, ya que este sector industrial en Colombia debe cumplir con las normas del consejo nacional de operación (CNO).
En el acuerdo 788 del 3 de septiembre de 2015(sector público y privado), el numeral 4 propone como objetivo al sector eléctrico el levantamiento de información que

permita identificar los activos críticos, los riesgos y vulnerabilidades, el nivel de gestión de ciberseguridad en la operación, ítems a los que se le da solución con las herramientas de NOZOMI NETWORKS.

El ataque de denegación de servicio dirigido al PLC fue una buena prueba a la vulnerabilidad del PLC Allen Bradley, que para efectos de funcionamiento del proceso no lo altero como tal, pero sí tuvo otro efecto en su servidor web, el cual se dejó sin funcionamiento al recibir tantas peticiones, algo que pudo repercutir en grandes daños o consecuencias si hubiera supervisado variables del proceso desde el servidor web.

La herramienta de SCADA GUARDIAN realizó su labor al detectar casi que de inmediato esta alteración de peticiones sobre un mismo recurso al tiempo, dando un mejor panorama a un administrador de red, para que tome las medidas necesarias y evitar este tipo de irrupciones a la seguridad.

Las fases de aprendizaje y protección de NOZOMI fueron acertadas en cuanto a los dispositivos conectados a la red OT, logrando un mapeo de todos los dispositivos conectados y protegiendo la red ante los ataques realizados, cabe aclarar que, NOZOMI es una herramienta para detección de vulnerabilidades de forma pasiva muy eficiente, pero que no funciona como mecanismo de defensa para mitigar dichas vulnerabilidades, por este motivo es un complemento de las herramientas de Fortinet.

La segmentación de la red es algo primordial, ya que al realizar este proceso con las Vlans podemos adicionar políticas de funcionamiento de acuerdo a lo que plantea cualquier tipo de red con sus dispositivos, para el caso del prototipo de red OT, se originaron con el fin de realizar la configuración de puerto espejo en el Switch y capturar el tráfico que viajaba desde la red de operación y la red de control, así el software de SCADA GUARDIAN captura todo el tráfico TCP/IP para des encapsular y realizar alertas de tráfico inusual.

5.2. Trabajos futuros

Se presentan algunas alternativas de trabajos futuros que pueden desarrollarse a partir de esta práctica empresarial, que por motivos de alcance no se desarrollaron o no fueron tratados con suficiente profundidad. Además, se sugieren algunos desarrollos específicos para apoyar o complementar la metodología implementada en el prototipo de red OT. Se destacan los siguientes trabajos futuros descritos a continuación:

- Realizar una detección de vulnerabilidades con otras herramientas diseñadas para redes OT, para complementar la información y poder comparar diversos productos que permitan desarrollar y encontrar nuevas capturas de datos con el fin de poder decidir entre varias opciones, para saber cuál es la solución más adecuada según los requerimientos del cliente. Un posible fabricante para tal fin es Tenable industrial Security, con el software NESSUS, desarrollado para identificar e investigar vulnerabilidades de forma precisa para infraestructura crítica en tecnologías operativas.
- Implementar configuraciones en dispositivos especializados para mitigar vulnerabilidades de manera automática en la red OT, con el fin de explotar las vulnerabilidades de encontradas por NOZOMI NETWORKS y realizar una integración y tener una red integrada y segura. Algunos de los proveedores recomendados para utilizar como equipos de solución de vulnerabilidades son Fortinet, Palo Alto Networks, Forcepoint, Checkpoint, todos los anteriores fabricantes de firewall de nueva generación, propicio para este tipo de integración de redes.
- Implementar el prototipo de red OT, realizando cambios en la arquitectura para tener comunicación con protocolos propietarios y así investigar sobre nuevos ataques a las redes, para comprobar que la infiltración a las redes industriales no necesariamente debe ser con una integración de las redes OT y las redes IT.

Anexos

Anexo A

Configuraciones de suite de Rockwell PLC y SCADA

Este anexo muestra las configuraciones necesarias para descargar el código Ladder a través de una conexión ethernet al PLC en el numeral 1, se da un paso a paso necesario para configurar una dirección IP mediante el software BOOTP/DHCP Server, luego se configura el driver ethernet en el software RSLinx Classic y así poder descargar el programa al PLC.
Para el numeral 2 se realiza un paso a paso para asociar el HMI con el código LADDER mediante una conexión OPC, así se podrá realizar el login en el HMI y poder controlar la planta de nivel y visualizar el estado de la instrumentación.

6. Configuración de LADDER

6.1. Configuración de dirección IP del PLC mediante BOOTP/DHCP Server

- Abrir el programa BOOTP/DHCP Server (ver Figura 32)

Figura 32: Inicio software BOOTP/DHCP Server. Fuente propia

- Crear una nueva entrada e ingresar la dirección MAC del PLC con su dirección IP, luego seleccionar OK, como se observa en la figura 33.

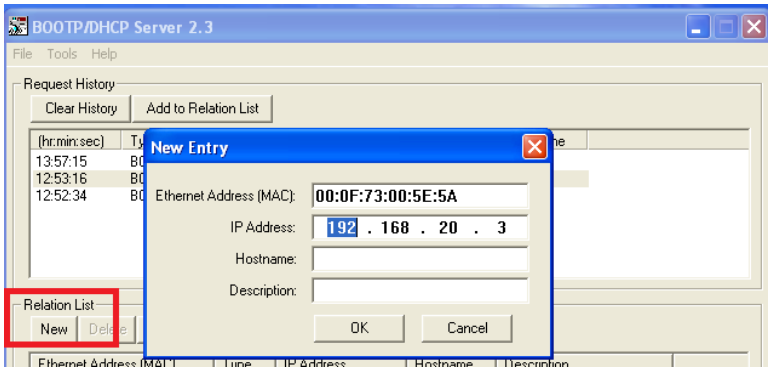


Figura 33: Seleccionar MAC y Dirección IP. Fuente propia

- Seleccionar la nueva entrada y luego clic en Disable BOOTP/DHCP

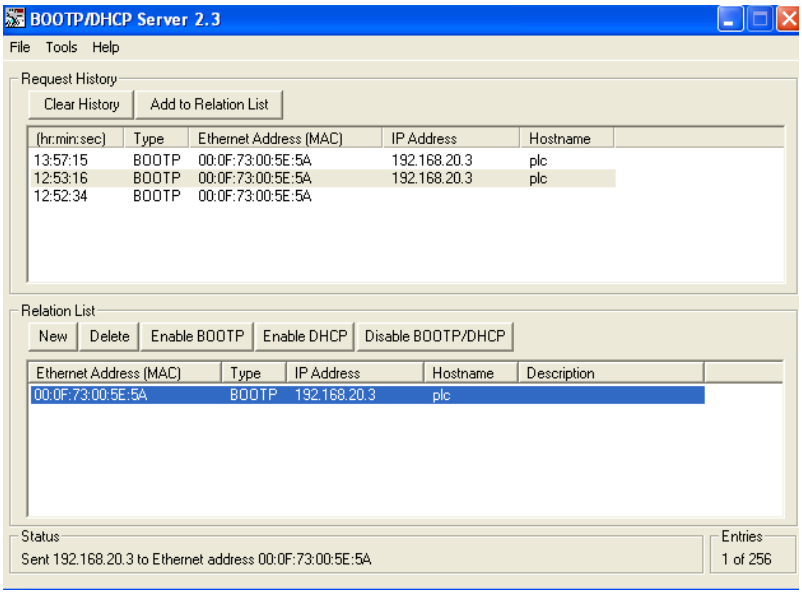


Figura 34: Asignar dirección IP a PLC. Fuente propia

- Al finalizar, el PLC tendrá una dirección IP como se presenta en la figura 35.

Figura 35: PLC configurado con dirección IP. Fuente propia

6.2. Configuración del Driver en RSLinx Classic

- Inicio de software RSLinx Classic

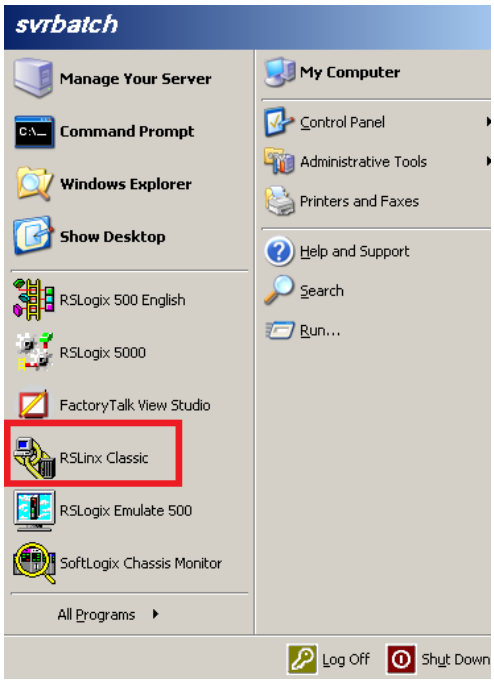


Figura 36: Inicio de Software RSLinx Classic. Fuente propia

- Seleccionar un nuevo Driver como se muestra en la figura 37.

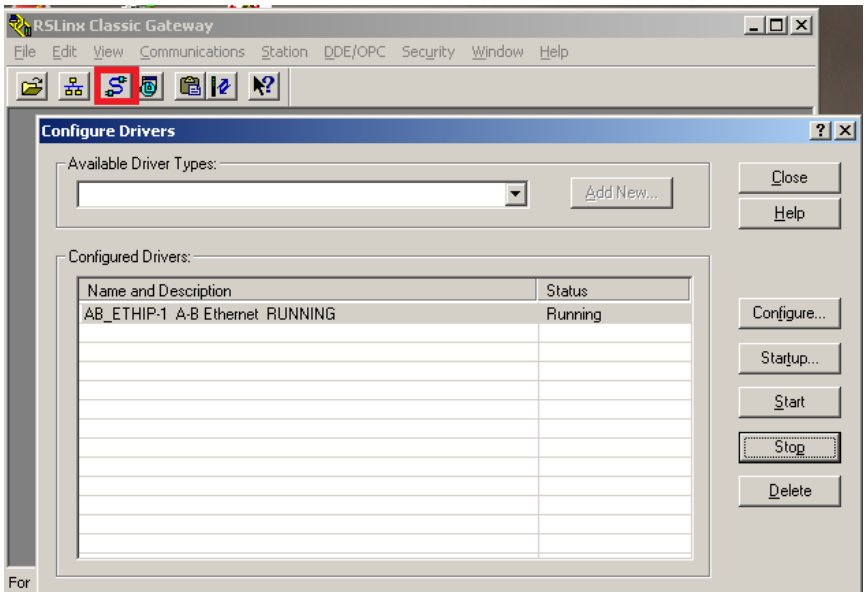


Figura 37: Configurar nuevo Driver. Fuente propia

- Agregar un nuevo Driver Ethernet

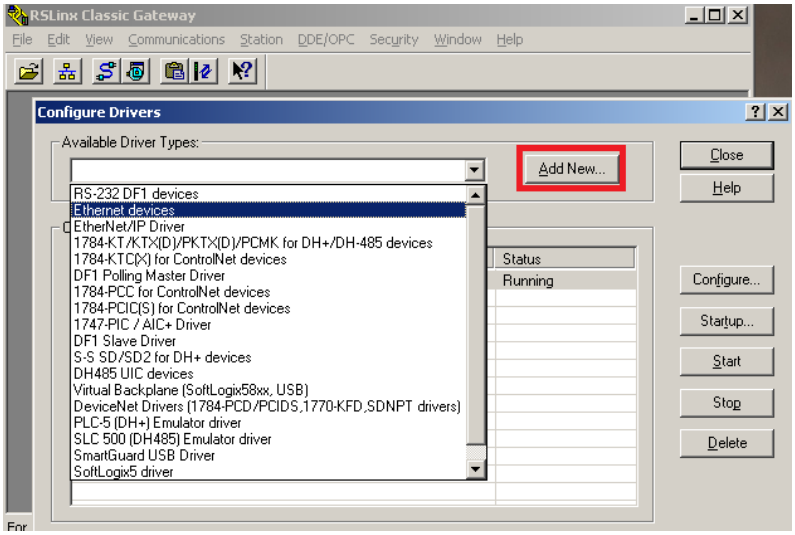


Figura 38:Selección de Driver. Fuente propia

- Seleccionar el Driver (Ethernet devices) y dar clic en OK

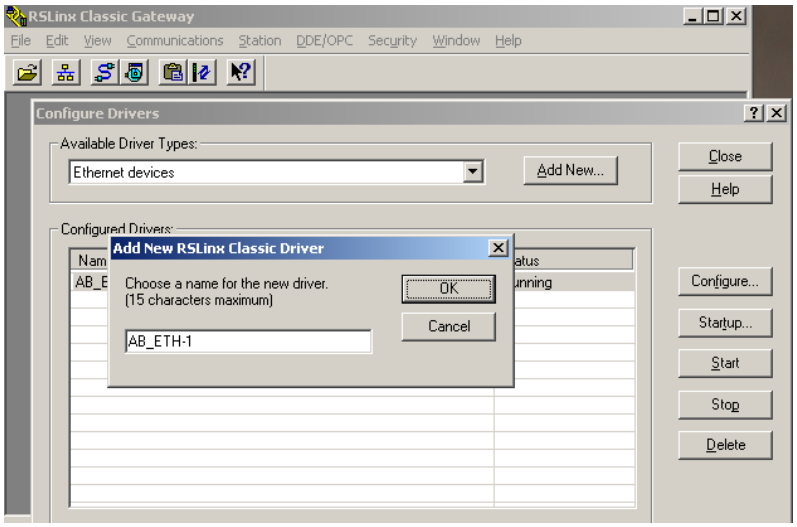


Figura 39: Nombre para el Driver. Fuente propia

- Para finalizar, se ingresa la dirección IP del PLC creada anteriormente y se selecciona OK, para luego cerrar el programa RSLinx Classic.

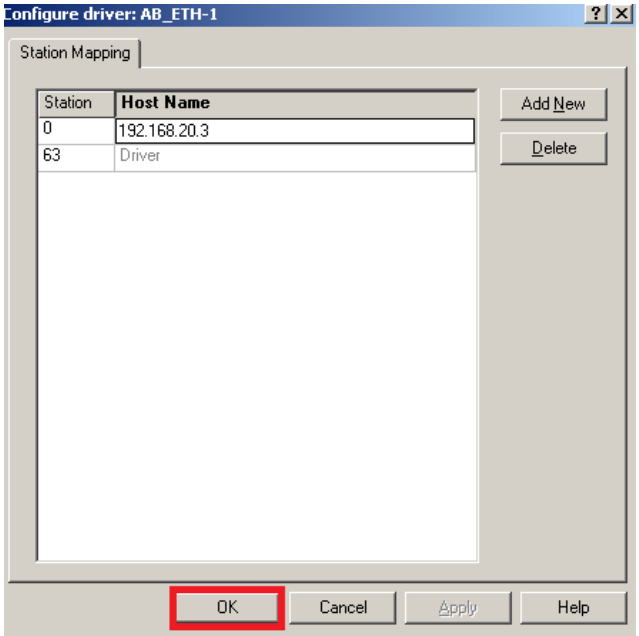


Figura 40:Configuración IP para el Driver. Fuente propia

6.3. Programación del PLC

El programa del controlador se realiza en lenguaje ladder usando la herramienta Rslogix 500 de rockwell software. Los pasos a seguir son los siguientes:

- Iniciar el software RSLogix 500

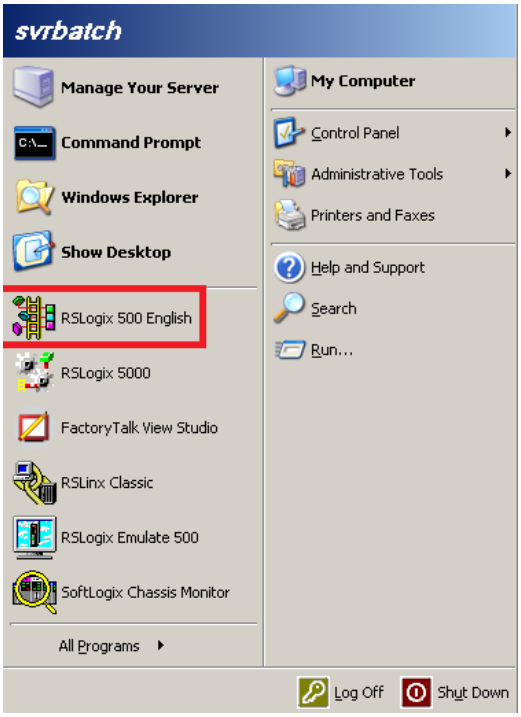


Figura 41: Inicio software RSLogix 500. Fuente propia

- Abrir el archivo anexo PLANTANIVEL.RSS

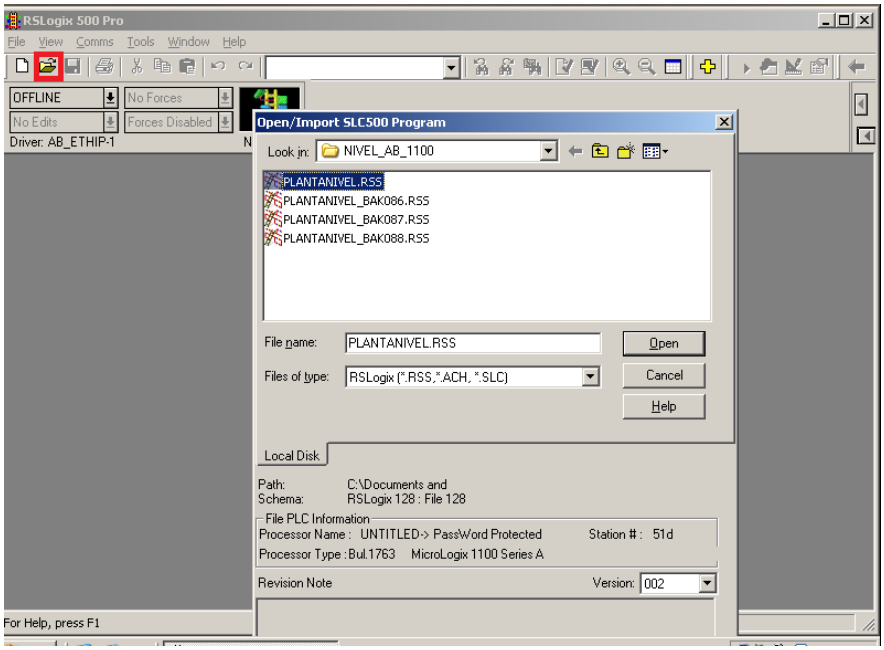


Figura 42: Abrir código LADDER. Fuente propia

- Ingresar código de acceso (9087)

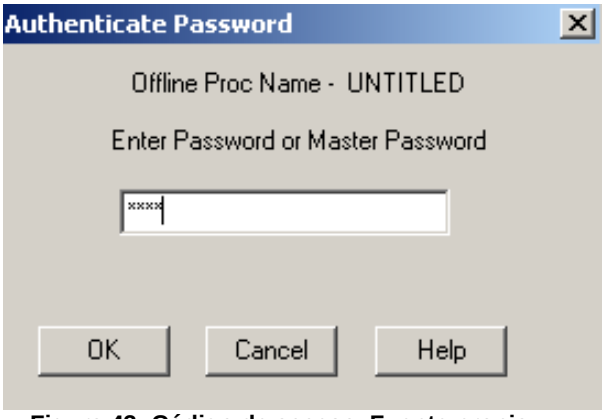


Figura 43: Código de acceso. Fuente propia

- Descargar el código LADDER al PLC, seleccionar la opción Comms, System Comms

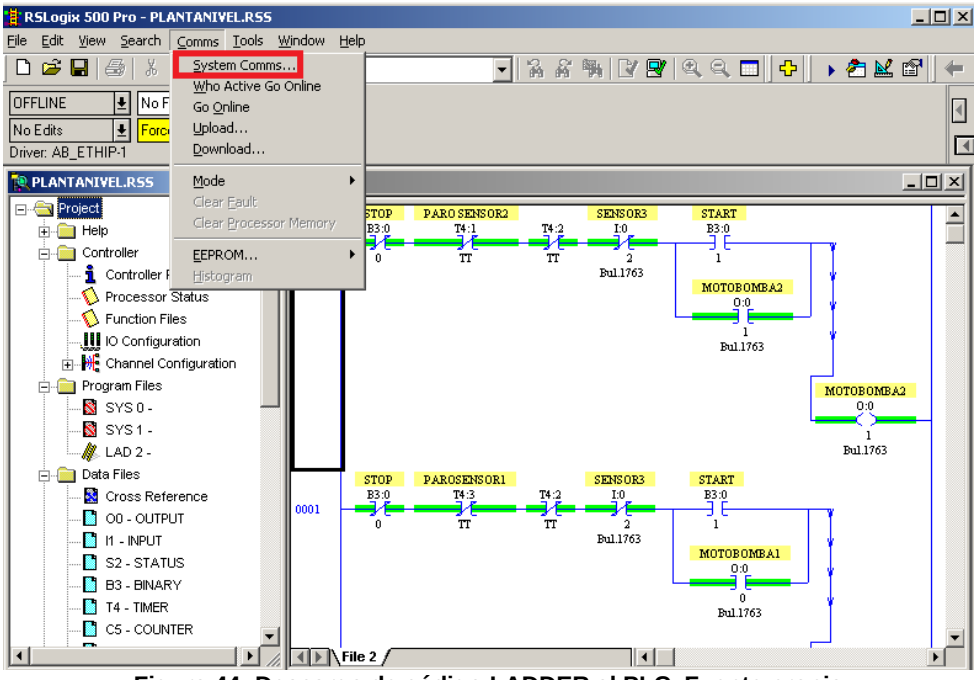


Figura 44: Descarga de código LADDER al PLC. Fuente propia

- Seleccionar el nodo creado con la dirección IP del PLC y luego descargar.

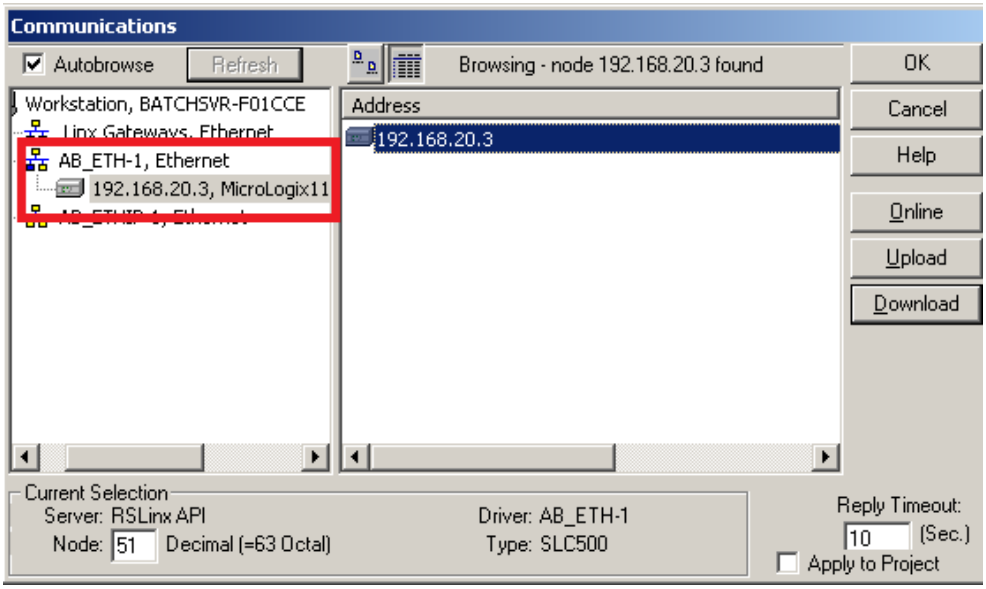


Figura 45: Descarga de código LADDER al PLC. Fuente propia

- Finalizando el proceso, el código estará en modo remoto en el PLC.

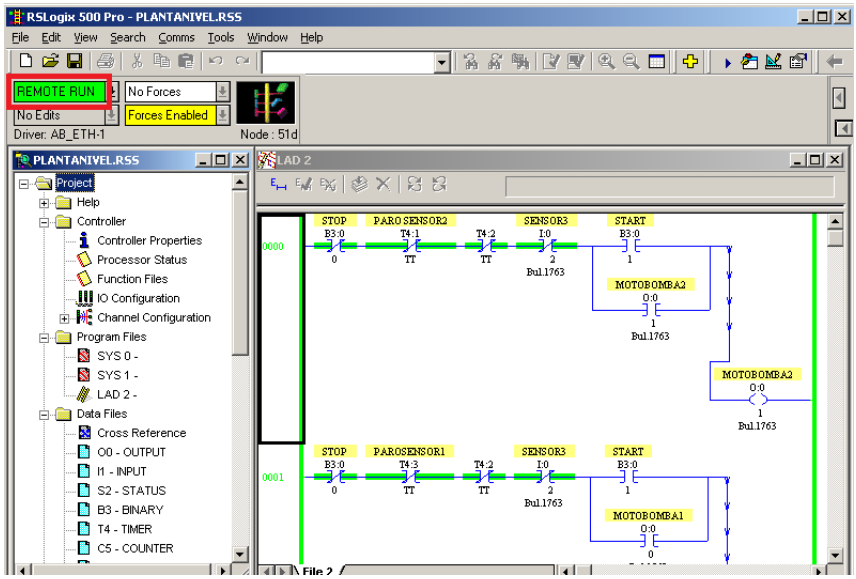


Figura 46: Código LADDER descargado a PLC. Fuente propia

7. Configuración y puesta en marcha de HMI

Para la integración del código LADDER y la interfaz hombre-máquina se realiza una conexión OPC Data Server a través del software RSLinx.

- Inicio software Factory Talk View ME

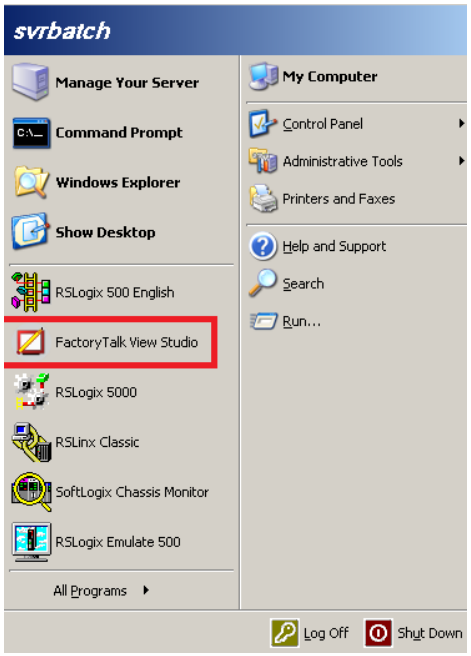


Figura 47: Inicio: Software Factory Talk View. Fuente propia

- Selección del entorno Machine Edition

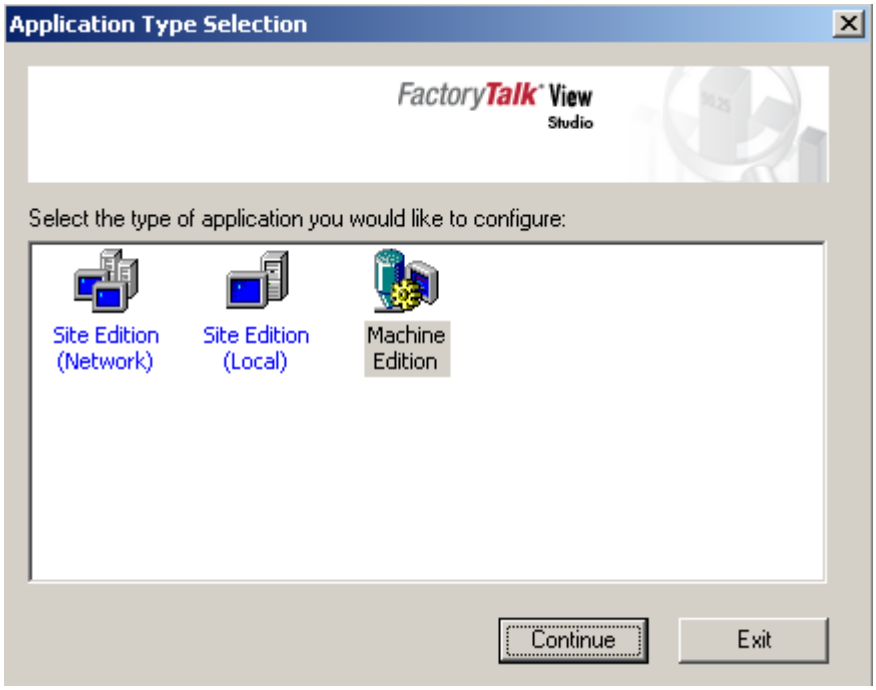


Figura 48:Entorno Machine Edition. Fuente propia

- Seleccionar el proyecto “Demo_Niv”, archivo adjunto como anexo.

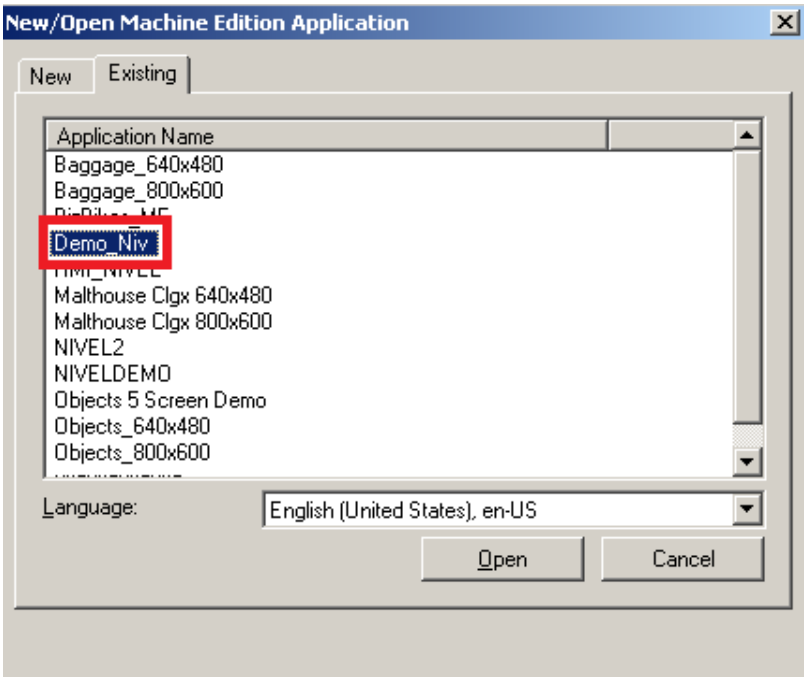


Figura 49:Proyecto Machine Edition. Fuente propia

- Crear nuevo servidor OPC Data Server, para la integración con LADDER de RSLogix 500

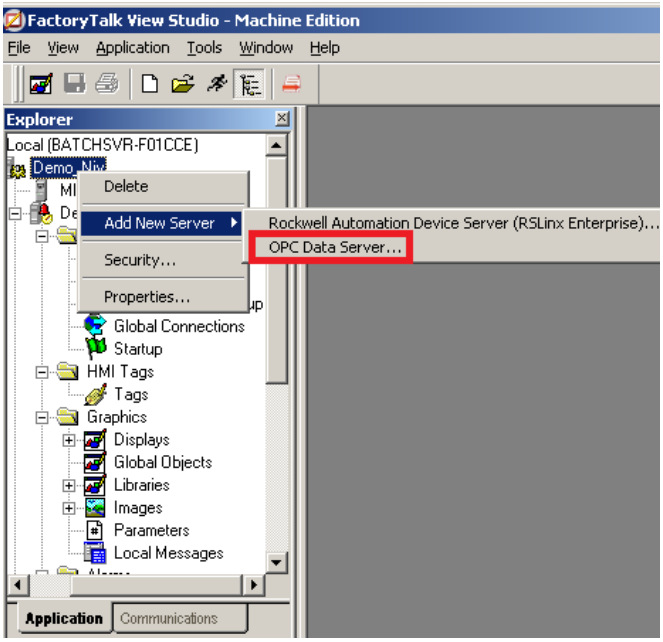


Figura 50: Crear servidor OPC Data Server. Fuente propia

- Seleccionar el nombre y el tipo de servidor

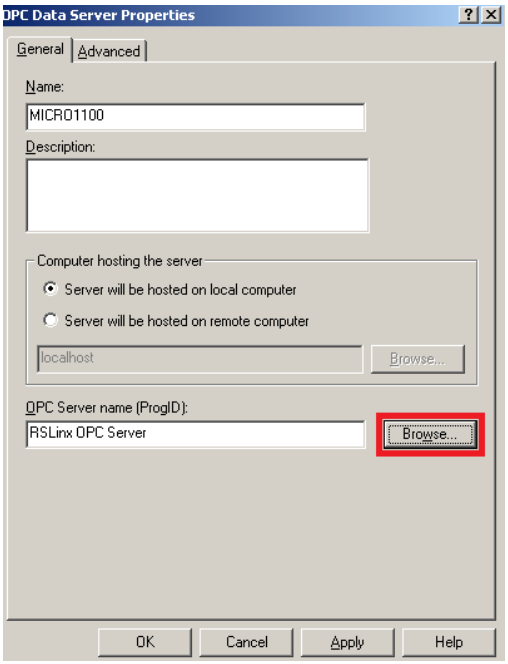


Figura 51:Nombre y tipo de servidor OPC. Fuente propia

- Nuevo servidor OPC creado

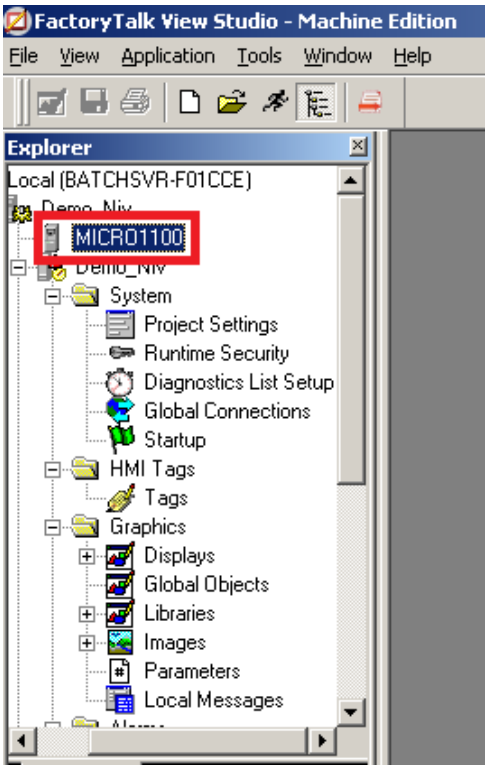


Figura 52:Nuevo servidor OPC creado. Fuente propia

- En el software RSLinx Classic se realiza la asociación del servidor OPC y el código LADDER.

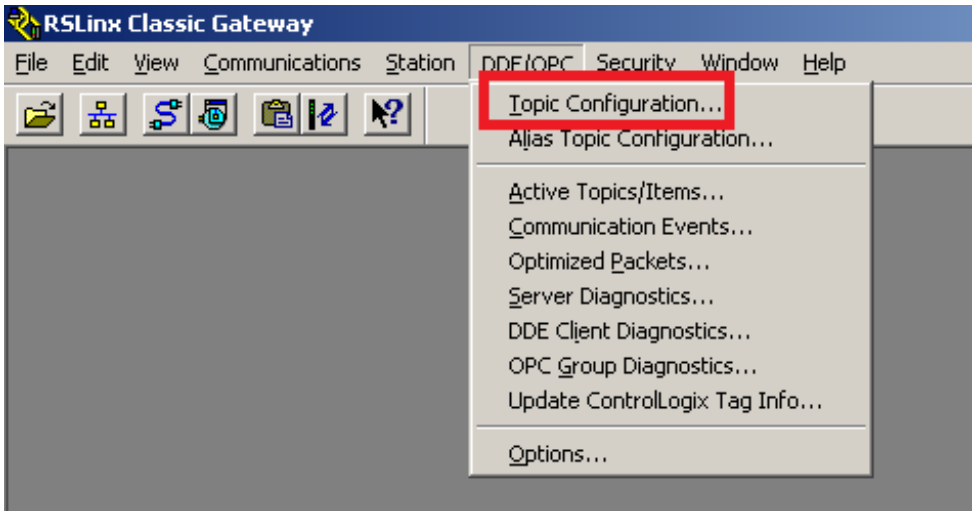


Figura 53: Configuración OPC. Fuente propia

- Se asocia el servidor OPC creado al PLC, con el código LADDER previamente cargado.

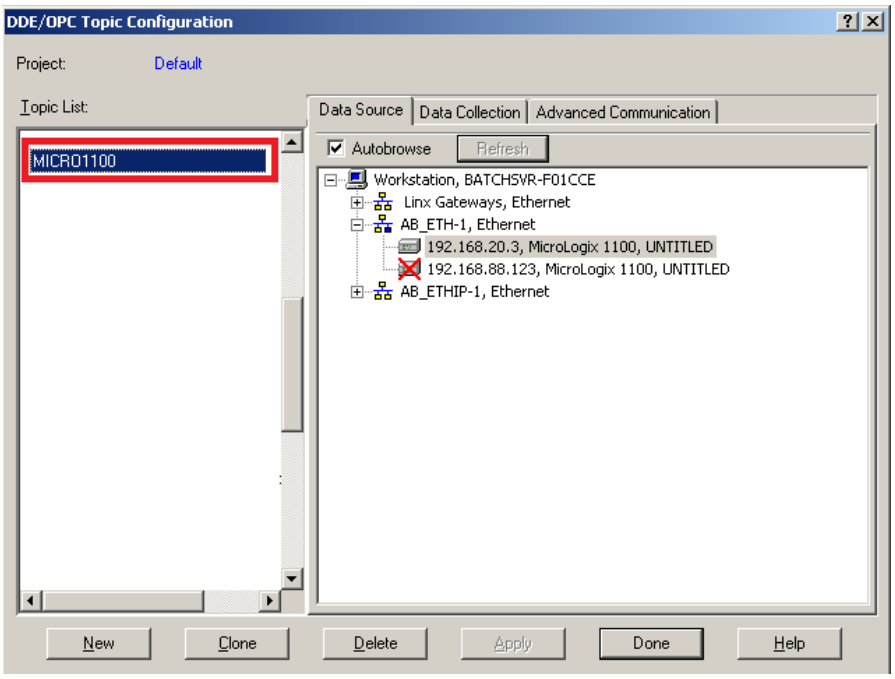


Figura 54: Asociar servidor OPC al código LADDER. Fuente propia

- Ejecutar HMI. A través del ícono de la barra de herramientas mostrado en la figura 55

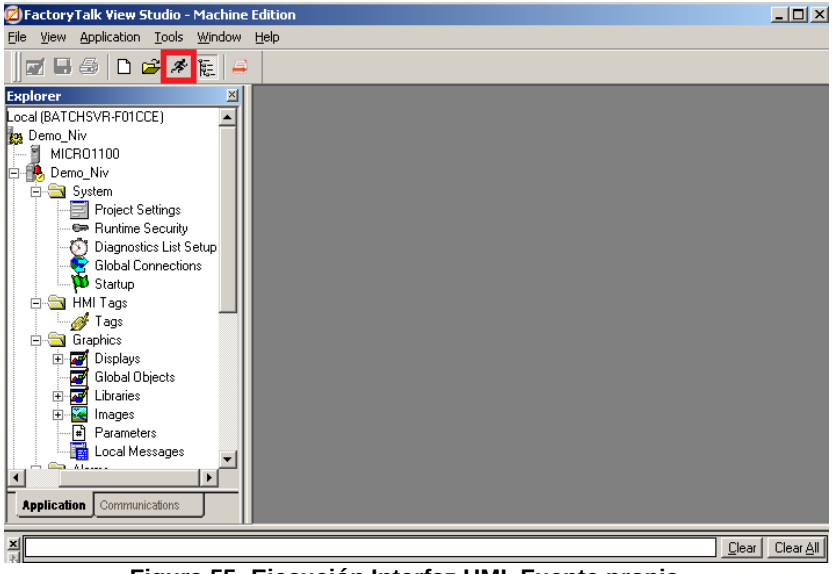


Figura 55: Ejecución Interfaz HMI. Fuente propia

- Autenticar usuario en la interfaz: Login: CON, Password:123

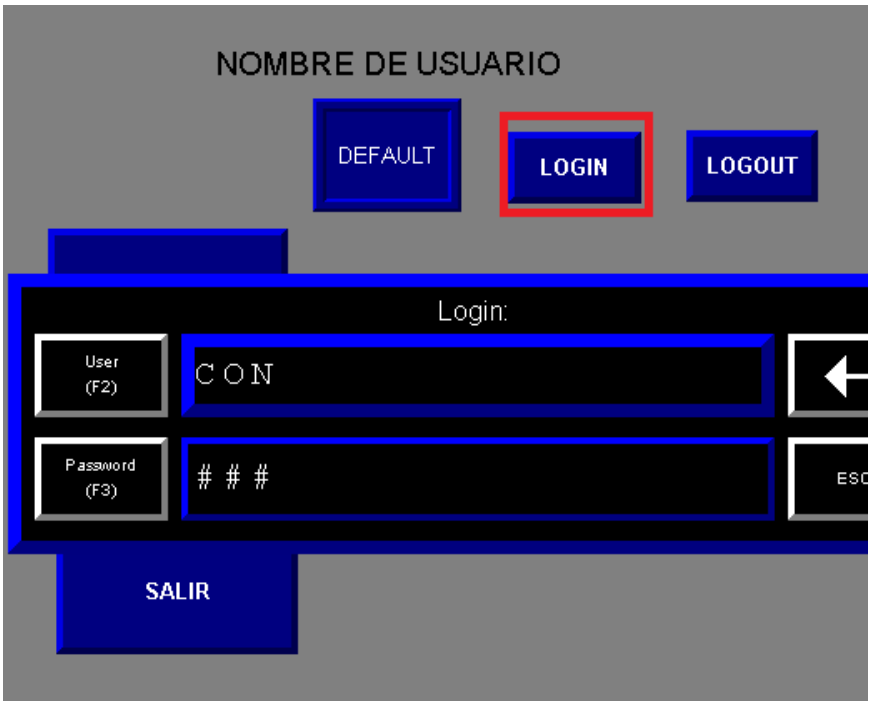


Figura 56: Autenticación de usuario en la interfaz. Fuente propia

- Usuario autenticado

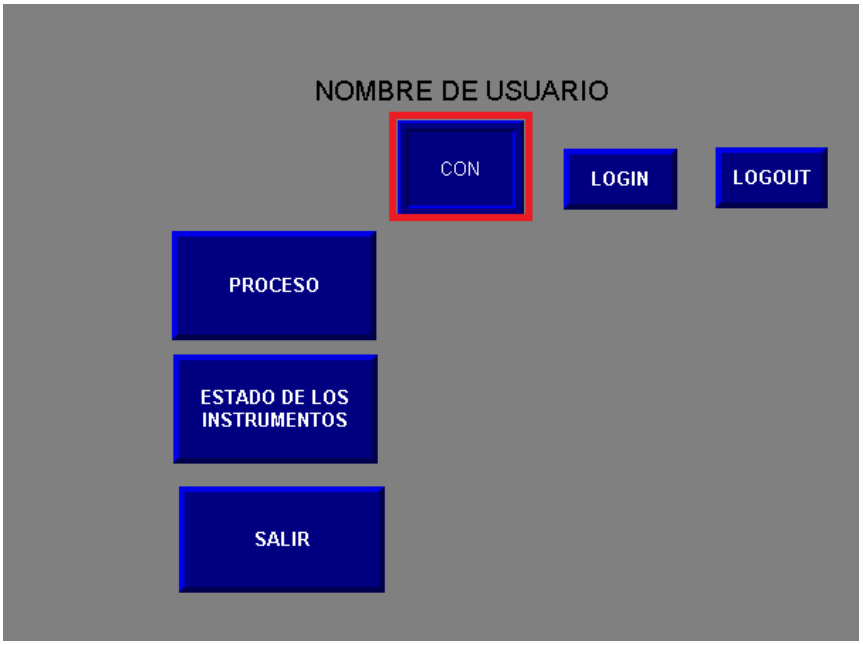


Figura 57 Usuario autenticado. Fuente propia

- Inicio y parada del Proceso

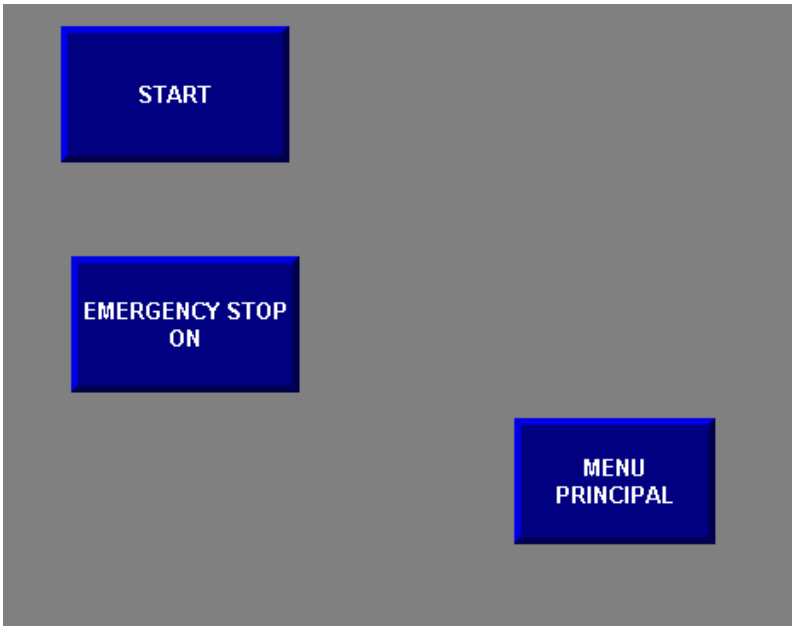


Figura 58: Inicio y parada del Proceso. Fuente propia

- Estado de los instrumentos del proceso

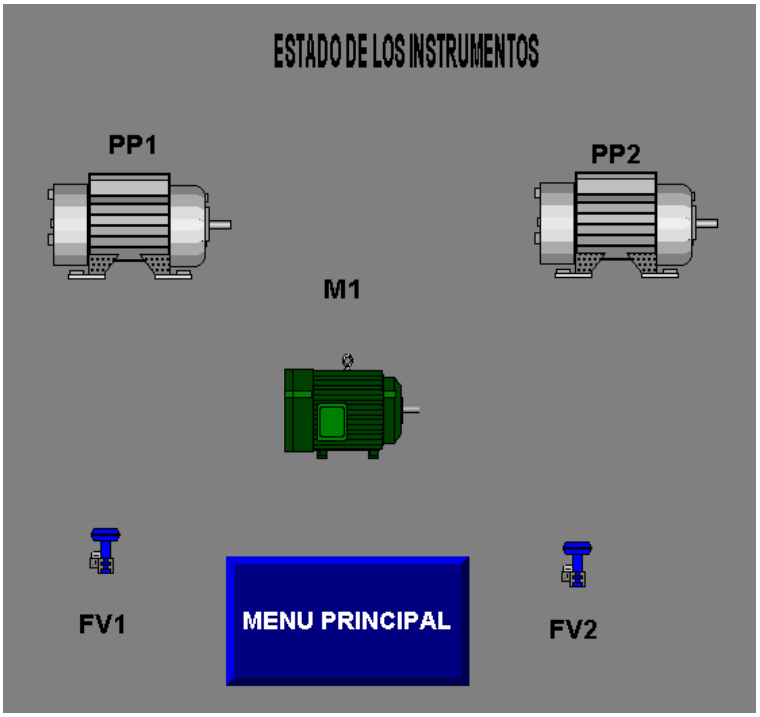


Figura 59: Estado de los instrumentos. Fuente propia

Anexo B

Este anexo muestra la conexión y configuración realizada para el prototipo de red OT realizando las conexiones paso a paso del FortiGate y el Switch. además de realizar las pruebas de comunicación de los equipos de Fortinet con la gestión de remota del equipo utilizado para la detección de vulnerabilidades en la red OT Conexión y configuración de prototipo de red OT.
La figura 60 indica la conexión física que se debe realizar y las direcciones con las que se va a trabajar para realizar una segmentación a través de Vlans

8. Conexión y configuración de prototipo de red OT

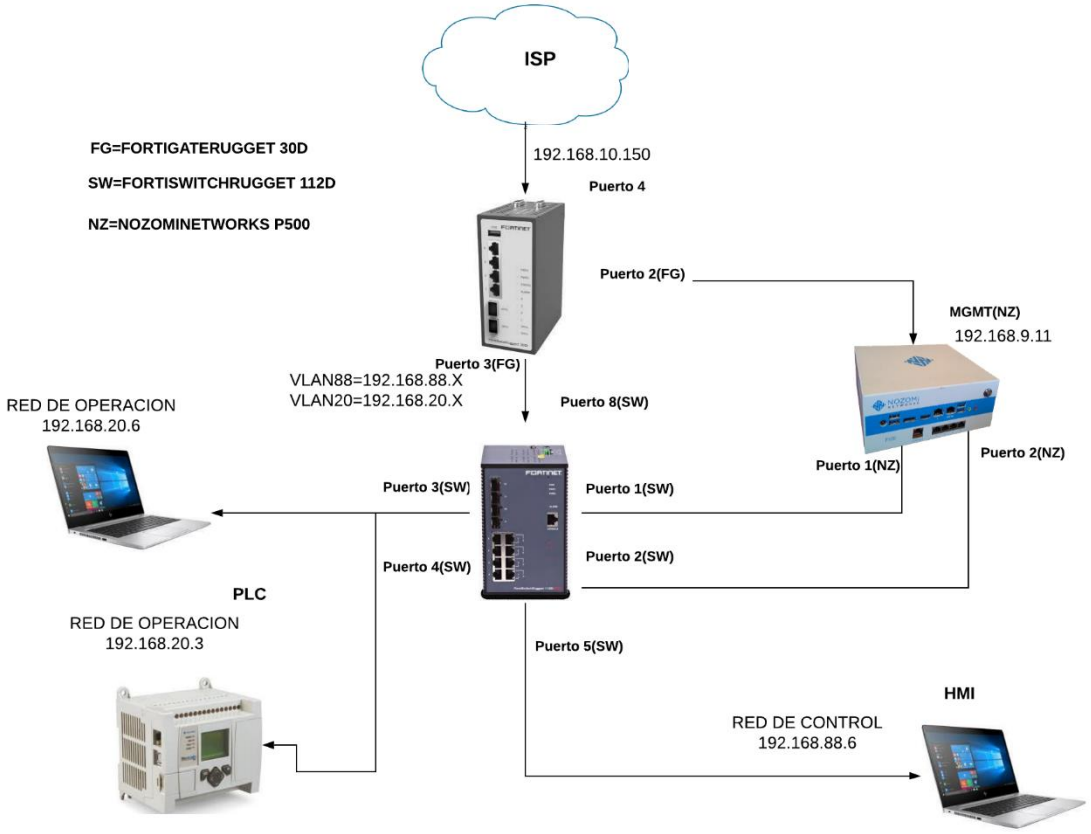


Figura 60: Configuración Firewall. Fuente propia

8.1. Configuración firewall FORTIGATERUGGED 30D

Para realizar la configuración de firewall se deben realizar los siguientes pasos:

- Ingresar a la interfaz: conectar el cable ethernet al puerto 1 del FORTIGATE y se tendrá una dirección IP, una Gateway por defecto como se muestra en la figura 61.

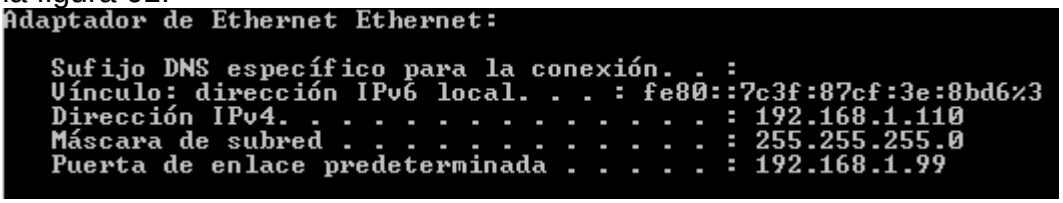


Figura 61: configuración de red. Fuente propia

- Acceder al navegador e ingresar a la interfaz por medio de la dirección https://192.168.1.99/login, con el usuario **admin** y sin contraseña (ver figura 62)

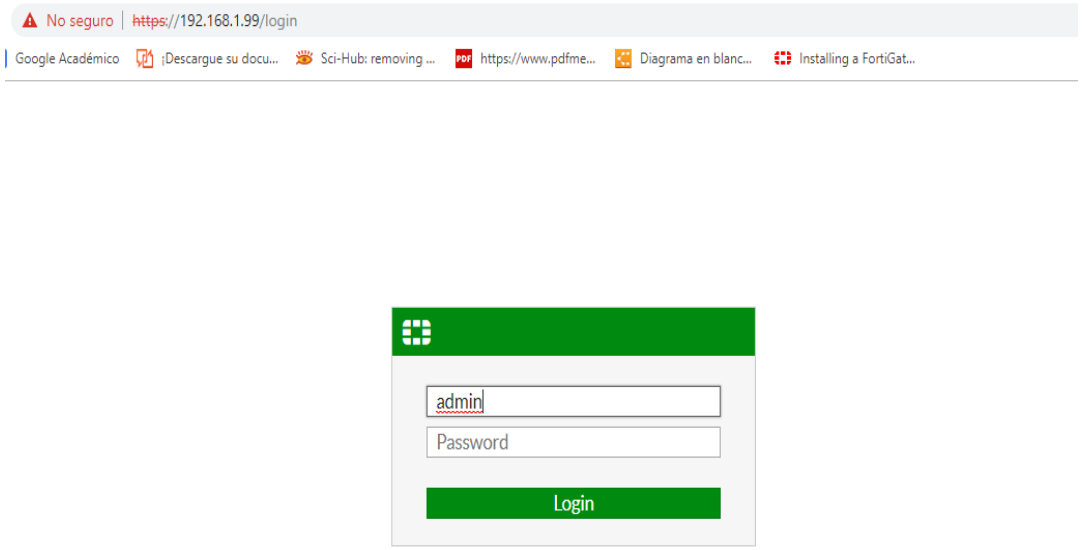


Figura 62: Login. Fuente propia

- En este paso, se configura el puerto 4 del Fortigate para ingresar el servicio de internet. Se debe seleccionar Network/Interfaces/lan4 y luego ingresar la dirección del ISP (proveedor de servicios de internet) como se muestra en la figura 63.

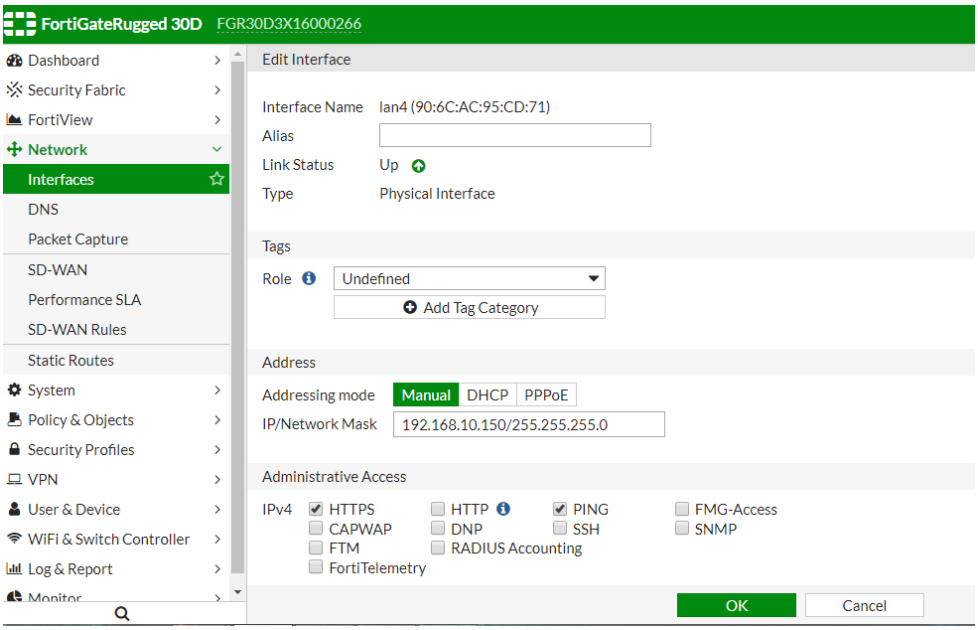


Figura 63: configuración LAN 4. Fuente propia

- Ahora, se debe seleccionar Network/Interfaces/Create New/Zone para crear una zona y agregar la interfaz LAN 4 como se muestra en la figura 64.

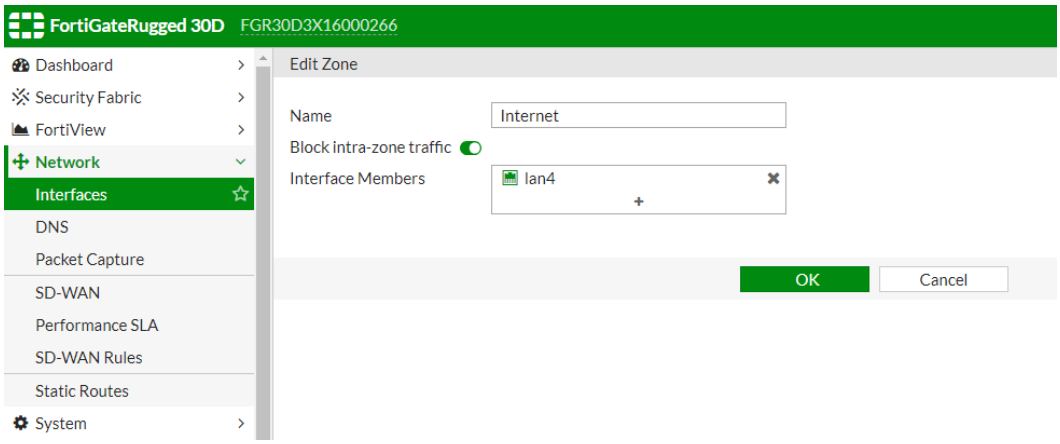


Figura 64: Crear zona. Fuente propia

- Dar clic OK y conectar físicamente el Fortigate, como se muestra en la figura 65.

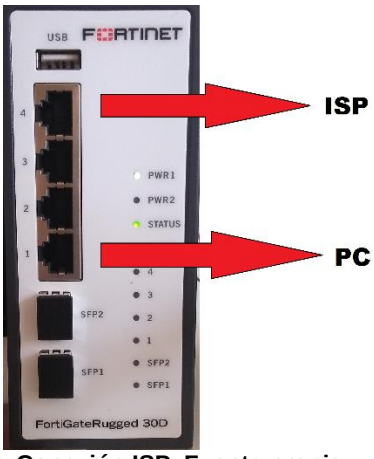


Figura 65: Conexión ISP. Fuente propia

Nota: Durante este paso aún no se cuenta con servicio de internet, ya que hasta el momento no se ha configurado una política de navegación en el Fortigate.

8.2. Configuración de VLAN

En los siguientes pasos se configura una VLAN (red de área local virtual) en el puerto físico LAN3 del Fortigate.

- Seleccionar Network/Interfaces/Create New/Interface/ y crear una interfaz para un segmento de la VLAN, como se muestra en la figura 66.

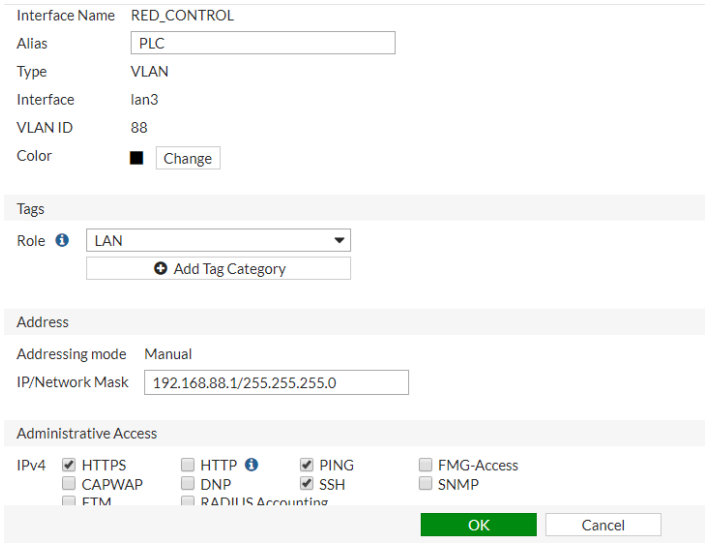


Figura 66: Segmento de VLAN 88 (Red de Control). Fuente propia

- Seleccionar OK y proceder a crear el otro segmento de VLAN.

- Seleccionar Network/Interfaces/Create New/Interface/ y crear una interfaz para un segmento de la VLAN como se muestra en la figura 67.

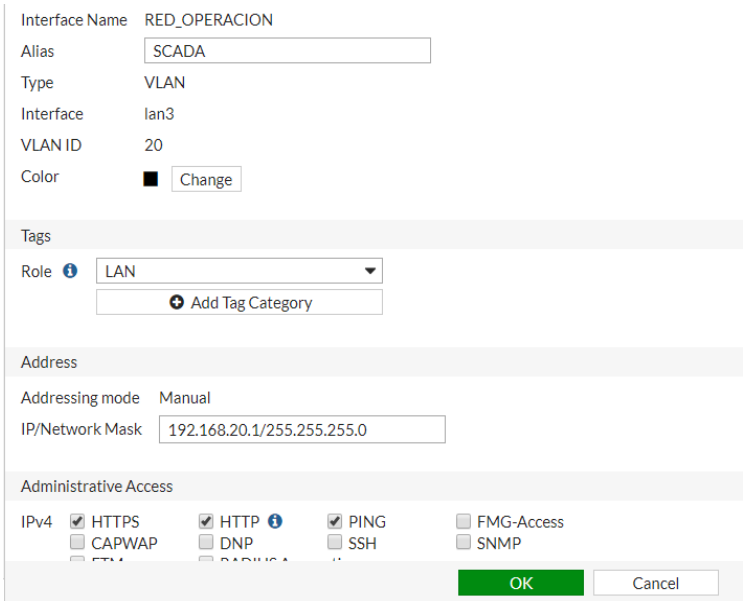


Figura 67: Segmento de VLAN 20 (Red de Operación). Fuente propia

8.3. Configuración de FortiSwitch

En la siguiente configuración se integra el Fortigate con el FortiSwitch, para ello se debe conectar físicamente el puerto 3 del Fortigate con el puerto 8 del Fortiswitch como se muestra en la figura 68.

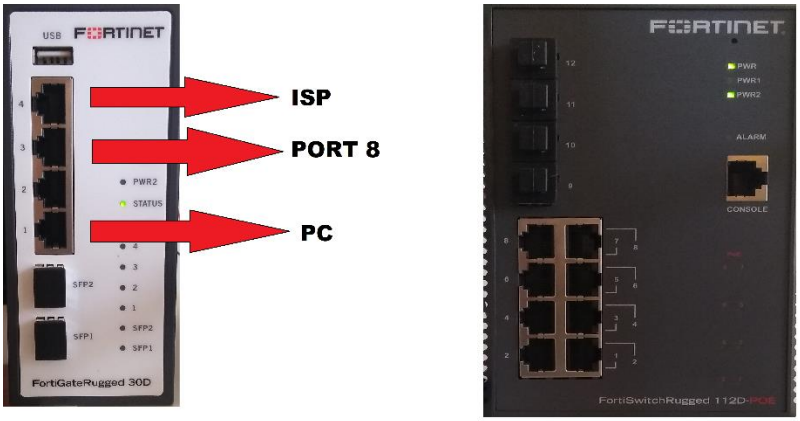


Figura 68: integración del FortiSwitch. Fuente propia

Configuración para administrar de forma remota el FORTISWITCHRUGGED 112D-POE desde el FORTIGATERUGGED 30D

Antes de conectar las unidades FortiSwitch y FortiGate, asegúrese de que la función de controlador de interruptor esté habilitada. La unidad FortiGate con la GUI o CLI de FortiGate para habilitar el controlador del interruptor. Se deben seguir los siguientes pasos para poder habilitar el control o gestión remota del FortiSwitch desde el Fortigate, así no debemos depender de una conexión directa física en el FortiSwitch.

A. Ir a System> Feature visibility.
B. Activar la función Switch Controller, que se encuentra en la lista de funciones básicas.
C. Seleccionar Aplicar. (ver figura 69)

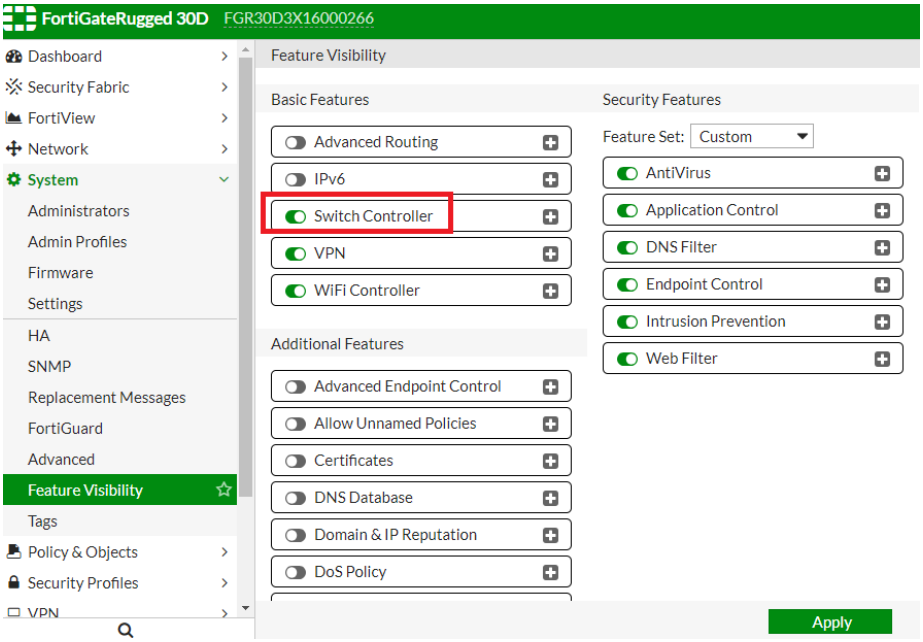


Figura 69: control remoto del Switch. Fuente propia

La opción de menú WiFi & Switch Controller aparecerá ahora.

- Usar el CLI de FortiGate

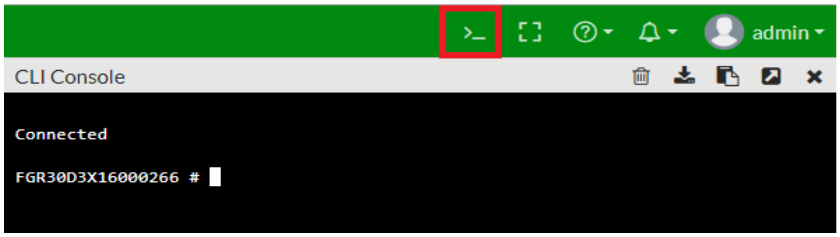


Figura 70: ingreso a consola del Fortigate. Fuente propia

- Use los siguientes comandos para habilitar el controlador del interruptor (ver figura 71)

```
FGR30D3X16000266 # config  system global

FGR30D3X16000266 (global) # set switch-controller enable

FGR30D3X16000266 (global) # end
```

Figura 71: Habilitar control de Switch desde consola. Fuente propia

-config system global
-set switch-controller enable
-end

- Al finalizar este ítem se tendrá control sobre el Fortiswitch desde el Fortigate, y damos clic en autorizar como se muestra en la figura 72.

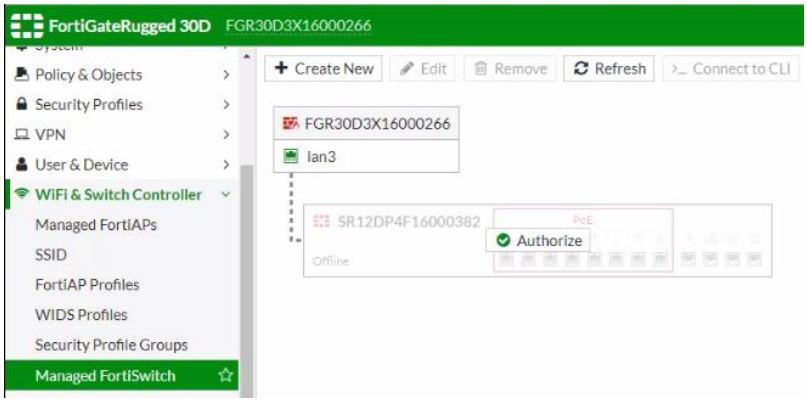


Figura 72: Control del FortiSwitch. Fuente propia

9. Pruebas de comunicación en red OT

Para realizar las pruebas de comunicación se realiza la conexión de todos los equipos al firewall del fabricante Fortinet, así toda la gestión se realizará desde este solo equipo.

9.1. Gestión de NOZOMI P500 desde Fortigate

Para la configuración del puerto de gestión, que permite la integración entre el Fortigate y NOZOMI P500, se debe seleccionar Network/Interfaces/lan4 e ingresar la configuración que se muestra en la figura 73.

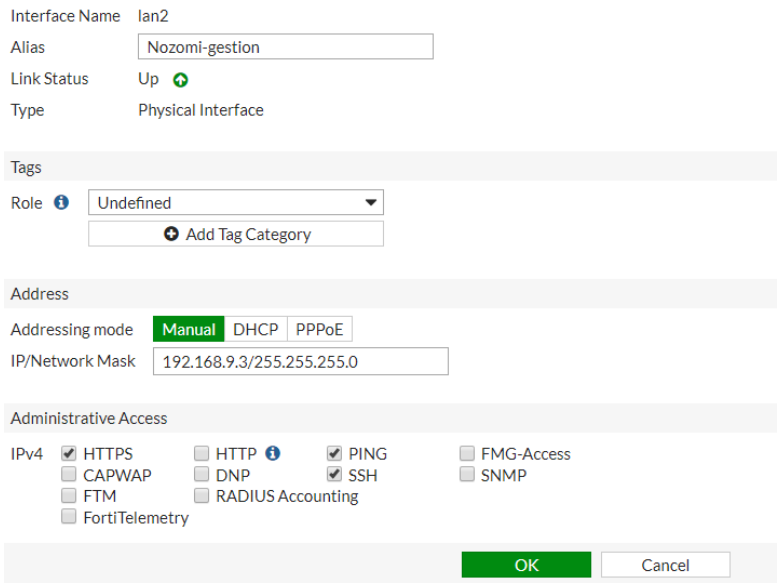


Figura 73: Configuración de puerto gestión de NOZOMI. Fuente propia

9.2. Asignación de VLAN a puertos del FortiSwitch

Para la asignación de VLAN a puertos del FortiSwitch se deben seguir los siguientes pasos:

- Asignar las VLAN creadas a los puertos del Fortiswitch. Se debe seleccionar /WIFI & Switch Controller/Managed FortiSwitch/ y luego dar clic en cualquiera de los puertos del FortiSwitch, como se muestra en la figura 74.

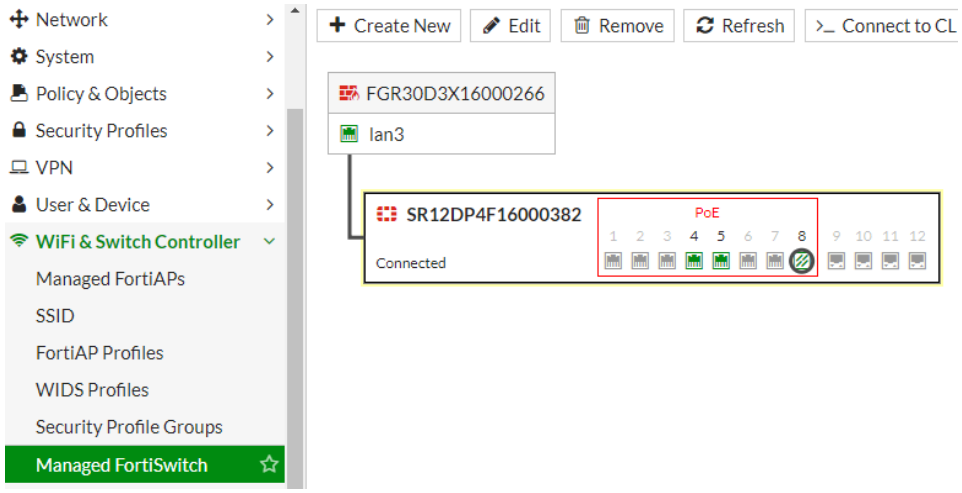


Figura 74: Configuración de puertos del FortiSwitch. Fuente propia

- Dar clic en Native VLAN de cada puerto y se selecciona cada VLAN a los puertos del FortiSwitch, como se muestra en la siguiente figura 75.

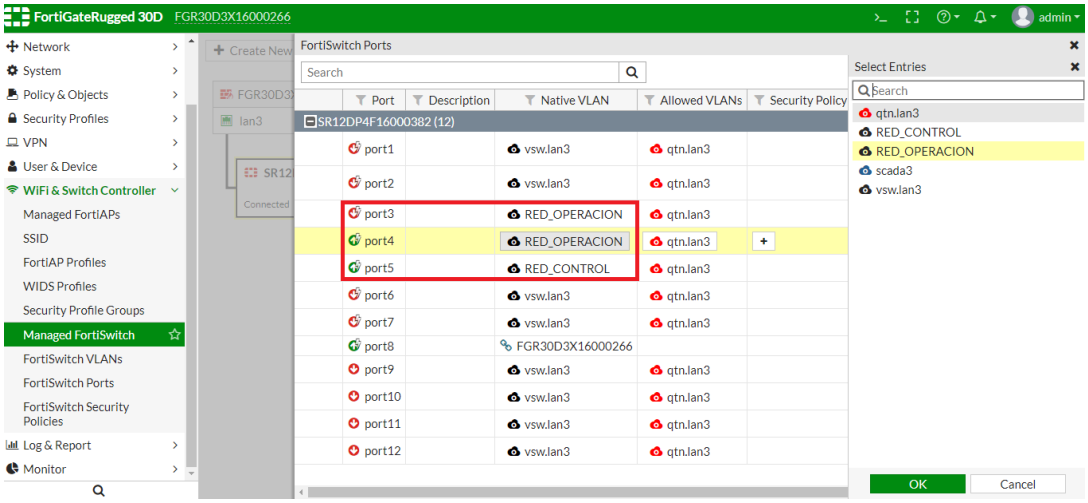


Figura 75: Asignar VLAN al puerto del FortiSwitch. Fuente propia

9.3. Configuración de políticas IPV4

- Para la configuración de políticas de IPV4. Se debe seleccionar /Policy & Objects/IPv4 Policy/Create New/ y crear cada política. se definieron seis políticas, ellas fueron: política de acceso de red de control a internet, política de acceso de red de control a gestión de NOZOMI P500, política de acceso de red de control a red de operación, política de acceso de red de operación a internet, política de acceso de red de operación a gestión de NOZOMI P500 y política de acceso de red de operación a red de control; tal como se muestra en las figuras 76,77,78,79,80,81, respectivamente.

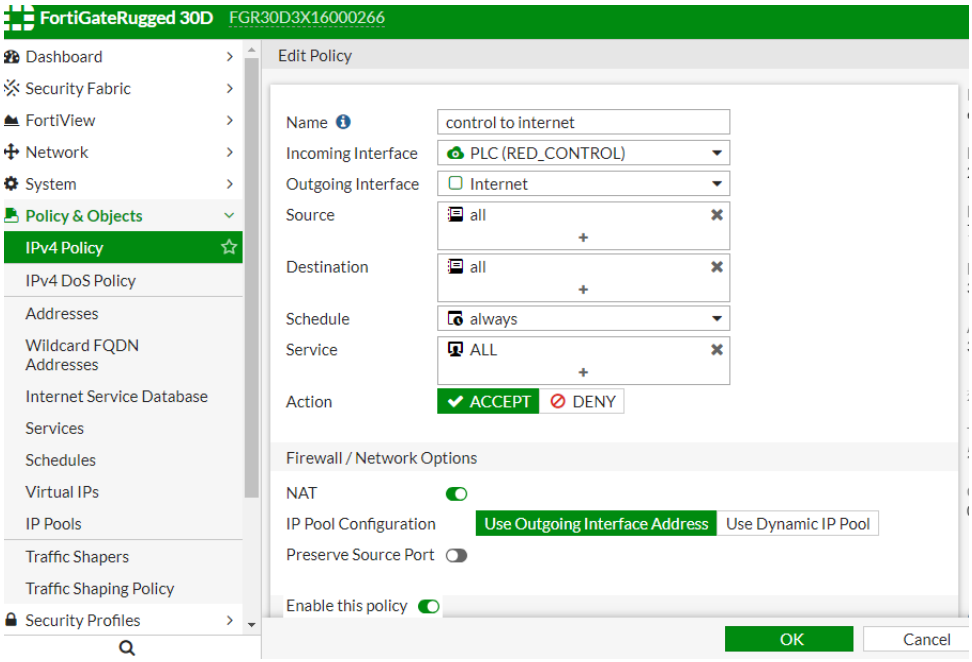


Figura 76: Red de control- Internet. Fuente propia

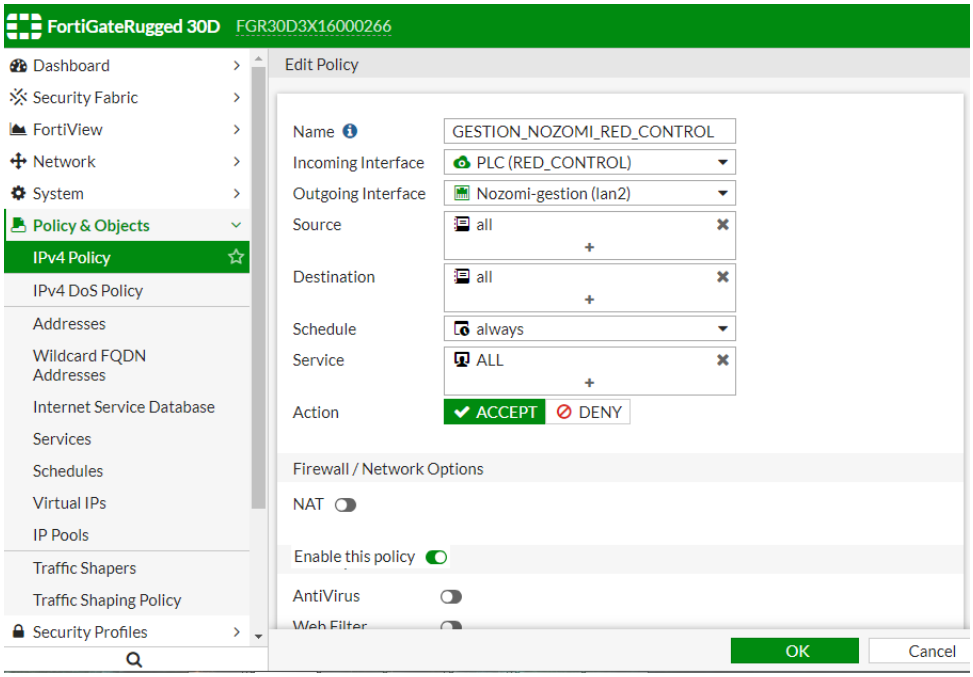


Figura 77: Red de control-NOZOMI P500. Fuente propia

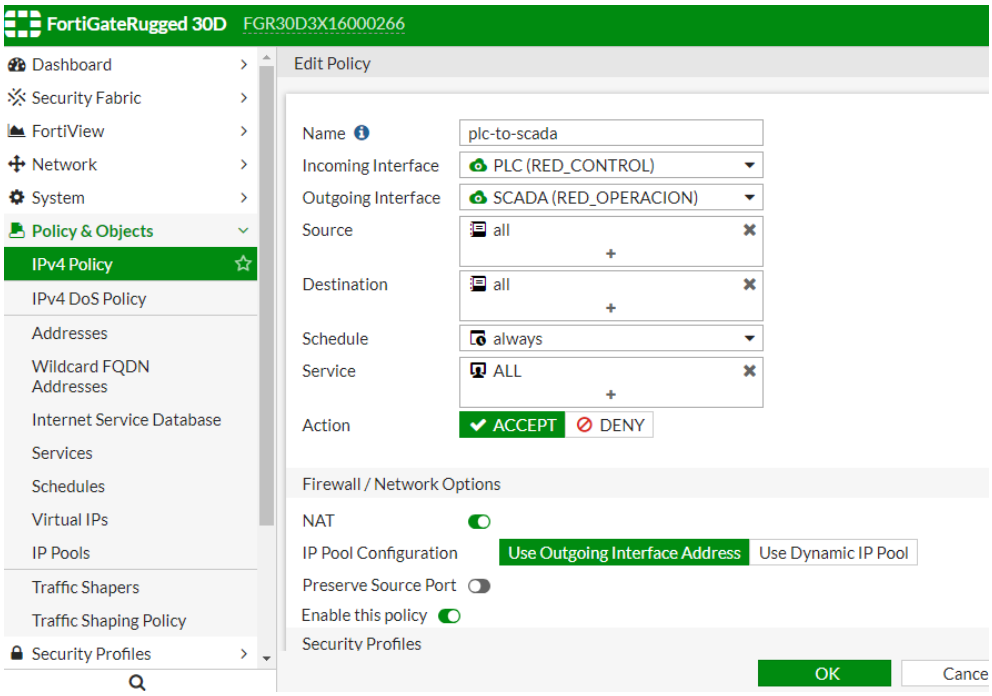


Figura 78:Red de control-Red de operación. Fuente propia

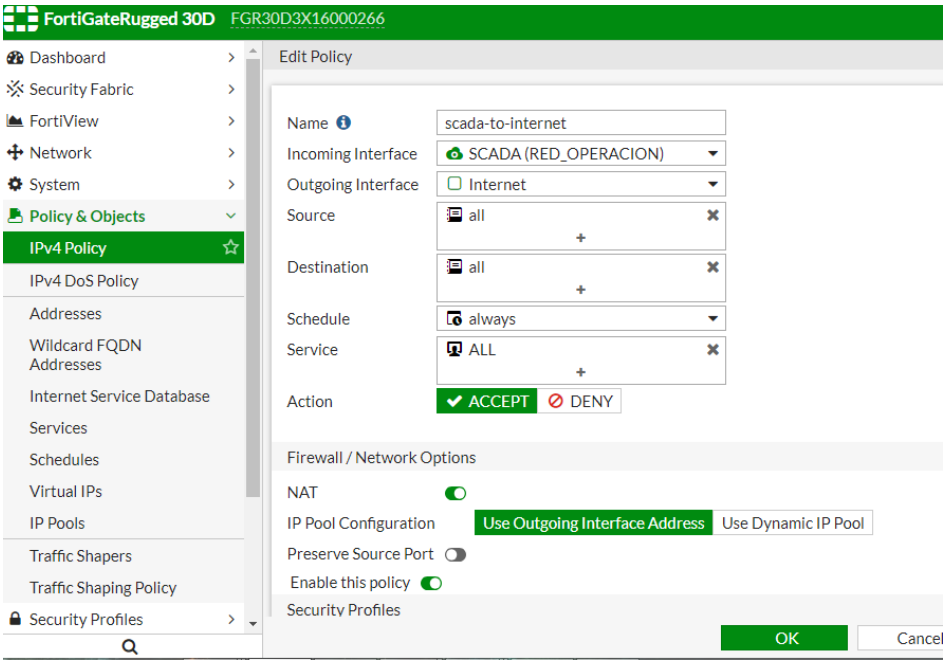


Figura 79:Red de operación-Internet. Fuente propia

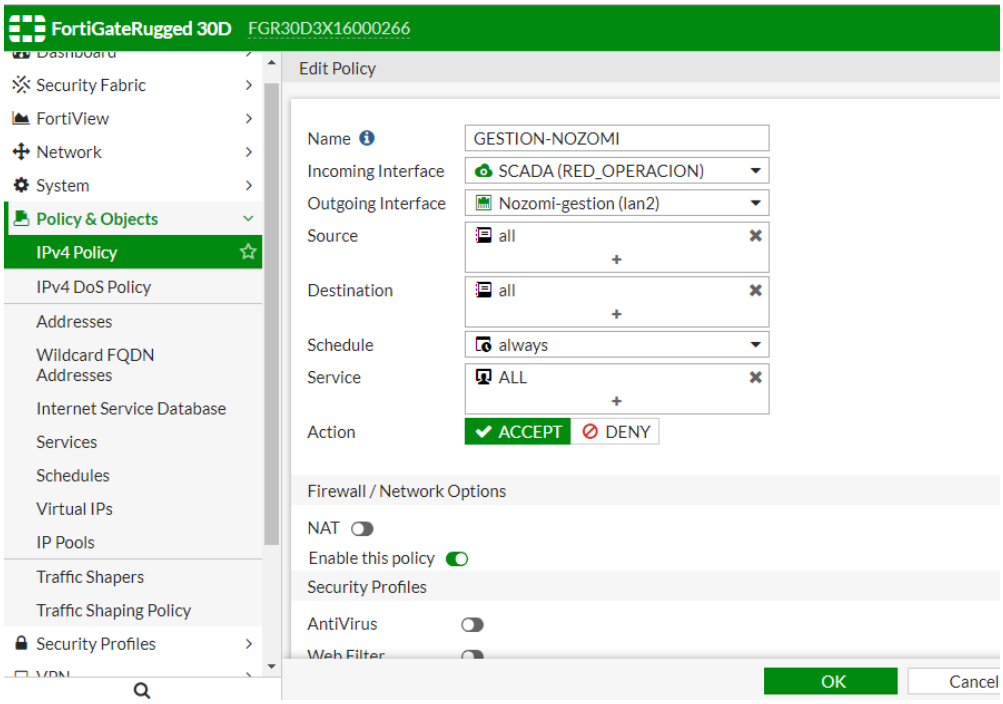


Figura 80: Red de operación-gestión NOZOMI P500. Fuente propia

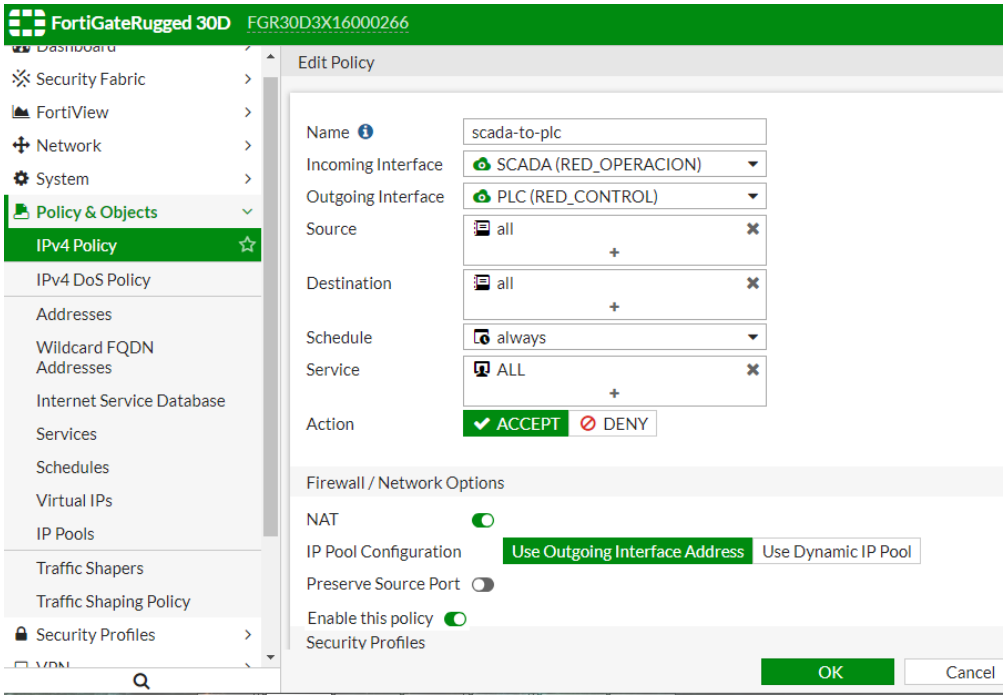


Figura 81:Red de operación-red de control. Fuente propia

- Se procede a realizar las conexiones físicas entre los equipos como se muestra en la figura 60.

- Para acceder de nuevo a la interfaz del FortiGate desde el host de la red de control, se debe fijar una dirección IP estática. En Windows 8.1 se realiza de la siguiente manera. Ingresar /Panel de control/Redes e Internet/Centro de redes y recursos compartidos/ clic en cambiar configuración de adaptador. (ver Figura 82)

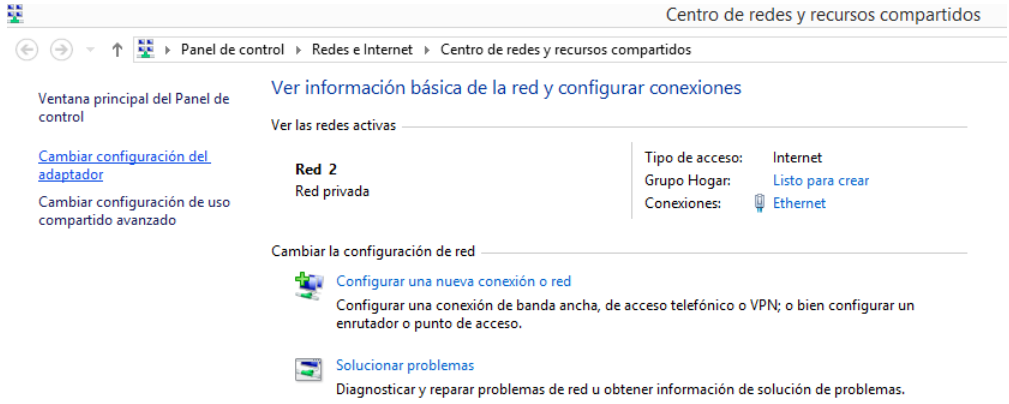


Figura 82: Cambiar configuración de Adaptador. Fuente propia

- Dar clic derecho en el adaptador Ethernet, luego clic en propiedades. (ver figura 83)

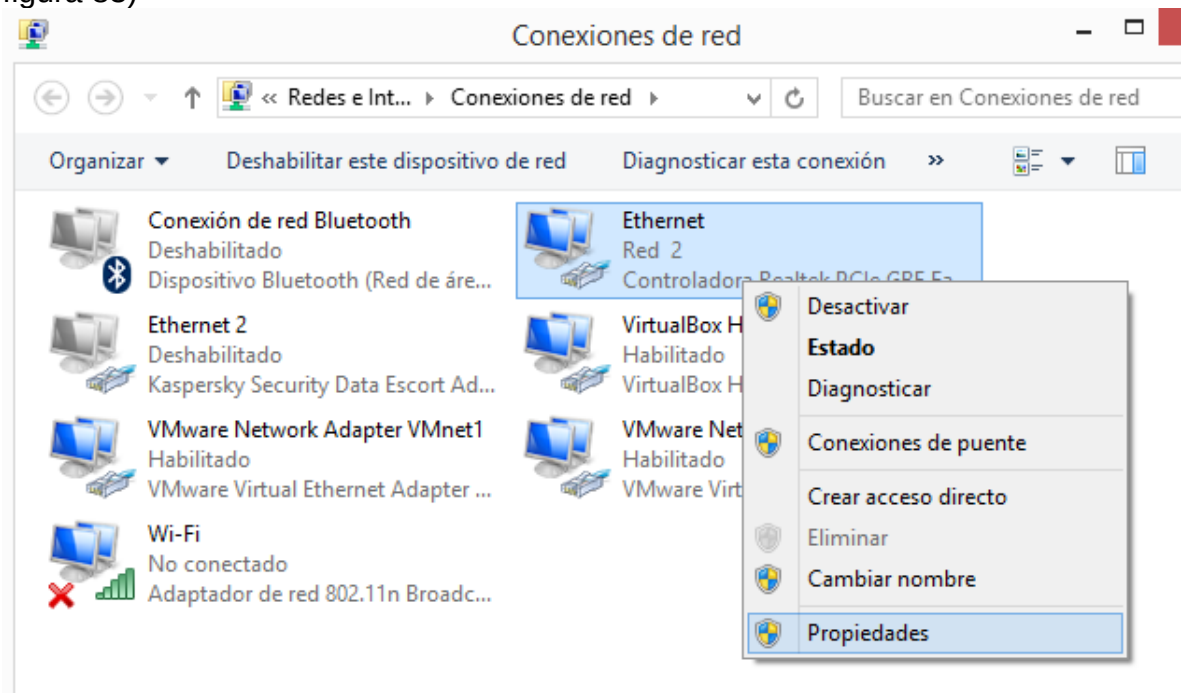


Figura 83: Adaptador Ethernet. Fuente propia

- Seleccionar protocolo de internet versión 4 y clic en propiedades

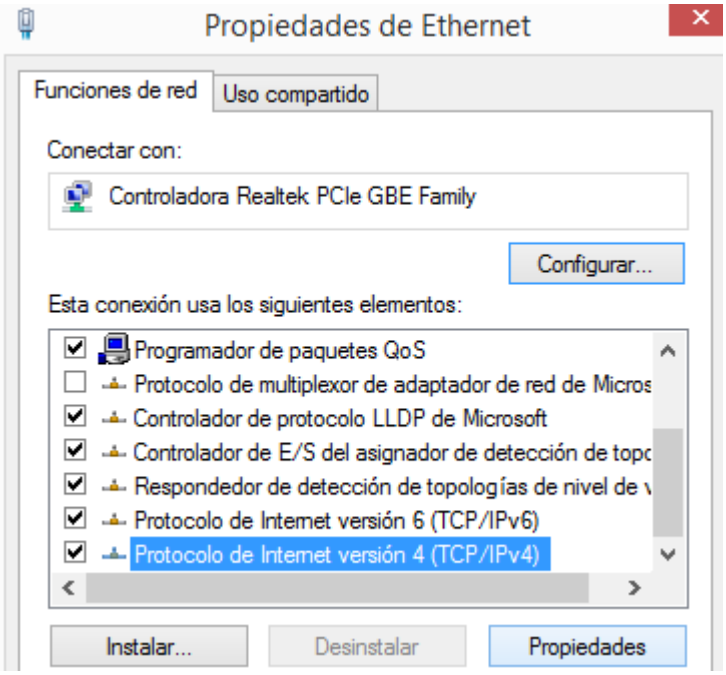


Figura 84: TCP/IPv4. Fuente propia

- Ingresar la configuración de IP estática y guardar la configuración (ver figura 85).

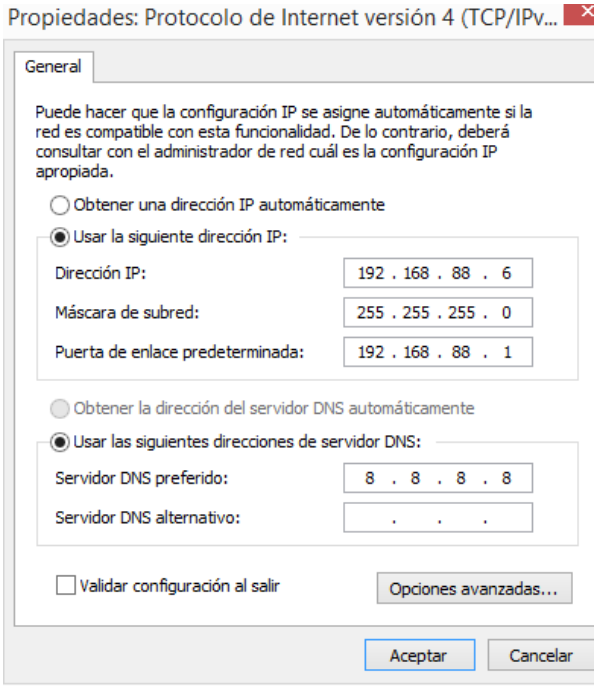


Figura 85: IP estática. Fuente propia

1. Para acceder de nuevo a la interfaz, se debe ingresar en el navegador la IP 192.168.88.1 login: admin y sin contraseña como se observa en la figura 86.

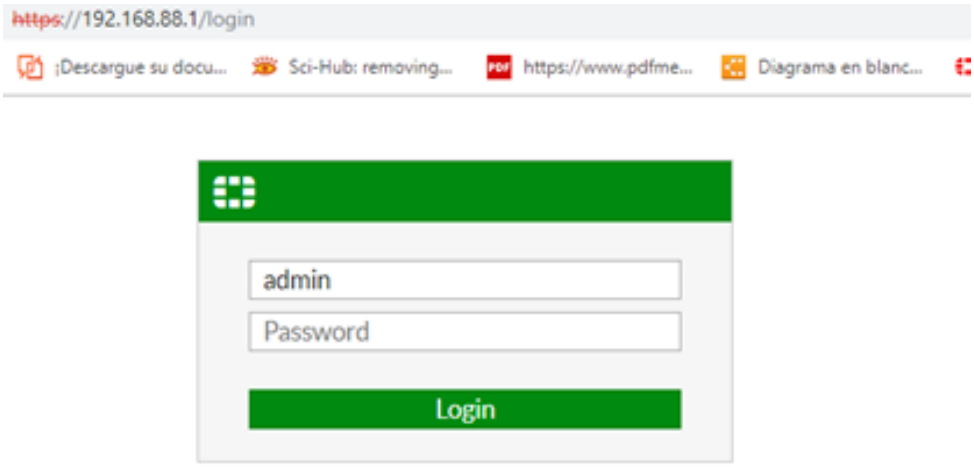


Figura 86: Nuevo acceso a interfaz del FortiGate. Fuente propia

2. Para acceder a la interfaz de NOZOMI P500, es necesario ingresar en el navegador la IP 192.168.9.11 login: admin y sin contraseña como se observa en la figura 87.

Figura 87: Acceso a NOZOMI P500. Fuente propia

9.4. Configuración Mirror Span

Se debe configurar un puerto espejo para capturar el tráfico del FortiGate y el FortiSwitch. Los pasos necesarios son los siguientes:

- Ingresar a la consola del FortiGate, como se muestra en la figura 88.

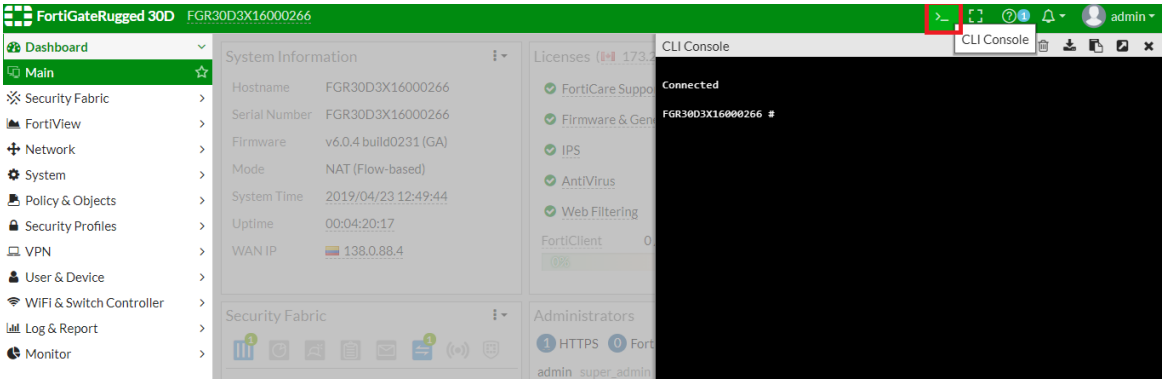


Figura 88: Ingreso a consola FortiGate. Fuente propia

- Se debe ingresar un listado de comandos (ver figura 89) para configurar el puerto 2 del FortiSwitch como espejo del tráfico que se presenta en los puertos 3,4,5 y 6.
    - config switch-controller managed-switch
    - edit **SR12DP4F16000382**
    - config mirror
    - edit nozomi
    - set status active
    - set dst port2
    - set switching-packet enable
    - set src-ingress port3 port4 port5 port6
    - set src-egress port3 port4 port5 port6

- Configuración mirror span para el FortiSwitch (ver figura 89)

```
FGR30D3X16000266 #
FGR30D3X16000266 # config switch-controller managed-switch

FGR30D3X16000266 (managed-switch) # edit SR12DP4F16000382

FGR30D3X16000266 (SR12DP4F16000382) # config mirror

FGR30D3X16000266 (mirror) # edit nozomi
new entry 'nozomi' added

FGR30D3X16000266 (nozomi) # set status active

FGR30D3X16000266 (nozomi) # set dst port1 port2

command parse error before 'port2'
Command fail. Return code -61

FGR30D3X16000266 (nozomi) # set dst port1

FGR30D3X16000266 (nozomi) # set dst port2

FGR30D3X16000266 (nozomi) # set switching-packet enable

FGR30D3X16000266 (nozomi) # set src-ingress port3 port4 port5 port6

FGR30D3X16000266 (nozomi) # set src-egress port3 port4 port5 port6
```

Figura 89: Configuración mirror Span. Fuente propia

- Para comprobar que la configuración esta correcta, se ingresa el comando **show** y se visualiza la configuración realizada (ver Figura 90).

```
FGR30D3X16000266 (nozomi) # show
config mirror
    edit "nozomi"
        set status active
        set switching-packet enable
        set dst "port2"
        set src-ingress "port3" "port4" "port5" "port6"
        set src-egress "port3" "port4" "port5" "port6"
    next
end

FGR30D3X16000266 (nozomi) #
```

Figura 90: Comprobar configuración mirror span. Fuente propia

Anexo C

SCADAguardian Report | 2019-04-11 11:44:19

Details for LUISFER (192.168.88.6)

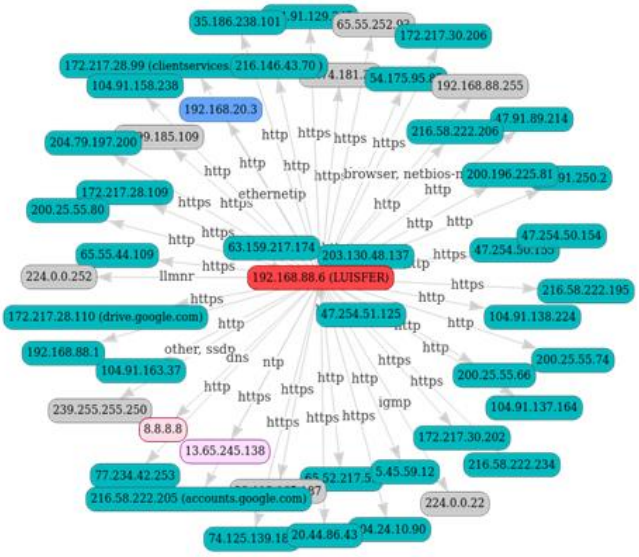
Type:computer

IP:192.168.88.6

MAC vendor :LCFC(HeFei) Electronics Technology Co., Ltd.

Roles: master

MAC address:192.168.88.6



Details for each node:192.168.88.6

appliance_host: nozomi-ids.local

label:LUISFER

id:192.168.88.6

ip:192.168.88.6

mac_address:28: d2:44:35:5e:99

mac_vendor: LCFC(HeFei) Electronics Technology Co., Ltd.

subnet: 192.168.88.0/24

zone: 192.168.88.0/24

type: computer

private_status: arp

is_confirmed : true

is_learned: true

is_fully_learned: true

_is_licensed: true

roles: master

links: 65.55.44.109, 216.58.222.234, 65.55.252.93, 65.52.217.59, 38.113.165.187, 104.91.163.37, 172.217.28.99, 20.44.86.43, 224.0.0.22, 200.25.55.66, 204.79.197.200, 216.58.222.206, 47.254.50.155, 47.91.89.214, 47.254.51.125, 216.146.43.70, 203.130.48.137, 47.254.50.154, 216.58.222.205, 38.99.185.109, 200.25.55.80, 104.91.138.224, 104.24.10.90, 63.159.217.174, 104.91.158.238, 192.168.20.3,224.0.0.252, 104.91.129.242,54.175.95.85, 35.186.238.101, 77.74.181.30, 200.25.55.74,88.191.250.2, 172.217.30.202, 192.168.88.1, 200.196.225.81,13.65.245.138, 216.58.222.195, 74.125.139.188, 77.234.42.253, 172.217.30.206, 5.45.59.12, 192.168.88.255, 172.217.28.109, 172.217.28.110, 104.91.137.164, 239.255.255.250, 8.8.8.8

links_count : 48

protocols : browser, dns, ethernetip, http, https, igmp, llmnr, netbios-ns, ntp,

created_at : other, ssdp 1554997024429

first_activity_time : 2019-04-11 10:37:04

last_activity_time : 2019-04-11 11:44:22

received.packets : 145317

received.bytes : 18729108

received.last_5m_bytes : 635754

received.last_15m_bytes : 2180136

received.last_30m_bytes : 4485920

sent.packets : 183955

sent.bytes : 48980640

sent.last_5m_bytes : 611580

sent.last_15m_bytes : 2129227

sent.last_30m_bytes : 4363175

tcp_retransmission.percent : 0.18

tcp_retransmission.packets : 204

tcp_retransmission.bytes : 120008

tcp_retransmission.last_5m_ bytes tcp_retransmission.last_15 m_bytes tcp_retransmission.last_30 m_bytes

properties: {"device_id"=>"LUISFER", "http.last_client_version"=>"Internet Explorer 9.0"}

bpf_filter : ip host 192.168.88.6

Installed software

Vendor	Product	Version	Update	Time
Microsoft	Internet Explorer	9	*	2019-04-11

Vulnerabilities

cve	cve score	cwe name
CVE-2014-1763	10.0	Resource Management Errors
CVE-2014-1776	10.0	Use After Free
CVE-2014-1764	10.0	Permissions, Privileges, and Access Controls
CVE-2013-3845	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-0307	9.3	Use After Free
CVE-2014-0308	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-0309	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-0310	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-0314	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-0322	9.3	Use After Free
CVE-2014-0324	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-0325	9.3	[unclassified]
CVE-2014-1751	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1753	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1755	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1770	9.3	Resource Management Errors
CVE-2014-1772	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1773	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1774	9.3	Improper Control of Generation of Code ('Code Injection')
CVE-2014-1775	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1779	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1783	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer

CVE-2014-1784	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1786	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1788	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1791	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1795	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1796	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1799	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1800	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1803	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-1805	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-2754	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-2757	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-2758	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-2759	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-2765	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2014-2766	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer

Anexo D

SCADAguardian Report | 2019-05-08 11:34:53

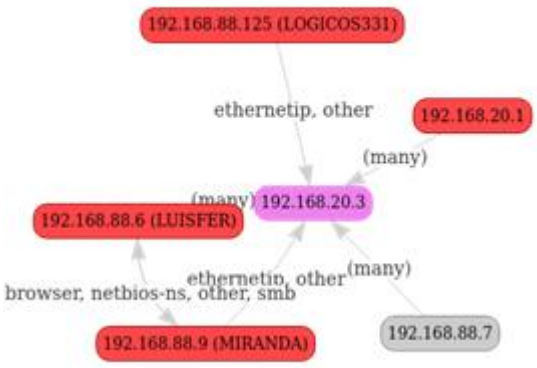
Details for MicroLogix 1763-L16BWA A/3.00 (192.168.20.3)

Type:PLC

OperatingSystemFirmware: 1.002 IP:192.168.20.3

MAC vendor: RS Automation Co., Ltd

Roles : dns_server, slave, web_server



Details for each node: 192.168.20.3

appliance_host : nozomi-ids.local

id: 192.168.20.3

ip: 192.168.20.3

mac_address: 00:0f:73:00:5e:5a

mac_vendor: RS Automation Co., Ltd

zone: Undefined

type: PLC

vendor: Rockwell Automation/Allen-Bradley

product_name: MicroLogix 1763-L16BWA A/3.00

firmware_version: 1.002

serial_number: 73005E5A

_private_status: arp

is_confirmed: true

is_learned: true

is_fully_learned: true

_is_licensed: true

roles: dns_server, web_server, slave

links:192.168.88.6, 192.168.88.6, 192.168.88.9, 192.168.88.7,192.168.20.1, 192.168.88.125

links_count: 6

protocols: bacnet-ip, cotp, dce-rpc, dns, ethernetip, ftps, ftps-data, http, https, ike, imap, imaps, kerberos, kms, ldaps, netbios-ns, netbios-ssn, other, pi-connect, pop3, smtp, snmp, ssh, tcp/1201, tcp/1332, tcp/1433, tcp/1521, tcp/19998, tcp/20000, tcp/2010, tcp/2404, tcp/3306, tcp/3389, tcp/4242, tcp/445, tcp/5001, tcp/502, tcp/55555, telnet, vnc

created_at: 1554997449147

first_activity_time: 2019-04-11 10:44:09

last_activity_time: 2019-05-08 11:34:56

received.packets: 5408181

received.bytes: 676263140

received.last_5m_bytes: 1169860

received.last_15m_bytes: 1909444

received.last_30m_bytes: 1909444

sent.packets: 5031011

sent.bytes: 698259588

sent.last_5m_bytes: 1247758

sent.last_15m_bytes: 2033864

sent.last_30m_bytes: 2033864

tcp_retransmission.percent: 0.0

tcp_retransmission.packets: 100

tcp_retransmission.bytes: 8590

tcp_retransmission.last_5m_: 0 bytes

tcp_retransmission.last_15: 0 m_bytes tcp_retransmission.last_30 : 0 m_bytes

properties:
{"ethernet_ip/product_code"=>"185","ethernet_ip/serial_number"=>"5A5E0073", "cip/serial_number"=>"73005E5A", "http.server_version"=>"A-B WWW/0.1", "ethernet_ip/product_name"=>"MicroLogix 1763- L16BWA A/3.00", "ethernet_ip/firmware_version"=>"1.002", "ethernet_ip/vendor"=>"Rockwell Automation/Allen-Bradley", "cip/device_type"=>"Communications Adapter", "device_id"=>"73005E5A", "cip/product_code"=>"185", "ethernet_ip/device_type"=>"Communications Adapter", "cip/firmware_version"=>"1.002", "cip/vendor"=>"Rockwell Automation/Allen-Bradley", "cip/product_name"=>"1763-L16BWA A/3.00"}

bpf_filter : ip host 192.168.20.3

Installed software

Vendor	Product	Version	Update	Time
A	B www	0.1	*	2019-04-25 10:45:33

Vulnerabilities

There are no vulnerabilities

Anexo E

SCADAguardian Report | 2019-05-03 14:10:47

Details for LOGICOS331 (192.168.20.125, 192.168.88.125,192.168.88.30)

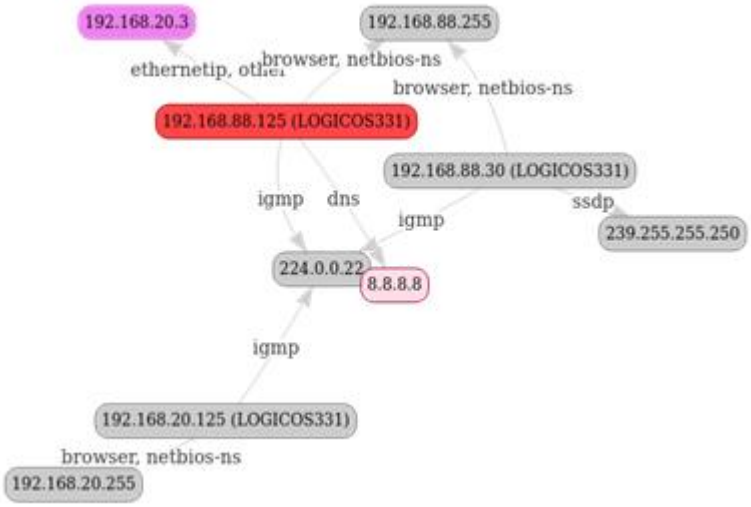
Type:computer Operating system :Windows XP

IP:192.168.20.125, 192.168.88.125, 192.168.88.30

MAC vendor:PCS Systemtechnik GmbH

Roles :master, other

MAC address:192.168.20.125, 192.168.88.125, 192.168.88.30



Details for each node:

192.168.20.125

appliance_host: nozomi-ids.local

label: LOGICOS331

id: 192.168.20.125

ip : 192.168.20.125

mac_address: 08:00:27:c3:34:8e

mac_vendor : PCS Systemtechnik GmbH

subnet: 192.168.20.0/24

zone: 192.168.20.0/24

type: computer

os: Windows XP

_private_status: no

is_confirmed: true

is_learned: true

is_fully_learned: true

_is_licensed: true

roles: other

links: 192.168.20.255, 224.0.0.22

links_count: 2

protocols: browser, igmp, netbios-ns

created_at: 1555331802115

first_activity_time: 2019-04-15 07:36:42

last_activity_time: 2019-04-26 10:31:06

received.packets: 15

received.bytes: 1470

received.last_5m_bytes: 0

received.last_15m_bytes:0

received.last_30m_bytes:0

sent.packets: 203

sent.bytes: 23858

sent.last_5m_bytes : 0

sent.last_15m_bytes : 0

sent.last_30m_bytes: 0

tcp_retransmission.percent : 0

tcp_retransmission.packets : 0

tcp_retransmission.bytes: 0

tcp_retransmission.last_5m_bytes: 0

tcp_retransmission.last_15m_bytes 0

tcp_retransmission.last_30m_bytes: 0

properties: {"device_id"=>"LOGICOS331"}

bpf_filter:ip host 192.168.20.125, 192.168.88.125

appliance_host: nozomi-ids.local

label: LOGICOS331

id: 192.168.88.125

ip: 192.168.88.125

mac_address: 08:00:27:c3:34:8e

mac_vendor: PCS Systemtechnik GmbH

subnet: 192.168.88.0/24

zone: 192.168.88.0/24

ype: computer

os: Windows XP

_private_status :arp

is_confirmed : true

roles: master

links: 192.168.20.3, 192.168.88.255, 8.8.8.8, 224.0.0.22

links_count: 4

protocols: browser, dns, ethernetip, igmp, netbios-ns, other

created_at: 1556290587480

first_activity_time: 2019-04-26 09:56:27

last_activity_time: 2019-05-03 14:04:04

received.packets: 379989

received.bytes: 52309299

received.last_5m_bytes: 0

received.last_15m_bytes: 0

received.last_30m_bytes:0

sent.packets: 384308

sent.bytes: 49248646

sent.last_5m_bytes: 0

sent.last_15m_bytes: 2732

sent.last_30m_bytes: 5464

tcp_retransmission.percent: 0.0

tcp_retransmission.packet: 10

tcp_retransmission.bytes: 1000

tcp_retransmission.last_5m_bytes: 0

Installed software

Vendor	Product	Version	Update	Time
Microsoft	Windows XP	-	*	2019-04-15 07:36:52
Microsoft	Windows XP	-	*	2019-04-26 09:57:31
Microsoft	Windows XP	-	*	2019-05-03 13:31:12

Vulnerabilities

cve	cve score	cwe name
CVE-2006-3441	10.0	[unclassified]
CVE-2010-2550	10.0	Improper Input Validation
CVE-2012-4786	10.0	Improper Control of Generation of Code ('Code Injection')
CVE-2011-1268	10.0	Improper Input Validation
CVE-2012-1853	10.0	Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2006-2373	10.0	Permissions, Privileges, and Access Controls
CVE-2006-3440	10.0	[unclassified]

Bibliografía

[1] «Red Seguridad.Revista especializada en Seguridad TIC». [En línea]. Disponible en: http://www.redseguridad.com/sectores-tic/infraestructuras-criticas/un-modelo-devops-entre-it-y-ot-es-mas-eficaz-que-su-convergencia. [Accedido: 10-jun-2019].

[2] «MCS | CONVERGENCIA DE IT Y OT». [En línea]. Disponible en: https://mcs.com.mx/convergencia-de-it-y-ot/. [Accedido: 12-feb-2019].

[3] «Tecnología de la Información - Qué es y Definición 2019». [En línea]. Disponible en: https://conceptodefinicion.de/tecnologia-de-la-informacion/. [Accedido: 12-jun-2019].

[4] «Tecnología Operacional – Tecnologías de Información». [En línea]. Disponible en: https://jnbello.co/tag/tecnologia-operacional/. [Accedido: 12-jun-2019].

[5] «Seguridad IT versus Ciberseguridad Industrial - Ciberseguridad Industrial, by Logitek.» [En línea]. Disponible en: https://www.ciberseguridadlogitek.com/seguridad-it-versus-ciberseguridad-industrial/. [Accedido: 16-may-2019].

[6] «Por qué debe plantearse la convergencia entre sistemas OT e IT | Actualidad | RED CW». [En línea]. Disponible en: https://red.computerworld.es/actualidad/por-que-debe-plantearse-la-convergencia-entre-sistemas-ot-e-it. [Accedido: 12-jun-2019].

[7] «¿Qué son las TI?», *InformeTICfacil.com*, 10-dic-2012. .

[8] «Buscar en el diccionario informático». [En línea]. Disponible en: https://www.lawebdelprogramador.com/diccionario/buscar.php?opc=1&charSearch=tarjeta+de+red. [Accedido: 26-jun-2019].

[9] «Qué es un servidor y para qué sirve - Blog Infortelecom». [En línea]. Disponible en: https://infortelecom.es/blog/que-es-un-servidor-y-para-que-sirve/. [Accedido: 26-jun-2019].

[10] «Routers». [En línea]. Disponible en: http://redesdecomputadores.umh.es/red/routers/default.html. [Accedido: 26-jun-2019].

[11] «¿Qué es un firewall? - Cisco». [En línea]. Disponible en: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html. [Accedido: 26-jun-2019].

[12] «▷ Modelo OSI: que es y para que se utiliza». [En línea]. Disponible en: https://www.profesionalreview.com/2018/11/22/modelo-osi/. [Accedido: 25-jun-2019].

[13] «Capa 4 OSI | Capa de Transporte | El Taller del Bit». [En línea]. Disponible en: https://eltallerdelbit.com/capa-4-osi-capa-de-transporte/. [Accedido: 25-jun-2019].

[14] «¿Qué es la seguridad de la red? | Seguridad | NetworkWorld». [En línea]. Disponible en: https://www.networkworld.es/seguridad/que-es-la-seguridad-de-la-red. [Accedido: 27-jun-2019].

[15] «¿Qué es SIEM?» [En línea]. Disponible en: https://www.helpsystems.com/es/blog/que-es-un-siem. [Accedido: 09-ago-2019].
[16] «¿Qué es y cómo funciona una VPN para la privacidad de la información? | WeLiveSecurity». [En línea]. Disponible en: https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/. [Accedido: 10-ago-2019].
[17] M. N. Solutions, «MCS | CONVERGENCIA DE IT Y OT». .
[18] «Redes OT». [En línea]. Disponible en: https://gotor.com/redes-ot-industria-4-0/. [Accedido: 12-feb-2019].
[19] «El modelo de Purdue para sistemas de control industrial - Ciberseguridad industrial.» [En línea]. Disponible en: https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems. [Accedido: 24-jul-2019].
[20] «Integración SIEM-SOC: Ciberseguridad-privacidad motores clave y esencia de la accesibilidad y sostenibilidad real y creíble - Electrónica». [En línea]. Disponible en: http://www.interempresas.net/Electronica/Articulos/232650-Integracion-SIEM-SOC-Ciberseguridad-privacidad-motores-clave-esencia-accesibilidad.html. [Accedido: 05-jul-2019].
[21] Nozomi Networks, «Real-time Cybersecurity and Visibility for Industrial Control Networks». .
[22] ISA, *Using the ISA/IEC 62443 Standard to Secure Your Control Systems*. .
[23] «La convergencia de los mundos IT y OT para afrontar la seguridad | SEGURIDAD EN CIFRAS | CSO España». [En línea]. Disponible en: https://cso.computerworld.es/seguridad-en-cifras/la-convergencia-de-los-mundos-it-y-ot-para-afrontar-la-seguridad. [Accedido: 12-feb-2019].
[24] Fortinet, *Asegurar los sistemas de control industrial con Fortinet Seguridad de principio a fin conforme a la norma IEC-62443*. 2015.
[25] «Secure&IT | Seguridad de la Información - Seguridad informática». [En línea]. Disponible en: https://www.secureit.es/. [Accedido: 05-jul-2019].
[26] «ANSI / ISA-62443-1-1 (99.01.01) -2007 Seguridad para sistemas de control y automatización industrial Parte 1-1: Terminología, conceptos y modelos». [En línea]. Disponible en: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=118192. [Accedido: 11-feb-2019].
[27] K. Ronald, *Industrial Automation and Control System Security Principles: Protecting the Critical Infrastructure*. .
[28] ISA, «Manufacturing and Control Systems Security-Part 1: Concepts, Models and Terminology». 2005.
[29] R. M. Oscar Hernán, «ESTUDIO DE METODOLOGÍAS DE ANÁLISIS FORENSE ANTE INCIDENTES DE CIBERSEGURIDAD».
[30] ISA, «Security Technologies for Manufacturing and Control Systems-ANSI/ISA—TR99.00.01». 2004.

[31] «seguridad informática y sus Características principales -Rentadvisor». [En línea]. Disponible en: https://www.rentadvisor.com.co/seguridad-informatica-caracteristicas/. [Accedido: 24-jul-2019].
[32] «Seguridad Informatica: ¿Para qué sirve la seguridad informática?» [En línea]. Disponible en: http://seguridadinformatica-ezequielgarcia.blogspot.com/2012/08/para-que-sirve-la-seguridad-informatica.html?m=1. [Accedido: 05-jul-2019].
[33] «Fortinet | Deliver Secure Digital Transformation». [En línea]. Disponible en: https://www.fortinet.com/. [Accedido: 24-jul-2019].
[34] «ICS Cyber Security | Superior Operational Visibility - Nozomi Networks». [En línea]. Disponible en: https://www.nozominetworks.com/products/solution-overview/. [Accedido: 14-feb-2019].
[35] «Escáner de vulnerabilidades Nessus Professional™». [En línea]. Disponible en: https://es-la.tenable.com/products/nessus/nessus-professional?tns_redirect=true. [Accedido: 16-may-2019].
[36] «Sistemas de control industrial de seguridad cibernética.» [En línea]. Disponible en: https://www.indegy.com/company/. [Accedido: 14-feb-2019].
[37] «Security Services | Cybersecurity Service Offerings | Carbon Black». [En línea]. Disponible en: https://www.carbonblack.com/resources/services/. [Accedido: 14-feb-2019].
[38] «Nmap: el mapeador de red - escáner de seguridad gratuito». [En línea]. Disponible en: https://nmap.org/. [Accedido: 01-ago-2019].