

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
SEDE VIÑA DEL MAR – JOSÉ MIGUEL CARRERA

DISEÑO Y ARQUITECTURA DE RED SEGURA PARA SCADA

Trabajo de Titulación para optar al Título de
Ingeniero de Ejecución en CONTROL E
INSTRUMENTACIÓN INDUSTRIAL

Alumno:

Michel Andruz Tretter Hidalgo

Profesor Guía:

Mag. Víctor Hugo Cárdenas Schweiger.

2026



CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título ☐ Tesis de Postgrado

Título del trabajo: Diseño y Arquitectura de Red Segura para SCADA

Nombre del candidato(a): Michel Andruz Tretter Hidalgo

Carrera/Grado: Ingeniería de ejecución en control e instrumentación industrial

Campus: Sede José Miguel Carrera, Viña del mar.

Departamento: Electrotecnia e Informática

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Víctor Cárdenas Schweiger, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución.

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL (marcar una opción)

☒ El trabajo **NO contiene** información que amerite confidencialidad y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (**embargo**) por (**marcar una opción**):

☐ 6 meses ☐ 12 meses ☐ 2 años ☐ 3 años ☐ 5 años ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 05-08-2026 Firma: 

Estudiante o Candidato(a):

Fecha: 05-08-2026 Firma: 

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

RESUMEN

KEYWORDS: SCADA, SEGURIDAD, REDES, VLAN.

El presente trabajo de título aborda el diseño y arquitectura de red segura para SCADA (Supervisión, Control y Adquisición de Datos), los cuales son ampliamente utilizados en las industrias debido a la gran cantidad de amenazas cibernéticas en entornos industriales, a su vez, se analizará la metodología basada en el análisis de estándares de ciberseguridad industrial (ISA/IEC 62443).

La estructura del desarrollo se desglosa en las siguientes etapas:

Capítulo 1: Se presentará la problemática actual de los entornos industriales y se evaluarán distintas alternativas tecnológicas. A través de un análisis comparativo, se seleccionarán las soluciones más efectivas para mitigar los riesgos detectados.

Capítulo 2: Se llevará a cabo el desarrollo técnico y la arquitectura de red, realizando la simulación de la topología propuesta en la plataforma GNS3. En esta fase se configurarán la segmentación de red y los controles de seguridad definidos.

Capítulo 3: Se realizará un análisis de resultados mediante pruebas de seguridad ofensiva utilizando Kali Linux para validar la robustez de la topología. Finalmente, se presentará un análisis de costos estimados para la implementación real del proyecto en un entorno industrial.

Como resultado, se espera aportar un diseño escalable y validado que garantice la confidencialidad, integridad y disponibilidad de los procesos críticos en entornos SCADA.

ÍNDICE

INTRODUCCIÓN	1
CAPÍTULO 1: ANTECEDENTES GENERALES	2
1 ANTECEDENTES GENERALES	3
1.1 PLANTEAMIENTO DEL PROBLEMA	3
1.2 DEFINICIÓN DEL PROBLEMA	3
1.3 IMPORTANCIA DE RESOLVERLO	5
1.3.1 Estado de la ciberseguridad OT en Chile	6
1.4 INVOLUCRADOS PRINCIPALES	7
1.4.1 Sectores más afectados en Chile	8
1.5 SOLUCIÓN DEL PROBLEMA	8
1.6 REQUERIMIENTOS	8
1.6.1 Segmentación de redes IT/OT	9
1.6.2 Creación de una zona desmilitarizada (DMZ)	9
1.6.3 Permisos de control de acceso	10
1.7 ALTERNATIVAS DE SOLUCIÓN	10
1.7.1 Alternativa 1: Aislar la red industrial	11
1.7.2 Alternativa 2: Mejorar la red	11
1.7.3 Alternativa 3: Rediseñar la Red	12
1.7.4 Evaluación de la solución	13
1.7.5 Elección de la solución	14
1.7.6 Herramientas tecnológicas de la solución seleccionada	15
1.7.6.1 GNS3	15
1.7.6.2 Kali Linux	15
1.7.6.3 VMware	16
1.7.6.4 pfSense	16
1.7.6.5 Packet Tracer	16
1.8 OBJETIVOS	17
1.8.1 Objetivo general	17
1.8.2 Objetivos específicos	17
CAPÍTULO 2: DESARROLLO DE LA SOLUCIÓN	19
2 DESARROLLO DE LA SOLUCIÓN	20
2.1 SEPARACIÓN DE LA RED IT DE LA OT	20
2.1.1 Arquitectura de referencia industrial	21

2.1.2	Rediseño de red	22
2.2	DISPOSITIVOS	24
2.2.1	Switch Cisco Catalyst 1300	24
2.2.2	Firewall	25
2.2.3	Computador	26
2.2.4	HMI	27
2.2.5	PLC	27
2.2.6	Servidores	28
2.2.7	Cloud	28
2.3	CONEXIONADO	29
2.4	CONFIGURACIÓN	31
2.4.1	Máquina virtual de GNS3	31
2.4.1.1	Enlace de máquina virtual con GNS3	32
2.4.2	VLAN	33
2.4.2.1	Creación de VLAN	34
2.4.2.2	Enlace troncal	34
2.4.2.3	Modo acceso	35
2.4.3	Instalación y configuración del firewall	36
2.4.3.1	Instalación pfSense	36
2.4.3.2	Configuración pfSense	38
2.4.3.3	Interfaz web pfSense	39
2.4.3.4	Reactivación de reglas del firewall	40
2.5	Enrutamiento inter-VLAN	40
2.6	Reglas del firewall	42
2.6.1	Acceso a Internet	42
2.6.2	Acceso a la DMZ IT	42
2.6.3	Regla de Aislamiento de la red OT	43
2.7	Topología de red en GNS3	44
2.8	Seguridad del sistema SCADA	46
CAPÍTULO 3: ANÁLISIS DE RESULTADOS Y COSTOS		49
3	ANÁLISIS DE RESULTADOS Y COSTOS	50
3.1	DIRECCIÓN IP	50
3.2	PRUEBAS DESDE KALI LINUX	51
3.2.1	Escaneo de puertos	52
3.2.1.1	Escenario A: Con firewall configurado	52
3.2.1.2	Escenario B: Con regla de acceso total	53

3.2.2	Prueba de ataque DoS	54
3.2.3	Prueba de escaneo de huella digital	55
3.2.3.1	Escenario A: Con firewall configurado.....	55
3.2.3.2	Escenario B: con regla de acceso total	56
3.2.2	Conclusión pruebas Kali Linux.....	57
3.3	EVALUACIÓN DE COSTOS	57
3.3.1	Profesionales necesarios	58
3.3.1.1	Ingeniero en control e instrumentación Industrial	58
3.3.1.2	Ingeniero en redes o ciberseguridad	58
3.3.1.3	Técnico en telecomunicaciones y redes	59
3.3.2	Fases y carga horaria	59
3.3.3	Costos profesionales.....	60
3.3.4	Costos de Dispositivos	61
3.3.4.1	Justificación de cada dispositivo	62
3.3.4.2	Consideraciones de diseño	63
3.3.5	Costos totales.....	63
3.3.5.1	Análisis de costos totales	64
CONCLUSIONES		65
BIBLIOGRAFÍA		66
ANEXOS.....		66
ANEXO A: SUELDOS PROMEDIO PROFESIONALES MIFUTURO.CL.....		67
ANEXO B: LINKS DE COMPRAS EQUIPOS.....		69

ÍNDICE DE FIGURAS

Figura 1-1 Protocolos de sistemas de control industrial	5
Figura 1-2 Nivel de sensibilidad de las organizaciones industriales	6
Figura 1-3 Prioridades del Triángulo de Seguridad CIA en Tecnologías IT y OT	9
Figura 1-4 Segmentación IT/OT mediante cortafuegos y zona desmilitarizada	10
Figura 1-5 Interfaz GNS3	15
Figura 1-6 Interfaz Kali Linux	16
Figura 2-1 Red sin segmentación	21
Figura 2-2 Modelo Purdue	22
Figura 2-3 Rediseño de la red con segmentación	23
Figura 2-4 Switch Cisco 1300	25
Figura 2-5 Switch 1300 en GNS3	25
Figura 2-6 pfSense en GNS3	26
Figura 2-7 PC en GNS3	26
Figura 2-8 HMI en GNS3	27
Figura 2-9 PLC en GNS3	27
Figura 2-10 Servidor en GNS3	28
Figura 2-11 Cloud en GNS3	29
Figura 2-12 Parámetros VM GNS3	32
Figura 2-13 Configuración VM en GNS3	33
Figura 2-14 Creación de VLAN en Switch-IT	34
Figura 2-15 Configuración de enlace troncal en Switch-IT	35
Figura 2-16 Configuración de acceso	36

Figura 2-17 Instalador pfSense.....	37
Figura 2-18 Consola pfSense	38
Figura 2-19 Asignación de interfaces	39
Figura 2-20 Interfaz web pfSense.....	41
Figura 2-21 Regla de paso	40
Figura 2-22 VLAN en firewall.....	41
Figura 2-23 Puertas de enlace.....	41
Figura 2-24 Regla para acceso DMZ-IT	43
Figura 2-25 Reglas de aislamiento OT	44
Figura 2-26 Topología de red en GNS3.....	45
Figura 2-27 Flujo de comunicación PLC	47
Figura 3-1 Prueba de escaneo A.....	53
Figura 3-2 Prueba de escaneo B.....	53
Figura 3-3 Comando DoS	54
Figura 3-4 Gráfico de uso del sistema.....	55
Figura 3-5 Resultado A	56
Figura 3-6 Resultado B	56

ÍNDICE DE TABLAS

Tabla 1-1 Causas principales	4
Tabla 1-2 Resumen principales afectados	7
Tabla 1-3 Calificación para la selección de alternativas	13
Tabla 1-4 Calificación de alternativas.....	14
Tabla 2-1 Conexión de interfaces.....	30
Tabla 3-1 Direcciones dispositivos	51
Tabla 3-2 Carta Gantt	59
Tabla 3-3 Pago por hora.....	60
Tabla 3-4 Costos de Dispositivos	61
Tabla 3-5 Costos totales.....	64

SIGLAS Y SIMBOLOGÍA

A. SIGLAS

ACK	: Acuse de recibo
CCI	: Centro de Ciberseguridad Industrial
DoS	: Denegación de Servicio
DMZ	: Zona Desmilitarizada
GNS3	: Graphical Network Simulator-3
HMI	: Interfaz Hombre-Máquina
HTTP	: Protocolo de Transferencia de Hipertexto
ICS	: Sistemas de Control Industrial
IEC	: Comisión Electrotécnica Internacional
IEEE	: Instituto de Ingenieros Eléctricos y Electrónicos
IP	: Protocolo de Internet
ISA	: Sociedad Internacional de Automatización
IT	: Tecnologías de la Información
MAC	: Dirección de Control de Acceso al Medio
OT	: Tecnologías de la Operación
PC	: Computadora Personal
PLC	: Controlador Lógico Programable
SCADA	: Supervisión, Control y Adquisición de Datos
SMTP	: Protocolo Simple de Transferencia de Correo
SSH	: Protocolo de Shell Seguro
TCP	: Protocolo de Control de Transmisión
UDP	: Protocolo de Datagramas de Usuario
VLAN	: Red de Área Local Virtual

VPN : Red Privada Virtual

B. SIMBOLOGÍA

b : bit

B : Byte

Mbps : Megabits por segundo

TB : Terabyte

VA: : Volt/Amperio

W : Watts

INTRODUCCIÓN

Los sistemas SCADA (Supervisión, Control y Adquisición de Datos) son pilares de los sistemas de automatización en la actualidad, su relevancia deriva no sólo de la eficiencia y la regulación, sino también de la continuidad operativa y la salvaguarda de las infraestructuras críticas. Sin las medidas de seguridad apropiadas, estos sistemas pueden ser fácilmente el punto débil más crítico de cualquier empresa o sector estratégico.

Una seguridad ineficiente en sistemas SCADA puede tener consecuencias graves, tanto a nivel técnico como económico y social.

En respuesta de la situación planteada, es clave desarrollar arquitecturas de red con mecanismos de seguridad adecuados que garanticen la confidencialidad, integridad y disponibilidad de la información, así como de los procesos industriales. Ésta es la premisa desde la que se construye este proyecto, que tiene como objetivo la propuesta del diseño de una red segura para entornos SCADA, teniendo en cuenta la segmentación que se hace entre redes IT/OT (Tecnologías de la Información/ Tecnologías de la Operación) y la implementación de la defensa en profundidad, así como los estándares internacionales de ciberseguridad industrial como ISA/IEC 62443, además, de la simulación de la topología en el software GNS3 para la validación de la propuesta como respuesta ante accesos no autorizados.

El alcance del proyecto se define sobre la propuesta de arquitectura y su validación bajo simulación, sin la necesidad de realizar una implementación física de la red o de la integración con sistemas SCADA reales, lo cual hace posible realizar evaluaciones de forma segura y controlada con respecto a las medidas de protección.

CAPÍTULO 1: ANTECEDENTES GENERALES

1 **ANTECEDENTES GENERALES**

En el desarrollo de este capítulo se consideran los antecedentes técnicos, operativos y económicos relacionados con los sistemas SCADA, con el fin de identificar la problemática existente y plantear soluciones que permitan proteger de manera efectiva estos sistemas. Asimismo, se incluyen las recomendaciones legales y normativas aplicables en Chile, asegurando que la arquitectura de red propuesta cumpla con los marcos regulatorios y estándares de ciberseguridad industrial, como la Ley N°21.459, la Ley N°19.628 y los lineamientos de ISA/IEC (Sociedad Internacional de Automatización y Comisión Electrotécnica Internacional) 62443, garantizando así la confidencialidad, integridad y disponibilidad de los procesos industriales.

1.1 **PLANTEAMIENTO DEL PROBLEMA**

El problema para solucionar es que muchos sistemas SCADA actuales presentan baja seguridad debido a la falta de segmentación de redes, arquitecturas obsoletas y configuraciones inadecuadas, lo que aumenta su vulnerabilidad frente a ciberataques y compromete la operación segura de los procesos industriales.

1.1.1 **Definición del problema**

Muchos sistemas SCADA siguen funcionando igual que hace años, sin cambios importantes en la red. Todavía no se separan bien las redes IT de las OT y no se usan medidas de seguridad por capas. Por eso es fácil que un ataque afecte la operación o interrumpa los procesos industriales, generando fallas o pérdida de datos. La tabla 1-1 muestra las categorías y causas específicas del problema

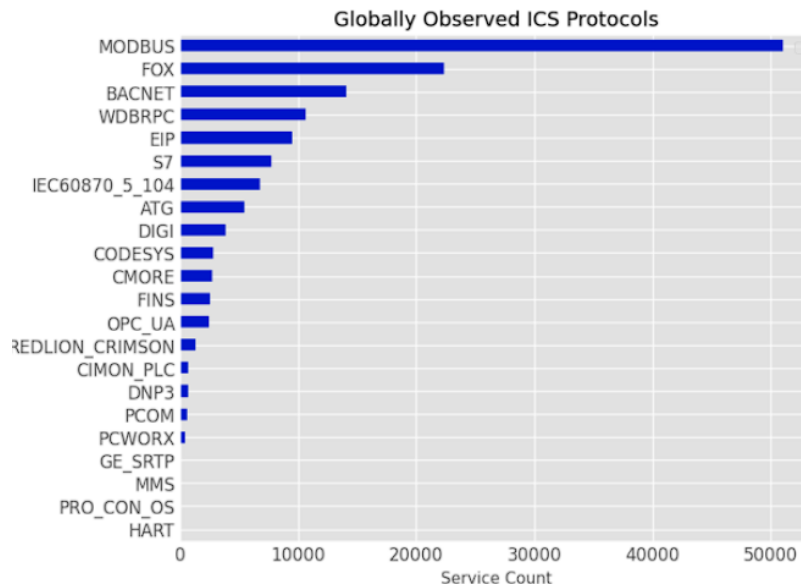
Tabla 1-1 Causas Principales.

Categoría	Causas específicas
Personas	- Falta de capacitación en ciberseguridad industrial. - Dependencia de prácticas heredadas y rutinarias. - Bajo nivel de conciencia sobre la separación entre redes IT y OT.
Procesos	- Ausencia de protocolos claros para actualización y respaldo. - Falta de políticas de control de acceso y auditorías periódicas. - Inexistencia de planes formales de respuesta ante incidentes.
Tecnología	- Equipos y PLC antiguos sin soporte del fabricante. - Redes planas sin segmentación ni VLAN. - Ausencia de DMZ industrial o cortafuegos dedicados.
Gestión / Política	- Falta de alineación con estándares como ISA/IEC 62443. - Presupuesto limitado para proyectos de seguridad. - Descoordinación entre las áreas IT y OT.
Entorno / Proveedores	- Uso de software o servicios externos sin control de seguridad. - Integraciones con terceros sin monitoreo ni acuerdos de protección adecuados.

Fuente: Elaboración propia.

1.2 IMPORTANCIA DE RESOLVERLO

En los últimos años han aumentado los casos de ataques a industrias debido a la cantidad de vulnerabilidades que presentan estos sistemas y la cantidad de protocolos que fueron creados hace décadas cuando la ciberseguridad no era una prioridad, esto puede traer por consecuencia no solamente que el proceso se detenga y por ende haya una pérdida económica considerable sino que también pueden poner en riesgo la vida de las personas, ya que los sistemas OT como los que controlan plantas eléctricas, refinerías, fábricas, trenes, plantas de agua o PLCs industriales, tienen funciones críticas y fundamentales como controlar variables como la temperatura, válvulas, motores, presión, etc. Por lo que, si un atacante logra detener o alterar estos procesos las consecuencias y el impacto no es solo digital sino también físico. La figura 1-1 muestra los principales protocolos y servicios de sistemas de control industrial (ICS) observados globalmente.

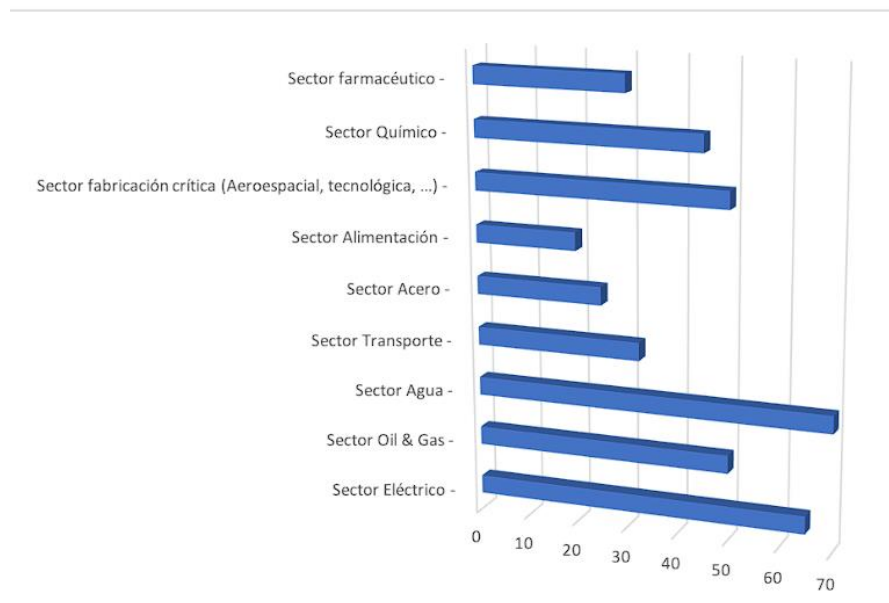


Fuente: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

Figura 1-1 Protocolos y servicios de sistemas de control industrial (ICS) observados a nivel mundial.

1.2.1 Estado de la ciberseguridad OT en Chile

El CCI (Centro de Ciberseguridad Industrial) indica que en Chile hay un aumento por el interés en mejorar la ciberseguridad en OT debido a la cantidad de ataques y la necesidad de proteger la infraestructura, sin embargo, esto aún se encuentra en etapas iniciales con muchos desafíos técnicos y normativos por delante. En la Figura 1-2 se muestra el nivel de sensibilidad de las organizaciones industriales en Chile, clasificado por sectores productivos según el Centro de Ciberseguridad Industrial (CCI-ES). Se observa que los sectores Eléctrico, Oil & Gas y Agua presentan los niveles más altos de sensibilidad, debido a que una interrupción o ataque en estos sistemas podría generar un impacto crítico en la infraestructura nacional.



Fuente: <https://www.cci-es.org/maps/chile/>

Figura 1-2 Nivel de sensibilidad de las organizaciones industriales.

1.3 INVOLUCRADOS PRINCIPALES

Los principales afectados de ataques cibernéticos en OT lógicamente son las industrias dentro de estas la principal área es la de operaciones es la que más impacto recibe porque suele alterar los procesos de producción y dañar los PLC, también el área de TI ya que, aunque un ataque se origine en OT, la convergencia TI/OT provoca que los servidores, redes corporativas y estaciones de trabajo también se vean comprometidas, así como también las personas debido a alteraciones físicas en los procesos, se recalca también la pérdida económica que se origina para la empresa afectada, el resumen de los afectados se muestra en la tabla 1-2.

Tabla 1-2 Resumen principales afectados.

Nivel interno afectado	Daño causado	Ejemplo
Producción (OT)	Daño a PLCs o maquinaria	Ransomware o sabotaje a HMI
Tecnología (IT)	Robo de datos	Fallo de Firewall
Personas	Riesgos Físicos	Cambios forzados de parámetros o variables
Administradores	Daños económicos severos	Tiempo de inactividad del proceso

Fuente: Elaboración propia.

1.3.1 Sectores más afectados en Chile

Según el reporte minero, portal de noticias del rubro en Chile las industrias más afectadas han sido energía, manufactura, minería y logística, intrusiones en OT subieron hasta un 73%, con 31 % de las empresas sufriendo más de seis ataques en 12 meses, según Redicom empresa que se dedica a brindar servicios de ciberseguridad en nuestro país, las principales amenazas que se presentan en los sistemas SCADA son los malwares específicos para estos sistemas y las puertas traseras en redes convergentes IT/OT.

1.4 SOLUCIÓN DEL PROBLEMA

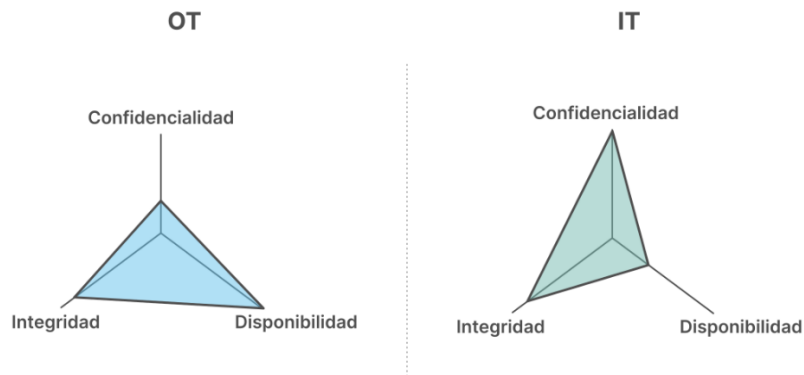
Para solucionar el problema de la falta de ciberseguridad en sistemas SCADA se propondrá un diseño de una arquitectura de red considerando las recomendaciones de la norma ISA/IEC 62443. Esto se traduce en segmentación de las redes IT y OT, este diseño busca proteger todos los dispositivos que giran en torno a una industria como los controladores y HMI como los servidores de supervisión que se usan en estos sistemas, evitando accesos no autorizados y garantizando la continuidad operativa.

1.5 REQUERIMIENTOS

Para solucionar el problema que hay con la falta de seguridad y segmentación en el sistema SCADA, es necesario diseñar una red más segura que separe bien los diferentes niveles de la red. Con esto se busca evitar fallas o accesos no autorizados, mantener la red operativa sin interrupciones y proteger los equipos de control que forman parte del sistema.

1.5.1 Segmentación de redes IT/OT

Separar la red administrativa (IT) de la red operativa (OT) mediante la implementación de VLAN y firewalls industriales evitando que incidentes inesperados de la red corporativa afecten también a la red operativa, ya que la disponibilidad es lo más importante en la industria. En la figura 1-3 se muestra una representación visual de las diferencias de prioridades.

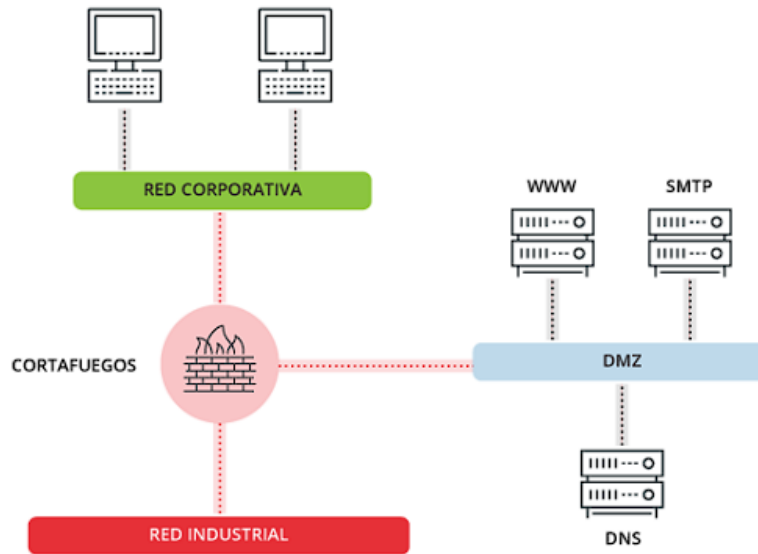


Fuente: <https://juancarlosaavedra.net/2023/08/redes-it-y-redes-ot-juntas-o-separadas/>

Figura 1-3 Prioridades del Triángulo de Seguridad CIA en Tecnologías IT y OT

1.5.2 Creación de una zona desmilitarizada (DMZ)

En redes industriales una DMZ funciona como un intermediario entre la red IT y la OT, sirve para separar y controlar la interacción entre ambas redes, de esta forma los usuarios no pueden entrar a un dispositivo de la zona OT. En la Figura 1-4 se observa la separación de redes corporativa e industrial a través de una DMZ y un cortafuegos.



Fuente: <https://www.incibe.es/incibe-cert/blog/diferencias-dmz-y-dmz-ti>

Figura 1-4 Segmentación IT/OT mediante cortafuegos y zona desmilitarizada.

1.5.3 Permisos de control de acceso

Definir niveles de permisos para diferentes tipos de usuarios (administradores, operadores, mantenimiento) a través de autenticación y contraseñas.

1.6 ALTERNATIVAS DE SOLUCIÓN

Con el objetivo de resolver los problemas de seguridad en un sistema SCADA se evaluarán tres alternativas a considerar para mejorar la protección de red y asegurar un funcionamiento correcto del sistema.

1.6.1 Alternativa 1: Aislar la red industrial

Esta alternativa consiste en mantener la red industrial completamente aislada, sin ningún tipo de conectividad con la red corporativa. Si bien es la opción que ofrece el mayor nivel de seguridad al evitar accesos externos, no aporta innovación tecnológica ni permite integrar servicios modernos de supervisión o mantenimiento remoto, dejando el sistema totalmente desconectado de tecnologías clave.

Ventajas:

- Minimiza los riesgos de ciberataques al eliminar puntos de acceso externos.
- Garantiza mayor estabilidad y control sobre los procesos industriales.

Desventajas:

- No permite comunicación ni intercambio de datos con la red corporativa.
- Dificulta la supervisión remota y la integración con nuevas tecnologías.
- Requiere intervención manual para mantenimiento o actualizaciones.
- Limita la escalabilidad y el crecimiento del sistema a futuro.

1.6.2 Alternativa 2: Mejorar la red

En esta alternativa se toma como opción reforzar la seguridad de la red mediante medidas básicas como un firewall sencillo, contraseñas seguras, antivirus actualizados.

Ventajas:

- Costo moderado comparado con un rediseño de la red
- Mejora algunos aspectos de seguridad básica
- Puede implementarse con muy pocos cambios en la infraestructura del sistema SCADA

Desventajas:

- No separa la red IT de la OT.
- La seguridad sigue siendo limitada.
- No cumple con normas internacionales como ISA/IEC 62443
- Mantiene cierto riesgo de accesos no autorizados.

1.6.3 Alternativa 3: Rediseñar la Red

Rediseñar la red del sistema SCADA creando una red segmentada que divida claramente la parte IT y la OT, usando VLAN, firewalls y una zona DMZ como intermediaria y aplicando las normas de seguridad ISA/IEC 62443 para sistemas industriales.

Ventajas:

- Ofrece la solución más robusta y moderna.
- Cumple con estándares internacionales de ciberseguridad.
- Mejora la disponibilidad, integridad y confidencialidad del sistema.

- Permite estar más seguro y ahorrar costos por ataques que dejen inoperativo el sistema SCADA

Desventajas:

- Requiere más tiempo de diseño y configuración.
- Mayor costo de implementación inicial.
- Necesita personal con conocimientos técnicos en redes y seguridad.

1.6.4 Evaluación de la solución

Para evaluar las alternativas de solución, se elabora una tabla para clasificar cada una de las alternativas (Tabla 1-4), se toma como base la escala de competencias genérica. (Tabla 1-3).

Tabla 1-3 Calificación para la selección de alternativas.

Muy deficiente	Deficiente	Aceptable	Bueno	Óptimo
1	2	3	4	5

Fuente: Elaboración propia con Excel.

Tabla 1-4 Calificación de alternativas.

	Aislar la red industrial	Mejorar la red	Rediseñar la red
Innovación	1	2	5
Costos	2	4	1
Consumo	4	4	3
Seguridad	5	3	5
Escalabilidad	1	2	5
Total:	13	15	19

Fuente: Elaboración propia en base a alternativas.

1.6.5 Elección de la solución

Después de analizar la tabla 1-4, la Alternativa 3 es la más conveniente, ya que ofrece una solución más completa y segura para el sistema. Además, es la opción más actualizada tecnológicamente, lo que permite tener una red moderna y preparada para futuros cambios o mejoras.

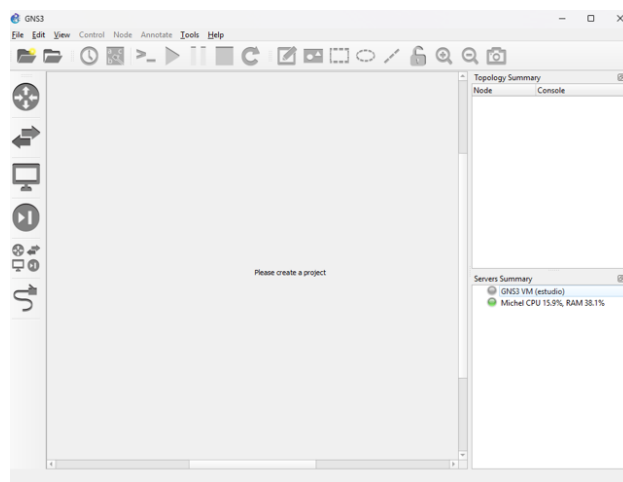
Aunque requiere una mayor inversión inicial y un trabajo más exhaustivo en su diseño e implementación, vale la pena a largo plazo. Esta alternativa mejora la infraestructura de red, protege eficazmente los equipos y sigue las buenas prácticas de seguridad industrial. Asimismo, es la opción que mayores ahorros puede generar, puesto que, mientras menos se detenga el proceso, mejores serán las ganancias obtenidas.

1.6.6 Herramientas tecnológicas de la solución seleccionada

A continuación, se presentan las herramientas de software fundamentales que se utilizarán para el desarrollo, simulación y validación de la alternativa tecnológica elegida:

1.6.6.1 GNS3

GNS3 (Graphical Network Simulator 3) es un simulador y emulador de redes de forma virtual usando distintos equipos de red como routers, switches, PCs entre otros sin la necesidad de tenerlos, con él se puede probar cómo funciona una red real y ver cómo se comunican los dispositivos, en la figura 1-5 se puede observar la interfaz de este programa.



Fuente: Elaboración propia.

Figura 1-5 Interfaz GNS3.

1.6.6.2 Kali Linux

Kali Linux es una distribución de código abierto basada en Debian, diseñada específicamente para la auditoría de seguridad, el análisis de redes y las pruebas de penetración.



Fuente: Elaboración propia.

Figura 1-6 Interfaz Kali Linux.

1.6.6.3 VMware

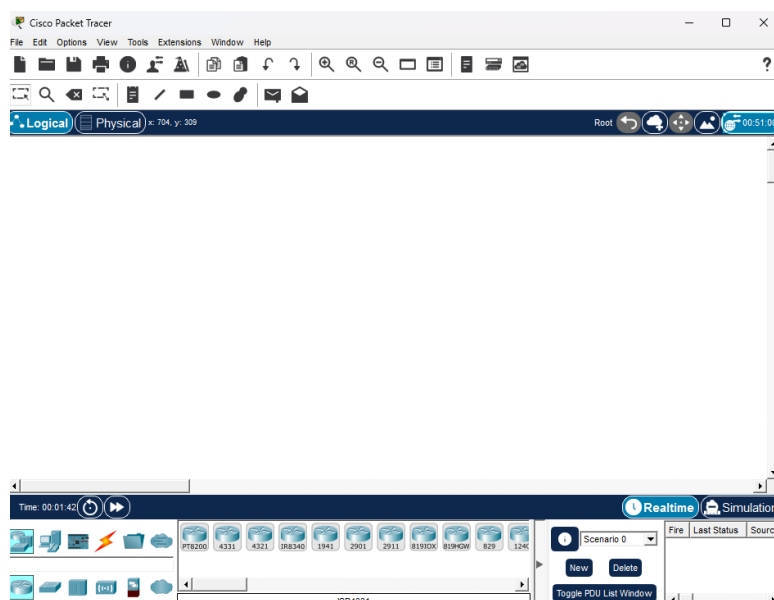
VMware es un programa que sirve para crear máquinas virtuales, o sea, instalar y usar varios sistemas operativos dentro de un mismo computador.

1.6.6.4 pfSense

pfSense es un sistema operativo gratuito basado en FreeBSD que funciona como un firewall y router, utilizado para proteger y controlar el tráfico entre diferentes redes.

1.6.6.5 Packet Tracer

Packet Tracer es un simulador de redes que permite crear topologías y hacer configuraciones de equipos Cisco.



Fuente: Elaboración propia.

Figura 1-7 Interfaz Packet Tracer.

1.7 OBJETIVOS

En este punto se exhibe tanto el objetivo general como los objetivos específicos para tener en cuenta para desarrollar en los capítulos posteriores.

1.7.1 Objetivo general

Diseñar una arquitectura de red segura para un sistema SCADA, que permita separar las redes IT y OT, aplicando buenas prácticas de ciberseguridad basadas en la norma ISA/IEC 62443.

1.7.2 Objetivos específicos

- Analizar el estado actual de la red y los principales riesgos de seguridad en el entorno SCADA.
- Proponer una topología de red segmentada entre las áreas IT y OT, incorporando una zona DMZ.
- Implementar medidas de defensa en profundidad mediante firewalls, VLAN y políticas de acceso.
- Simular el diseño de red en GNS3 para validar la conectividad y la separación entre las zonas.
- Elaborar documentación técnica con los resultados, beneficios y mejoras logradas con el diseño propuesto.
- Realizar un análisis de costos y factibilidad económica del diseño de red propuesto,
- considerando los recursos técnicos necesarios.

CAPÍTULO 2: DESARROLLO DE LA SOLUCIÓN

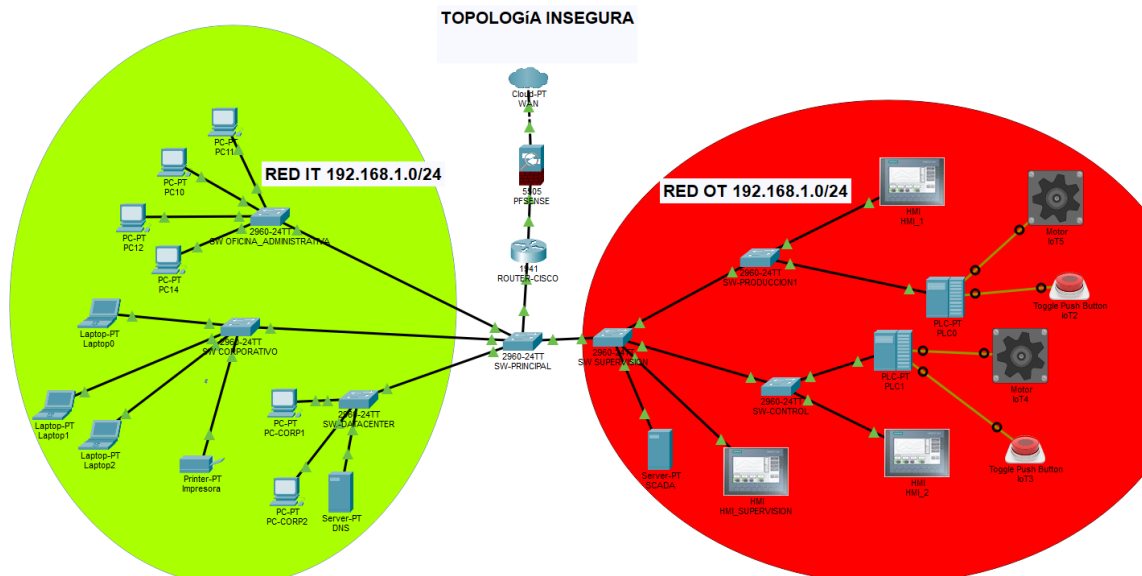
2 DESARROLLO DE LA SOLUCIÓN

En este capítulo se detalla el proceso de diseño y arquitectura de una red segura para sistemas SCADA, siguiendo las normas de la serie ISA/IEC 62443. Se abordará desde el rediseño de una red sin segmentación, mostrando sus vulnerabilidades, hasta la propuesta de una arquitectura segura con separación entre las áreas IT y OT. Además, se describirán los equipos utilizados, las configuraciones aplicadas y la implementación final realizada en el entorno de simulación GNS3.

2.1 SEPARACIÓN DE LA RED IT DE LA OT

La segmentación de redes consiste en dividir una red en distintas zonas o subredes con el objetivo de mejorar la seguridad, el control y el rendimiento. En entornos industriales, este proceso implica separar la red IT (Tecnologías de la Información) de la red OT (Tecnologías Operacionales), estableciendo límites de comunicación y políticas específicas entre ambas para prevenir accesos no autorizados y proteger los sistemas de control industrial.

Una red no segmentada mantiene el área IT y el área OT dentro del mismo rango de red, sin la presencia de un firewall ni políticas que las separen. Esta falta de aislamiento genera un alto nivel de inseguridad en ambas áreas, especialmente en la red industrial, que puede verse expuesta a amenazas provenientes del entorno corporativo. En la Figura 2-1 se muestra un ejemplo de una red sin segmentación, donde ambas áreas operan dentro de la misma infraestructura.



Fuente: Elaboración propia con Packet Tracer.

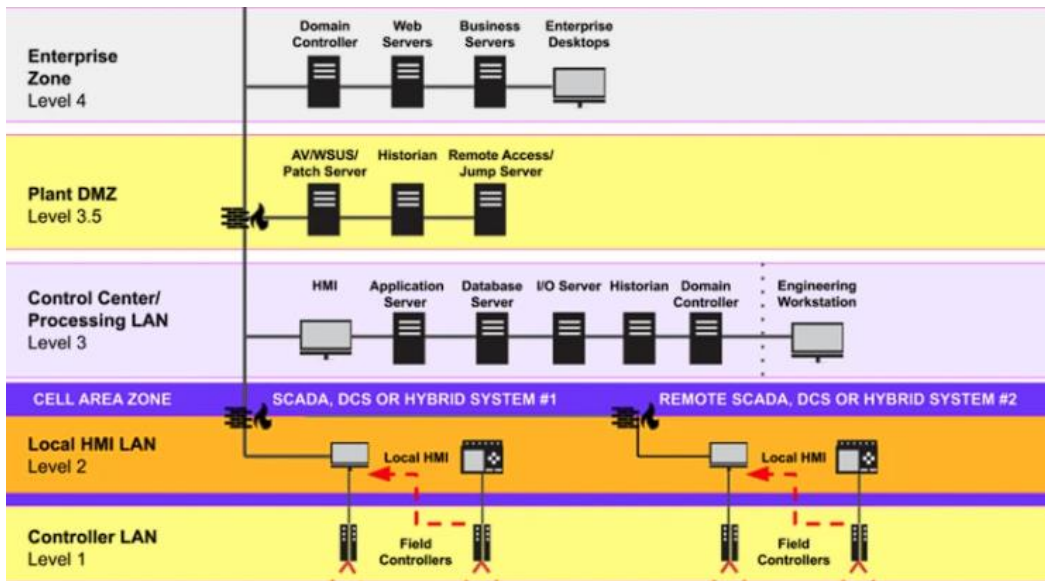
Figura 2-1 Red sin segmentación.

En la topología anterior se observa que el área verde corresponde a la red IT, mientras que el área roja representa la red OT. Ambas operan bajo el mismo rango de red 192.168.1.0/24 y no cuentan con un firewall que controle o restrinja los accesos entre ellas. Además, no se evidencian VLAN configuradas para separar las distintas subáreas, lo que refleja una ausencia total de segmentación y control en la infraestructura.

2.1.1 Arquitectura de referencia industrial

Como referencia para la organización de la arquitectura industrial, se considera el Modelo Purdue mostrado en la figura 2-2 ampliamente utilizado en entornos de Sistemas de Control Industrial (ICS) para estructurar la separación entre los niveles de operación, supervisión y gestión empresarial. Si bien el presente proyecto no implementa todos los niveles definidos por este modelo debido al alcance de la simulación, el diseño desarrollado mantiene la separación funcional entre las redes IT y OT mediante VLAN, zonas DMZ y un firewall central. Asimismo,

incorpora principios de ciberseguridad establecidos en la norma ISA/IEC 62443, tales como la segmentación por zonas, la defensa en profundidad y el control de acceso entre los distintos dominios de la red.

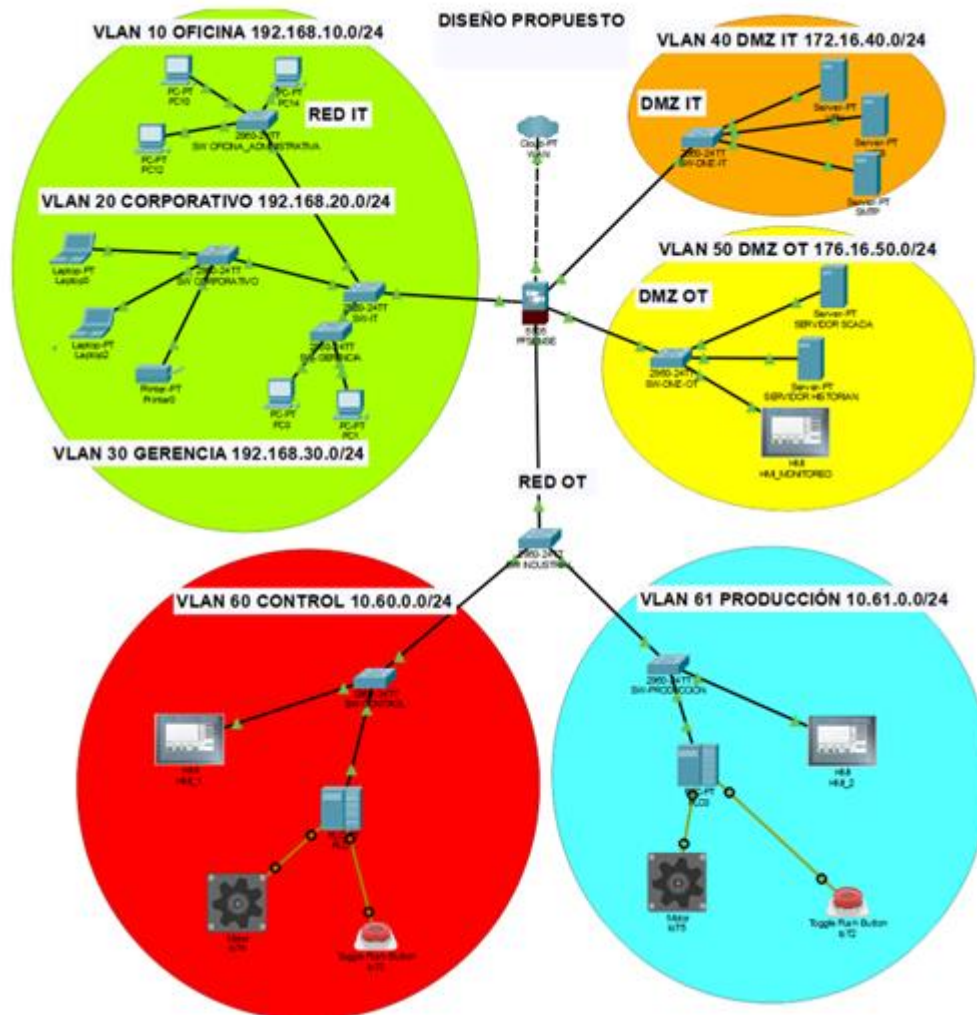


fuelle: <https://claroty.com/blog/ics-security-the-purdue-model>

Figura 2-2 Modelo Purdue.

2.1.2 Rediseño de red

En base a lo anterior, se propone la siguiente topología de red segmentada, diseñada para separar y proteger cada zona de la organización mediante VLAN y un firewall central (ver figura 2-3).



Fuente: Elaboración propia con Packet Tracer.

Figura 2-3 Rediseño de la red con segmentación.

Como se ve en la figura 2-3, la topología propuesta segmenta la red en distintas áreas según su función: la red IT agrupa las VLAN 10, 20 y 30 correspondientes a Oficina, Finanzas y Gerencia; la DMZ IT (VLAN 40) aloja los servidores web, VPN y correo; la DMZ OT (VLAN 50) resguarda los sistemas SCADA, Historian y HMI de monitoreo; y finalmente, la red OT se divide en las VLAN 60 y 61 destinadas al control y la producción industrial.

En esta nueva arquitectura se elimina el router tradicional, ya que el firewall pfSense asume también el rol de enrutador principal, gestionando el tráfico entre las distintas subredes y controlando los accesos mediante reglas de seguridad.

Esta estructura permite aislar cada zona, mejorar la seguridad y mantener un flujo de comunicación controlado a través del firewall central pfSense, garantizando así una arquitectura más ordenada y protegida. De esta forma, se cumplen las recomendaciones establecidas por la norma ISA/IEC 62443 para el diseño de redes industriales seguras.

2.2 DISPOSITIVOS

A continuación, se presentan los distintos dispositivos necesarios para simular la topología de red. Es importante mencionar que, aunque estos equipos se utilizarán de manera virtual dentro del simulador GNS3, existen también en su forma física real y se configuran bajo los mismos parámetros, permitiendo una representación fiel del entorno industrial y corporativo que se busca implementar.

2.2.1 Switch Cisco Catalyst 1300

Un switch es un dispositivo que conecta distintos equipos dentro de una red local. En este proyecto se utiliza el modelo Cisco IOSvL2, equivalente al switch Cisco Catalyst 1300 que se observa en la figura 2-4, como conmutador principal para cada área, permitiendo crear VLAN y ordenar el tráfico interno antes de llegar al firewall.

En GNS3, este modelo será representado por un Cisco 2691 con el módulo NM-16ESW, el cual ofrece la compatibilidad necesaria para simular funciones de switching y segmentación.



Fuente: <https://www.tonitrus.com/C1300-24T-4G> 15

Figura 2-4 Switch Cisco 1300.

Este dispositivo se representa en GNS3 con la figura 2-5.



Fuente: Captura de pantalla propia de GNS3.

Figura 2-5 Switch 1300 en GNS3.

2.2.2 Firewall

Un firewall o cortafuegos (figura 2-6), es un sistema de seguridad que gestiona el tráfico que entra y sale de una red. Su función es actuar como una barrera entre una red interna, conocida y confiable, y otra que no lo es, como por ejemplo Internet. De esta forma, ayuda a proteger los sistemas frente a accesos no autorizados y posibles amenazas externas. Puede ser un dispositivo físico o un software. En esta ocasión se utilizará pfSense que es una solución basada en software que cumple la función de firewall principal para proteger y controlar la comunicación entre las

distintas áreas de la red, también funciona como router permitiendo conectar redes distintas entre sí.



Fuente: Captura de pantalla propia de GNS3.

Figura 2-6 pfSense en GNS3.

2.2.3 Computador

Un PC (figura 2-7) es un dispositivo de cómputo de uso general, diseñado para que una persona pueda ejecutar aplicaciones, acceder a servicios, procesar información y realizar tareas administrativas u operativas se considera un equipo de usuario.



Fuente: Captura de pantalla propia de GNS3.

Figura 2-7 PC en GNS3.

2.2.4 HMI

HMI (figura 2-8) es un hardware y software que permite al operador observar, supervisar y controlar un proceso industrial, mostrando la información mediante la pantalla. La HMI muestra los datos en dicho control en tiempo real, alarmas o bien los estados de los equipos, permitiendo la interacción directa entre el usuario y las máquinas (PLC, sensores, actuadores).



Fuente: Captura de pantalla propia de GNS3.

Figura 2-8 HMI en GNS3.

2.2.5 PLC

El PLC (figura 2-9) es un elemento fundamental en las industrias. ya que cumple la función de controlar y automatizar procesos.



Fuente: Captura de pantalla propia de GNS3.

Figura 2-9 PLC en GNS3.

2.2.6 Servidores

Un servidor (figura 2-10) es un equipo encargado de ofrecer servicios y recursos a otros dispositivos dentro de la red. En esta topología, los servidores cumplen funciones críticas como autenticación, historización, correo, web y acceso remoto, pero el más relevante es el servidor SCADA, que centraliza la supervisión y control de los procesos industriales, recibe los datos enviados por los PLC desde las VLAN OT y permite monitorear en tiempo real el estado de la planta. Su correcto aislamiento y protección son esenciales para garantizar la continuidad operativa y la ciberseguridad del sistema.



Fuente: Captura de pantalla propia de GNS3.

Figura 2-10 Servidor en GNS3.

2.2.7 Cloud

El nodo Cloud (ver figura 2-11) que proporciona GNS3 define la conexión de la propia topología simulada y con la red física del equipo host que albergue la ejecución de este emulador. En este sentido, se utiliza para establecer el punto de conexión que le da carácter real a la conexión de la red virtual donde los dispositivos tales como el firewall y los routers desarrollados en GNS3 tienen acceso a servicios externos. En este caso, el Cloud va a permitir simular la interfaz WAN, actuando, así como el punto de encuentro allí donde la red de la que estamos hablando se conecta a un proveedor de servicios de Internet (ISP).



Fuente: Captura de pantalla propia de GNS3.

Figura 2-11 Cloud en GNS3.

2.3 CONEXIONADO

En GNS3 el conexionado se realiza de manera automática, ya que la plataforma selecciona el tipo de cable adecuado según el tipo de interfaz conectada (directo, cruzado o consola), replicando el funcionamiento de AUTO-MDIX presente en equipos modernos. En la mayor parte de la topología se utilizan enlaces Ethernet equivalentes a cables directos, mientras que la conexión entre pfSense y el nodo Cloud representa el enlace WAN hacia el proveedor de Internet; aunque en la simulación se utiliza un conector Ethernet, en un entorno real correspondería a un enlace óptico que llega primero al ONT del ISP y luego se entrega al firewall mediante un puerto RJ45, las interfaces utilizadas para esta topología se muestran en la tabla 2-1.

Tabla 2-1 Conexionado de interfaces.

Nodo	Interfaz	Conectado a	Interfaz Remota
pfSense	em0	WAN	eth0
pfSense	em1	SW-IT	Fa1/0
pfSense	em2	SW-OT	Fa1/0
pfSense	em3	SW-DMZ-OT	Fa1/0
pfSense	em4	SW-DMZ-IT	Fa1/0
SW-IT	Fa1/0	pfSense	em1
SW-IT	Fa1/1	SW-OFICINA/SW-CORPORATIVO/SW-GERENCIA	Fa1/0
SW-OFICINA	Fa1/0	SW-IT	Fa1/1
SW-OFICINA	Fa1/1	PC1 / PC2	Eth0
SW-CORPORATIVO	Fa1/0	SW-IT	Fa1/2
SW-CORPORATIVO	Fa1/1	PC3 / PC4	Eth0
SW-GERENCIA	Fa1/0	SW-IT	Fa1/3
SW-GERENCIA	Fa1/1	PC5 / PC6	Eth0
SW-OT	Fa1/0	pfSense	em2
SW-OT	Fa1/1	SW-CONTROL/SW-PRODUCCION	Fa1/0
SW-CONTROL	Fa1/0	SW-OT	Fa1/1
SW-CONTROL	Fa1/1	PLC-PRODUCCIÓN / HMI-PRODUCCION	Eth0
SW-PRODUCCIÓN	Fa1/0	SW-OT	Fa1/2
SW-PRODUCCIÓN	Fa1/1	PLC-CONTROL / HMI-CONTROL	Eth0
SW-DMZ-IT	Fa1/0	pfSense	em4
SW-DMZ-IT	Fa1/1	SERVIDOR-SMTP / SERVER-WEB / SERVER-VPN	Eth0
SW-DMZ-OT	Fa1/0	pfSense	em3
SW-DMZ-OT	Fa1/1	SERVIDOR-HISTORIAN / SERVIDOR-SCADA / HMI-MONITOREO	Eth0

Fuente: Elaboración propia con Excel.

Como se muestra en la tabla 2-1, se emplean puertos FastEthernet los cuales ofrecen una velocidad de entre 10Mbps y 100Mbps para enlazar los switches, ya que el modelo utilizado en la simulación no dispone de puertos Gigabit. Aunque en un entorno real los enlaces Gigabit ofrecen velocidades muy superiores de 1000 Mbps, dentro de GNS3 este switch solo permite trabajar con FastEthernet.

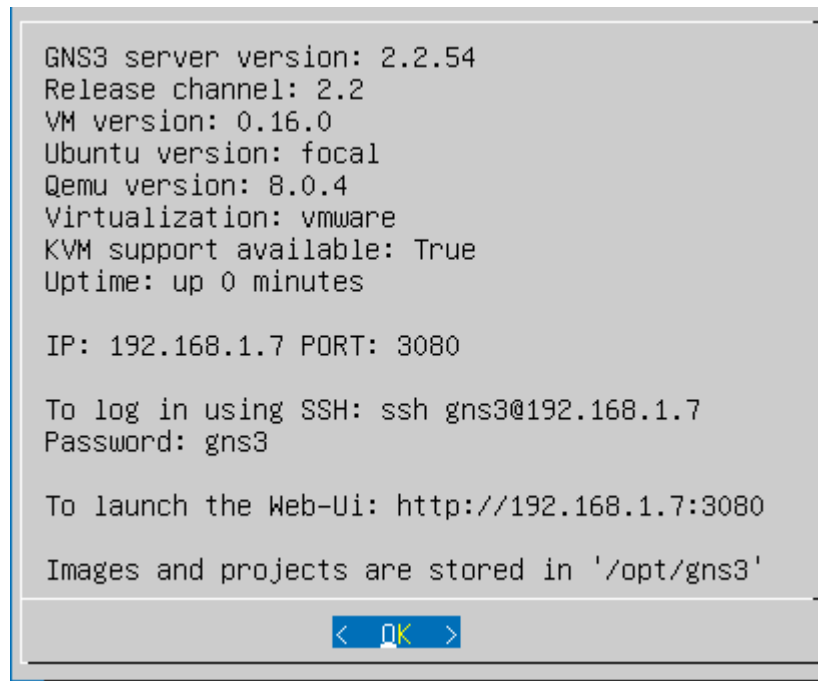
2.4 CONFIGURACIÓN

En este apartado se realizará la configuración de la topología, así como las configuraciones que necesita GNS3 para emular de manera correcta la red.

2.4.1 Máquina virtual de GNS3

La máquina virtual de GNS3 es un sistema operativo basado en Linux encargado de ejecutar los dispositivos virtuales más complejos de la simulación, como pfSense y los switches IOSvL2. Esta máquina virtual proporciona un entorno optimizado con soporte para QEMU/KVM, que son necesarios ya que QEMU es un software de virtualización que permite emular hardware completo y KVM viene integrada en el kernel de Linux y convierte a Linux en un hipervisor, haciendo que se ejecute más rápido todo el entorno y los dispositivos emulados, en la figura 2-12 se pueden observar los parámetros de esta máquina virtual.

Adicionalmente, la arquitectura de esta máquina virtual permite una gestión eficiente de los recursos del host, delegando la carga computacional intensiva de la emulación hacia el hipervisor. Esta separación entre la interfaz gráfica de usuario (GUI) y el motor de ejecución no solo mejora la estabilidad del sistema, sino que también facilita la escalabilidad de topologías de red complejas al aprovechar al máximo la capacidad de procesamiento del hardware subyacente.

A screenshot of a terminal window from a GNS3 virtual machine. The terminal displays the following text: GNS3 server version: 2.2.54, Release channel: 2.2, VM version: 0.16.0, Ubuntu version: focal, Qemu version: 8.0.4, Virtualization: vmware, KVM support available: True, Uptime: up 0 minutes. Below this, it shows IP: 192.168.1.7 PORT: 3080. Then, it provides instructions: 'To log in using SSH: ssh gns3@192.168.1.7' and 'Password: gns3'. Next, it says 'To launch the Web-Ui: http://192.168.1.7:3080'. Finally, it states 'Images and projects are stored in '/opt/gns3''. At the bottom of the terminal window, there is a blue button with the text '< OK >'.

```
GNS3 server version: 2.2.54
Release channel: 2.2
VM version: 0.16.0
Ubuntu version: focal
Qemu version: 8.0.4
Virtualization: vmware
KVM support available: True
Uptime: up 0 minutes

IP: 192.168.1.7 PORT: 3080

To log in using SSH: ssh gns3@192.168.1.7
Password: gns3

To launch the Web-Ui: http://192.168.1.7:3080

Images and projects are stored in '/opt/gns3'
```

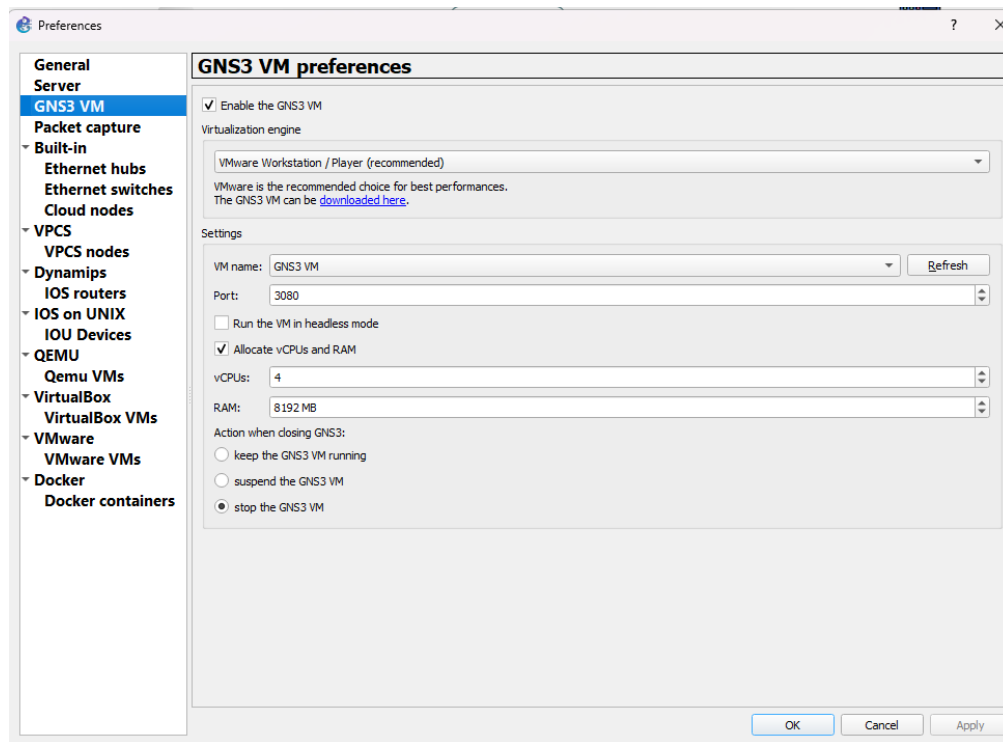
Fuente: Captura de pantalla propia de VM de GNS3.

Figura 2-12 Parámetros VM GNS3.

En la figura 2-12 se puede observar que la máquina virtual de GNS3 se encuentra operativa bajo VMware, con aceleración KVM habilitada y con una IP real de la red local (192.168.1.7), lo que permite ejecutar correctamente los dispositivos virtuales del proyecto, también cuenta con SSH (Secure Shell) para acceso remoto con sus credenciales y para comunicarse con GNS3 se utiliza el puerto TCP 3080 en esta ocasión.

2.4.1.1 Enlace de máquina virtual con GNS3

Para enlazar la máquina se debe ir a configuración en GNS3 y en la sección “GNS3 VM” podemos ajustar los parámetros como el puerto TCP y la cantidad de memoria de la máquina virtual (ver figura 2-13).



Fuente: Captura de pantalla propia de GNS3.

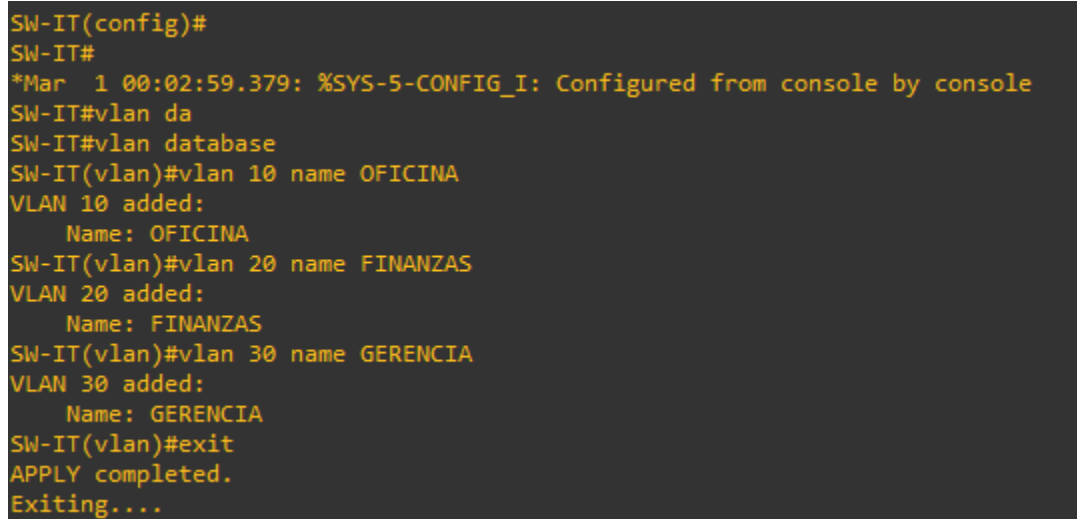
Figura 2-13 Configuración VM en GNS3.

2.4.2 VLAN

Una VLAN es una red local virtual que permite segmentar y aislar diferentes áreas de una red (como IT, DMZ y OT) con el fin de mejorar la seguridad, controlar el tráfico entre zonas y reducir el riesgo de accesos no autorizados dentro de la infraestructura, se procederán a crear y configurar a nivel de capa 2, esto quiero decir a nivel de red de área local para luego más adelante en pfSense configurarlas en capa 3.

2.4.2.1 Creación de VLAN

La configuración de las VLAN en los switches (que en este caso corresponden a un Router Cisco 2691 emulando un switch con el módulo NM-16ESW) difiere del método usado en un switch Cisco Catalyst 1300. Sin embargo, la lógica y funcionalidad es la misma (ver figura 2-14).



```
SW-IT(config)#
SW-IT#
*Mar  1 00:02:59.379: %SYS-5-CONFIG_I: Configured from console by console
SW-IT#vlan da
SW-IT#vlan database
SW-IT(vlan)#vlan 10 name OFICINA
VLAN 10 added:
    Name: OFICINA
SW-IT(vlan)#vlan 20 name FINANZAS
VLAN 20 added:
    Name: FINANZAS
SW-IT(vlan)#vlan 30 name GERENCIA
VLAN 30 added:
    Name: GERENCIA
SW-IT(vlan)#exit
APPLY completed.
Exiting....
```

Fuente: Captura de pantalla del terminal del GNS3.

Figura 2-14 Creación de VLAN en Switch-IT.

2.4.2.2 Enlace troncal

Una vez creadas las VLANs, se procede a configurar el enlace troncal (trunk) entre el SW-IT y pfSense. Esto permite transmitir el tráfico de múltiples VLANs (mediante el etiquetado de tramas IEEE 802.1Q) a través de un único enlace físico, delegando en pfSense la función de Gateway para el enrutamiento inter-VLAN.

```

SW-IT(config)#interface fa1/0
SW-IT(config-if)#sw
SW-IT(config-if)#switchport tr
SW-IT(config-if)#switchport trunk al
SW-IT(config-if)#switchport trunk allowed vlan 1,10,20,30,1002-1005
SW-IT(config-if)#end
SW-IT#cop
*Mar  1 01:48:04.339: %SYS-5-CONFIG_I: Configured from console by console
SW-IT#copy r
SW-IT#copy run
SW-IT#copy running-config s
SW-IT#copy running-config star
SW-IT#copy running-config startup-config
Destination filename [startup-config]?

```

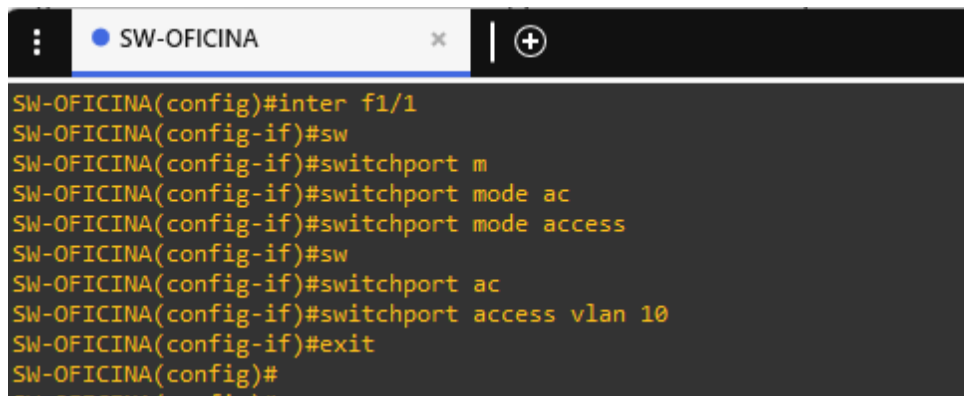
Fuente: Captura de pantalla del terminal del GNS3.

Figura 2-15 Configuración de enlace troncal en Switch-IT.

El módulo NM-16ESW requiere que la lista de VLAN permitidas en el trunk incluya explícitamente la VLAN 1 y las VLAN de sistema/control (1002-1005) por esa razón se agregan en la configuración, en los switches de cada subárea (oficina, corporativo, etc.)

2.4.2.3 Modo acceso

A diferencia de los enlaces troncales, las interfaces conectadas a los dispositivos finales se deben configurar en modo acceso. De esta manera, el puerto queda asociado a una única VLAN y transmite las tramas de datos sin etiquetar hacia los equipos de usuario (ver figura 2-16).



```
SW-OFICINA(config)#inter f1/1
SW-OFICINA(config-if)#sw
SW-OFICINA(config-if)#switchport mode access
SW-OFICINA(config-if)#exit
SW-OFICINA(config)#
```

Fuente: Captura de pantalla terminal del GNS3.

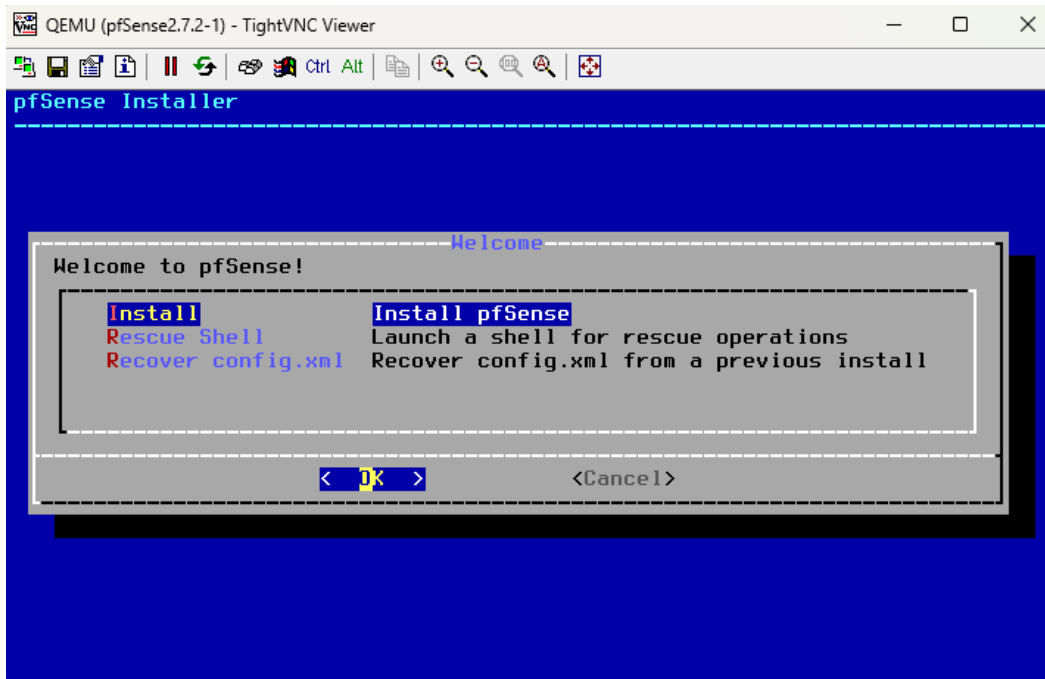
Figura 2-16 Configuración de acceso.

2.4.3 Instalación y configuración del firewall

El firewall será la principal fuente de seguridad de la arquitectura de red, como se mencionó anteriormente se utilizará pfSense que es un firewall por software basado en un sistema operativo.

2.4.3.1 Instalación pfSense

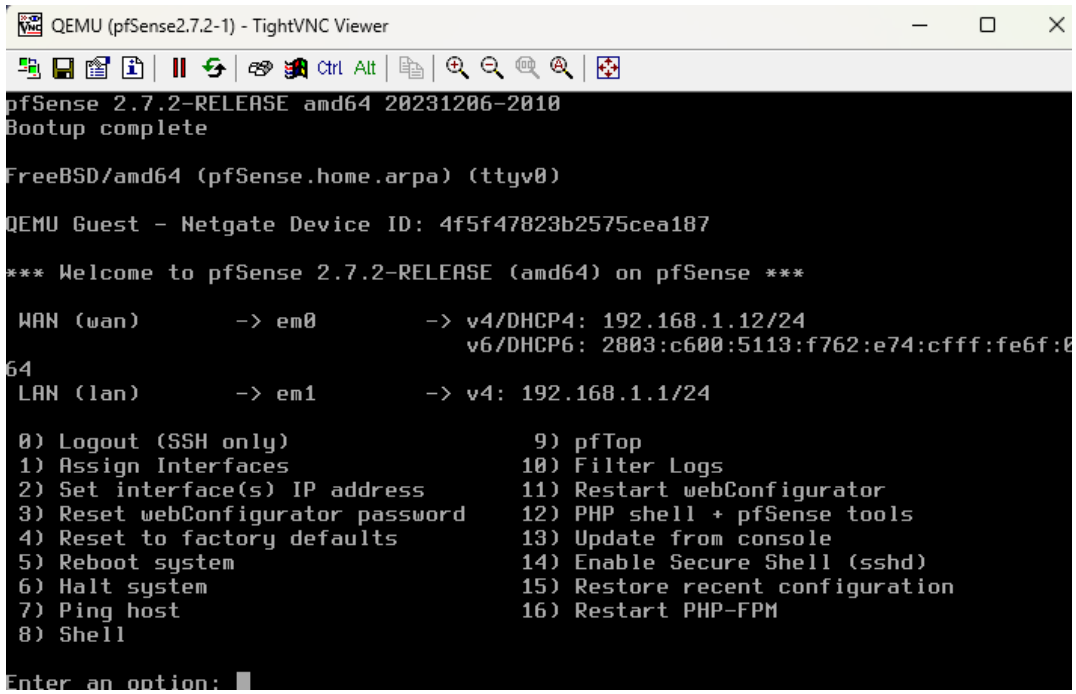
pfSense se instala de manera muy similar a un sistema operativo tradicional ya que se basa en FreeBSD. La principal diferencia es que pfSense está optimizado exclusivamente para funcionar como Firewall/Router (Gateway), por lo que el proceso es rápido y la configuración se centra inmediatamente en las interfaces de red (WAN/LAN). En la figura 2-17 se puede observar el cliente de instalación.



Fuente: Captura de pantalla pfSense.

Figura 2-17 instalador pfSense.

Una vez instalado se podrá ver la consola de configuración de pfSense (ver figura 2-18) la cual asigna automáticamente la WAN en la interfaz em0 y la LAN con la interfaz em1 con la IP por defecto 192.168.1.1. Sin embargo, la topología propuesta requiere que em1 sea la interfaz que maneje las VLAN para la Red IT (10, 20, 30), y que también use las interfaces em2, em3, y em4 para las otras zonas (OT y DMZ).



```

QEMU (pfSense2.7.2-1) - TightVNC Viewer
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
QEMU Guest - Netgate Device ID: 4f5f47823b2575cea187

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.12/24
                v6/DHCP6: 2803:c600:5113:f762:e74:cfff:fe6f:0
64
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option:

```

Fuente: Captura de pantalla terminal pfSense.

Figura 2-18 Consola pfSense.

2.4.3.2 Configuración pfSense

Para iniciar la configuración de VLAN en capa 3, se deben asignar los puertos correspondientes. En este caso, em1 se configura como LAN por defecto y em0 como WAN. Las interfaces restantes (em2, em3, em4 y em5) se asignan como interfaces opcionales para las distintas redes LAN independientes (ver figura 2-19).

```

WAN (wan)      -> em0
LAN (lan)      -> em1
OPT1 (opt1)    -> em2
OPT2 (opt2)    -> em3
OPT3 (opt3)    -> em4
OPT4 (opt4)    -> em5

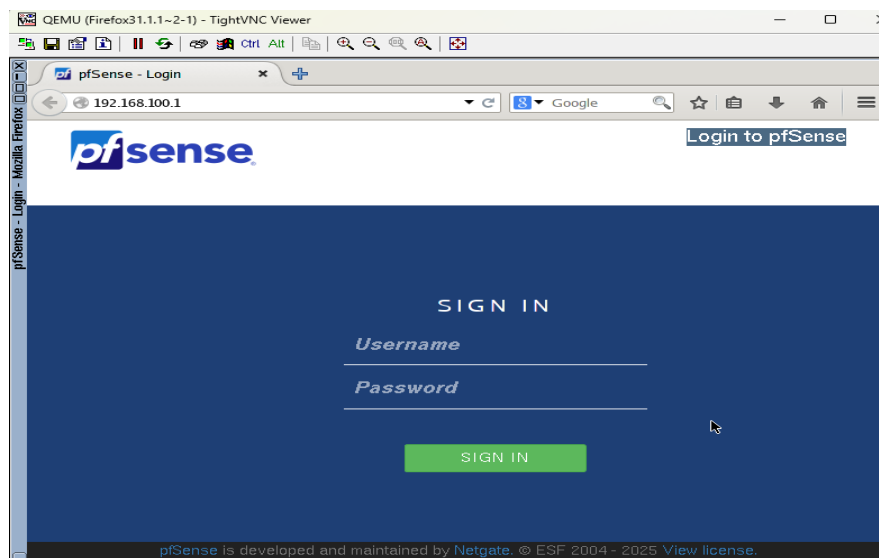
```

Fuente: Captura de pantalla propia terminal pfSense.

Figura 2-19 Asignación de interfaces.

2.4.3.3 Interfaz web pfSense

Para continuar de manera más sencilla con la configuración, se utilizará la interfaz web de pfSense. Para ello, se accede desde el nodo Firefox de GNS3 a la dirección IP 192.168.100.100. En el firewall, a la interfaz em5 se le asigna la IP 192.168.100.1. Luego, para facilitar la comunicación entre el nodo de gestión y el firewall pfSense, se desactiva temporalmente el filtrado de paquetes mientras se establecen las reglas de entrada correspondientes. En la Figura 2-20 se muestra el acceso a la interfaz web, la cual mantiene las credenciales por defecto: usuario **admin** y contraseña **pfsense**.

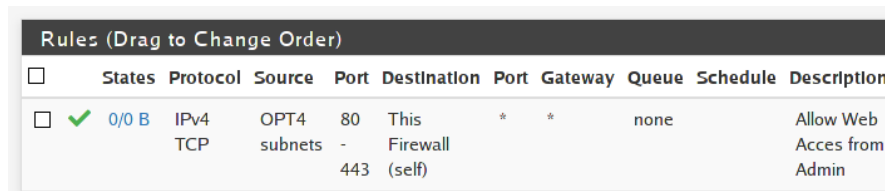


Fuente: Captura de pantalla propia del terminal pfSense.

Figura 2-20 Interfaz web pfSense.

2.4.3.4 Reactivación de reglas del firewall

Se procedió a crear una regla de paso (ver figura 2-21). Explícita para la interfaz OPT4 con el objetivo de permitir el tráfico TCP hacia el Firewall mismo a través de los puertos 80 (HTTP) y 443 (HTTPS). Tras guardar y aplicar esta regla, se utilizó el comando **pfctl -e** en la Shell de pfSense para reactivar el filtro de paquetes (Firewall), asegurando que el acceso administrativo web sea permanente y seguro



Rules (Drag to Change Order)										
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☒	✓	0/0 B	IPv4 TCP	OPT4 subnets	80 -	This Firewall 443 (self)	*	*	none	Allow Web Access from Admin

Fuente: Captura de pantalla propia pfSense.

Figura 2-21 Regla de paso.

2.5 ENRUTAMIENTO INTER-VLAN

El enrutamiento inter-VLAN es el mecanismo de Capa 3 que permite que el tráfico de datos fluya y se comuniquen entre diferentes redes lógicas o VLAN que están separadas. Su importancia en una arquitectura segura para SCADA radica en que el Firewall se convierte en el único punto de control (Gateway) para todas las zonas. Esto asegura que toda la comunicación entre, por ejemplo, la Red IT y los PLCs de la Red OT, deba ser inspeccionada y filtrada por reglas estrictas, aplicando el principio de Mínimo Privilegio y aislando lógicamente los sistemas críticos de control industrial del riesgo de la red corporativa. En la figura 2-22 se observa la creación de etiquetas en el firewall para proceder con la configuración de puertas de enlace.

VLAN Interfaces				
Interface	VLAN tag	Priority	Description	Actions
em1 (lan)	10		VLAN_10_OFICINA	 
em1 (lan)	20		VLAN_20_FINANZAS	 
em1 (lan)	30		VLAN_30_GERENCIA	 
em4 (opt3)	40		VLAN_40_DMZ_IT	 
em3 (opt2)	50		VLAN_50_DMZ_OT	 
em2 (opt1)	60		VLAN_60_CONTROL	 
em2 (opt1)	61		VLAN_61_PRODUCCION	 
				 Add

Fuente: Captura propia de interfaz web pfSense.

Figura 2-22 VLAN en firewall.

- Asignación de Gateway

Para habilitar el Gateway, se crearon siete subinterfaces de VLAN en pfSense, asignando a cada una su dirección Gateway estática. Esto permite la comunicación inicial, pero requiere configurar reglas de Firewall estrictas para limitar el tráfico y mantener el aislamiento de seguridad necesario entre las zonas IT, OT y DMZ (ver Figura 2-23).

```
VLAN_10 (opt5) -> em1.10      -> v4: 192.168.10.1/24
VLAN_20 (opt6) -> em1.20      -> v4: 192.168.20.1/24
VLAN_30 (opt7) -> em1.30      -> v4: 192.168.30.1/24
VLAN_40 (opt8) -> em4.40      -> v4: 172.16.40.1/24
VLAN_50 (opt9) -> em3.50      -> v4: 172.16.50.1/24
VLAN_60 (opt10) -> em2.60     -> v4: 10.0.60.1/24
VLAN_61 (opt11) -> em2.61     -> v4: 10.0.61.1/24
```

Fuente: Captura propia de terminal pfSense.

Figura 2-23 Puertas de enlace.

2.6 REGLAS DEL FIREWALL

La configuración de las Reglas de Firewall es donde la seguridad de la topología SCADA cobra vida. Ahora mismo, la red está en un estado de "Denegar todo" entre las zonas OPT, lo cual es muy seguro, pero inoperable.

2.6.1 Acceso a Internet

Se implementó una regla de firewall en pfSense con el objetivo de permitir que los usuarios pertenecientes a la red corporativa puedan acceder a Internet a través de la interfaz WAN. Esta regla filtra el tráfico saliente únicamente desde las redes internas autorizadas, garantizando que solo los equipos corporativos tengan salida hacia servicios externos. Esta medida contribuye a reforzar la seguridad perimetral.

2.6.2 Acceso a la DMZ IT

Se crean reglas Pass (figura 2-24) en las interfaces correspondientes a la red IT para el tráfico de salida. La regla permite a las subredes IT comunicarse con la red DMZ IT (172.16.40.0/24) usando el protocolo TCP y limitándose estrictamente a los puertos HTTP (80), HTTPS (443) y SMTP (25). Esto garantiza que solo el acceso web seguro y el correo saliente pasen el firewall hacia los servidores de la DMZ.

Reglas (arrastrar para cambiar el orden)							
☐	Departamento	Protocolo	Fuente	Puerto	Destino	Puerto	
☐	✓ 0/0 B	IPv4 TCP	VLAN_10_OFICINA subnets	*	VLAN_40_DMZ_IT subnets	25 (SMTP)	
☐	✓ 0/0 B	IPv4 TCP	VLAN_10_OFICINA subnets	*	VLAN_40_DMZ_IT subnets	80 - 443	

Fuente: Captura de pantalla propia de pfSense-

Figura 2-24 Regla para acceso DMZ-IT.

2.6.3 Regla de Aislamiento de la red OT

La configuración de esta regla es fundamental, ya que actúa como el pilar de la seguridad OT al aplicar el principio de Mínimo Privilegio. El tráfico originado en la Red Industrial PLC y HMI en VLAN 60 y 61 se encuentra bloqueado por defecto y para permitir la operación, se crea una regla permitir, explícita en las interfaces VLAN60_CONTROL y VLAN61_PRODUCCION. Esta regla autoriza únicamente el tráfico TCP (o UDP, según el servicio configurado) hacia el puerto 102 se utiliza para transferir datos entre sistemas de control industrial, lo que lo hace vital para la comunicación con PLCs. Al restringir el acceso a este puerto 102/TCP, se asegura la funcionalidad al permitir que los sistemas de control reporten datos, al mismo tiempo que se garantiza la seguridad impidiendo categóricamente que los dispositivos OT inicien cualquier conexión no autorizada hacia la Red IT o Internet (ver figura 2-24).

VLAN_60_CONTROL

VLAN_61_PRODUCCION

Reglas (arrastrar para cambiar el orden)											
☐	Departamento	Protocolo	Fuente	Puerto	Destino	Puerto	Puerta de enlace	Cola	Horario	Descripción	Acciones
☐	✓ 0/2 KiB	IPv4 ICMP any	VLAN_60_CONTROL subnets	*	Este servidor de seguridad (auto)	*	*	ninguno		permitir ping al gateway	
☐	✓ 0/0 B	IPv4 UDP	VLAN_60_CONTROL subnets	*	Este servidor de seguridad (auto)	53 (DNS)	*	ninguno		Permitir DNS	
☐	✓ 0/0 B	IPv4 TCP	VLAN_60_CONTROL subnets	*	VLAN_50_DMZ_OT subnets	102	*	ninguno		Regla de Acceso a SCADA	

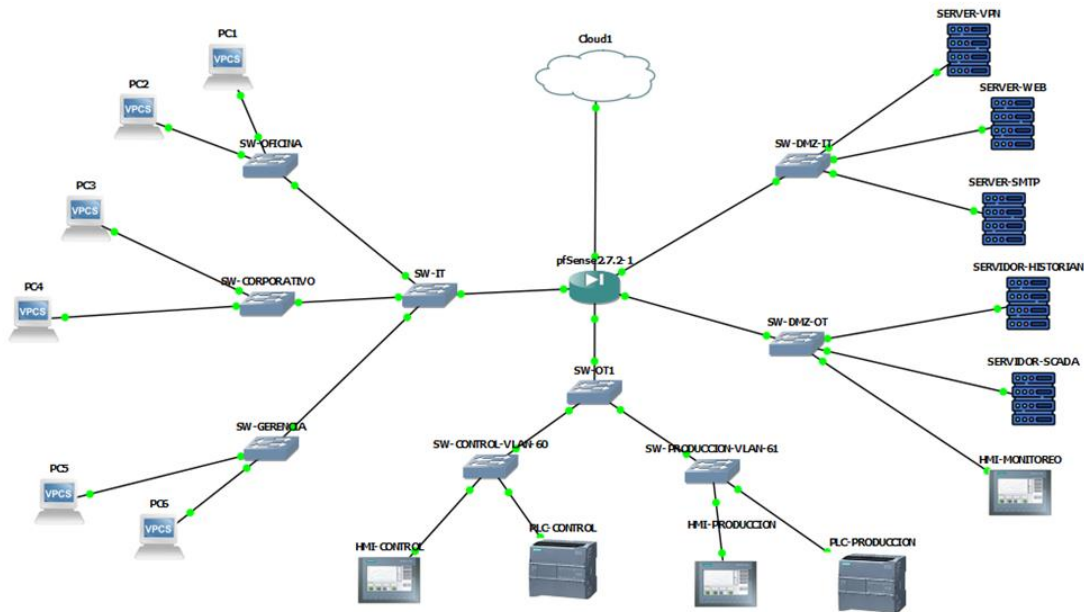
Fuente: Captura de pantalla propia de pfSense.

Figura 2-25 Reglas de aislamiento OT.

2.7 TOPOLOGÍA DE RED EN GNS3

La topología de red desarrollada en GNS3 representa una arquitectura segmentada enfocada en la correcta distribución del tráfico entre áreas IT y OT, (ver figura 2-26). En el diagrama se muestran pocos dispositivos finales (PC, PLC y HMI). Solo para simplificar la visualización, aunque en un entorno real cada zona podría contener más de 20 equipos industriales por área.

Este diseño sigue las recomendaciones de las normas ISA/IEC 62443, ya que implementa segmentación por zonas y conductos, separación entre IT y OT, uso de DMZ para servicios esenciales y control de tráfico mediante un firewall central, cumpliendo así principios fundamentales de ciberseguridad industrial.



Fuente: Captura de pantalla propia de GNS3.

Figura 2-26 Topología de red en GNS3.

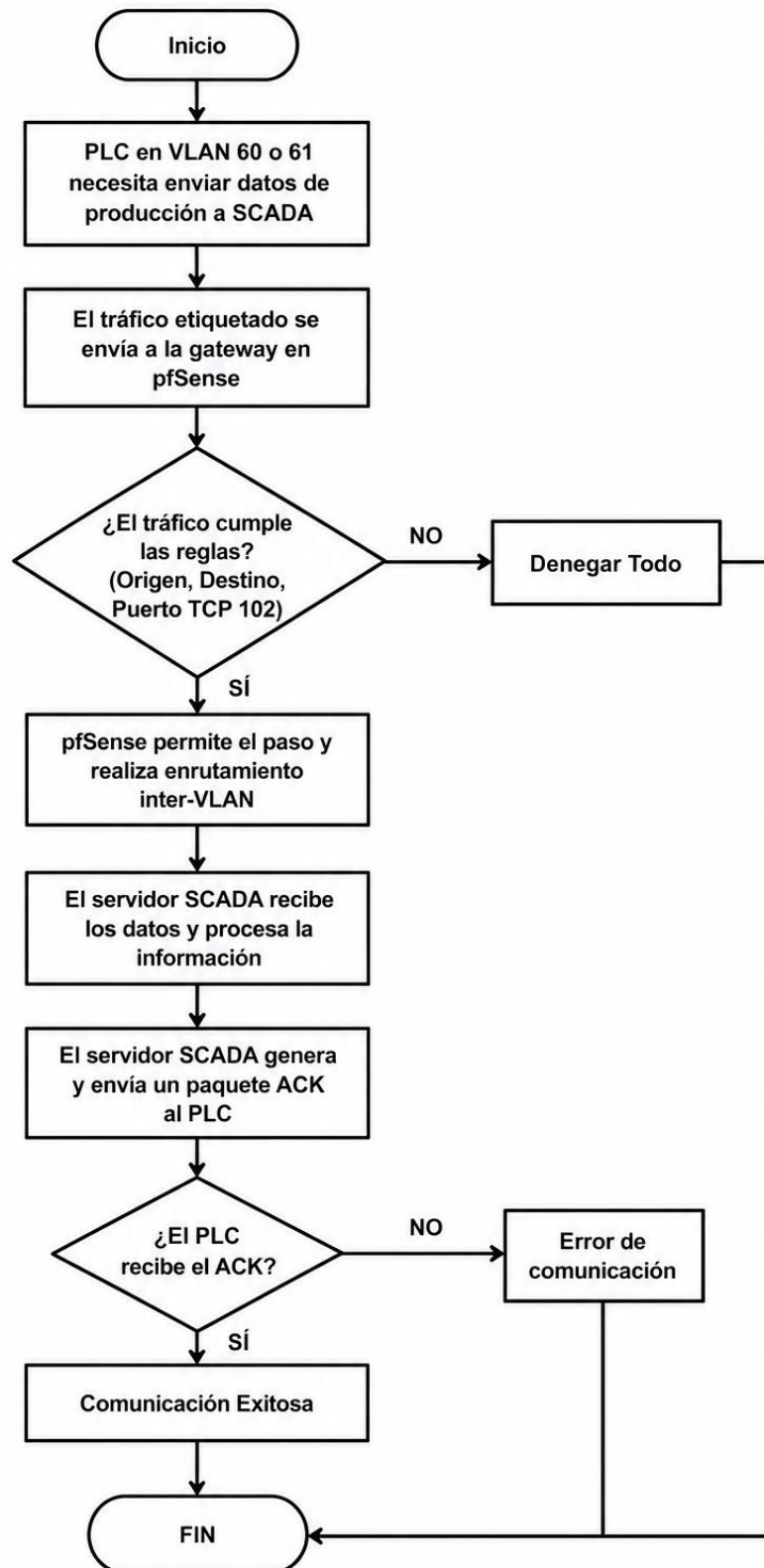
La infraestructura se articula mediante un Firewall central (pfSense) que gestiona la convergencia entre el mundo IT y OT. La separación física y lógica permite que los flujos de datos de administración no interfieran con los procesos de control en tiempo real. Se destaca la implementación de DMZ independientes, diseñadas para aislar servidores críticos como el SCADA e Historian, asegurando que el acceso a los datos de planta se realice bajo estrictas políticas de filtrado y sin exposición directa a redes externas.

2.8 SEGURIDAD DEL SISTEMA SCADA

Los PLC ubicados en las VLAN 60 o 61 envían datos de producción hacia el servidor SCADA. Ese tráfico llega al firewall pfSense, donde se valida que cumpla con los parámetros de seguridad definidos: origen permitido, destino en la VLAN 50 y uso del protocolo TCP/102. Si el tráfico coincide con esos criterios, es autorizado y se enruta correctamente hacia la VLAN 50, permitiendo que el servidor SCADA reciba los datos. Todo tráfico que no cumpla estas condiciones es bloqueado para evitar accesos no autorizados (ver Figura 2-27).

El protocolo TCP, exige que el servidor SCADA emita un acuse de recibo (ACK) tras la recepción de los datos. En caso de que el PLC no reciba dicha confirmación a través del firewall, la transacción se considera incompleta, activando los mecanismos de reintento del dispositivo de control. De este modo, el diagrama de flujo integra el ciclo de retroalimentación necesario para garantizar la fiabilidad en entornos industriales.

Además del filtrado básico entre las VLAN 60/61 y la VLAN 50, el sistema incorpora controles de seguridad adicionales. El firewall pfSense aplica una política de “denegación por defecto”, permitiendo solo el tráfico estrictamente necesario (IP de PLC al servidor SCADA por TCP/102) y bloqueando cualquier comunicación no autorizada entre VLAN. Esta segmentación, alineada con buenas prácticas como ISA/IEC-62443, reduce riesgos de accesos indebidos, movimientos laterales y posibles ataques desde la red IT, asegurando que el servidor SCADA reciba únicamente datos válidos y verificados.



Fuente: Elaboración propia.

Figura 2-27 Flujo de comunicación PLC.

CAPÍTULO 3: ANÁLISIS DE RESULTADOS Y COSTOS

3 ANÁLISIS DE RESULTADOS Y COSTOS

En este capítulo se presentan los resultados obtenidos al montar la arquitectura de red propuesta en el simulador GNS3. El objetivo es comprobar si el diseño realmente funciona y si las reglas configuradas en el pfSense logran segmentar el tráfico de forma efectiva, pasando de una red plana a una estructura de zonas basada en la norma ISA/IEC 62443. Para la validación, se realizaron pruebas de conectividad (pings y escaneo de puertos) entre las distintas áreas: la red administrativa (IT), la zona de control (SCADA) y la zona de producción (PLC). El foco principal fue verificar que los dispositivos de una VLAN no puedan acceder a otra sin permiso, cumpliendo con el principio de "denegación por defecto". Además, se detalla un análisis de costos para demostrar que es factible implementar esta solución en una planta real.

3.1 DIRECCIÓN IP

Para que la segmentación de red funcione, cada dispositivo (ya sea un PLC, el servidor SCADA) requiere una dirección IP. Se puede definir de forma sencilla como la identidad numérica de cada equipo dentro de la red. Su función es similar a una dirección particular: permite que el tráfico de datos sepa exactamente a qué dispositivo debe llegar y desde dónde está saliendo la información.

La máscara de subred es el límite de la red. Determina qué direcciones IP pertenecen a la misma sección y cuáles están fuera. La puerta de enlace es la IP del firewall en este caso, pfSense, a la que los equipos envían los datos para comunicarse con otras redes, en la tabla 3-1, se ven las direcciones asignadas a los dispositivos.

Cabe recalcar que el enlace del ISP es a través de DHCP, debido a que esto permite que el firewall pfSense obtenga de forma dinámica y automática tanto su dirección IP pública como su puerta de enlace y servidores DNS. Esta configuración simplifica la conectividad con el exterior, asegurando que, ante cualquier cambio en la infraestructura del proveedor de servicios, el firewall

mantenga la salida a Internet para actualizaciones de seguridad y gestión remota sin necesidad de intervención manual o configuraciones estáticas complejas.

Tabla 3-1 Direcciones dispositivos.

Dispositivo	IP	Máscara de subred	Puerta de enlace	VLAN
WAN	DHCP	DHCP	DHCP	
PC1	192.168.10.15	255.255.255.0	192.168.10.1	10
PC2	192.168.10.20	255.255.255.0	192.168.10.1	10
PC3	192.168.20.15	255.255.255.0	192.168.20.1	20
PC4	192.168.20.20	255.255.255.0	192.168.20.1	20
PC5	192.168.30.15	255.255.255.0	192.168.30.1	30
PC6	192.168.30.20	255.255.255.0	192.168.30.1	30
HMI-CONTROL	10.0.60.15	255.255.255.0	10.0.60.1	60
PLC-CONTROL	10.0.60.20	255.255.255.0	10.0.60.1	60
HMI-PRODUCCIÓN	10.0.61.15	255.255.255.0	10.0.61.1	61
PLC-PRODUCCIÓN	10.0.61.20	255.255.255.0	10.0.61.1	61
SERVER-VPN	172.16.40.15	255.255.255.0	172.16.40.1	40
SERVER-WEB	172.16.40.20	255.255.255.0	172.16.40.1	40
SERVER-SMTP	172.16.40.25	255.255.255.0	172.16.40.1	40
SERVER-HISTORIAN	172.16.50.20	255.255.255.0	172.16.50.1	50
SERVER-SCADA	172.16.50.15	255.255.255.0	172.16.50.1	50
HMI-MONITOREO	172.16.50.20	255.255.255.0	172.16.50.1	50

Fuente: Elaboración propia.

3.2 PRUEBAS DESDE KALI LINUX

Kali Linux es una distribución especializada en ciberseguridad, diseñada para la realización de auditorías de red y pruebas de penetración. Es utilizada por profesionales del área debido a

que integra un conjunto preconfigurado de herramientas para la identificación, evaluación y mitigación de vulnerabilidades en infraestructuras tecnológicas.

Se realizará una simulación de un ataque de "Salto de Zona". El objetivo es ver si desde una zona de menor seguridad (como la PC de un invitado o un administrativo) puede "tocar" un activo crítico (como el PLC de Control).

3.2.1 Escaneo de puertos

Se conecta una máquina virtual Kali Linux en el switch de oficina y se le agregará la VLAN 10, se intentará ver que hay en la red industrial a través del comando **nmap**, que es una herramienta que permite identificar los dispositivos conectados a una red, así como los servicios que se encuentran en funcionamiento, por ejemplo, páginas web, cámaras, routers o servidores y los puertos que permanecen abiertos en cada uno de ellos.

3.2.1.1 Escenario A: Con firewall configurado

Se realizó un escaneo Nmap desde la VLAN de IT hacia el PLC (10.0.60.20). Como se muestra en la Figura 3-1, el host aparece como "Down".

```
(kali㉿kali)-[~]
$ nmap 10.0.60.20
Starting Nmap 7.95 ( https://nmap.org ) at 2026-03-03 13:34 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or
specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds
```

Fuente: Captura de pantalla Kali Linux.

Figura 3-1 Prueba de escaneo A.

El resultado es que el pfSense bloquea el tráfico cumpliendo el privilegio mínimo y seguridad para la red industrial.

3.2.1.2 Escenario B: Con regla de acceso total

Al habilitar la regla permisiva de “aceptar todo”, el escaneo reveló múltiples puertos críticos abiertos (ver figura 3-2).

```
(kali㉿kali)-[~]
$ nmap 10.0.60.20
Starting Nmap 7.95 ( https://nmap.org ) at 2026-03-03 14:11 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or
specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.60.20
Host is up (0.0075s latency).

PORT      STATE SERVICE
1/tcp     open  tcpmux
3/tcp     open  compressnet
4/tcp     open  unknown
6/tcp     open  unknown
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
20/tcp    open  ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
```

Fuente: Captura de pantalla Kali Linux.

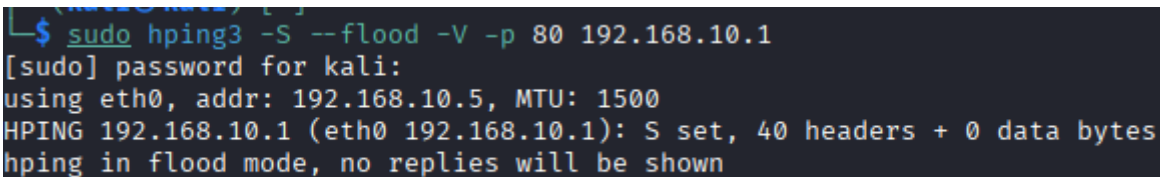
Figura 3-2 Prueba de escaneo B.

El escaneo en el Escenario B reveló una superficie de ataque crítica. Al no existir restricciones en el firewall, servicios como Telnet (23), FTP (21) y HTTP (80) quedaron visibles desde la red administrativa. Esto demuestra que cualquier usuario de la oficina, o un intruso vía Wi-Fi, podría realizar desde Capturas de tráfico (sniffing) hasta el sabotaje total del PLC.

En conclusión, la falta de segmentación anula la seguridad del entorno OT, dejando los activos de producción a merced de protocolos inseguros que transmiten datos y credenciales en texto plano.

3.2.2 Prueba de ataque DoS

Para verificar si el firewall soporta un ataque real, se lanzó una inundación de paquetes desde la red de oficina (Kali Linux) a la puerta de enlace usando el comando **hping3 --flood**. El objetivo es saturar la puerta de enlace para ver si el pfSense se bloquea o deja de responder (ver figura 3-3).



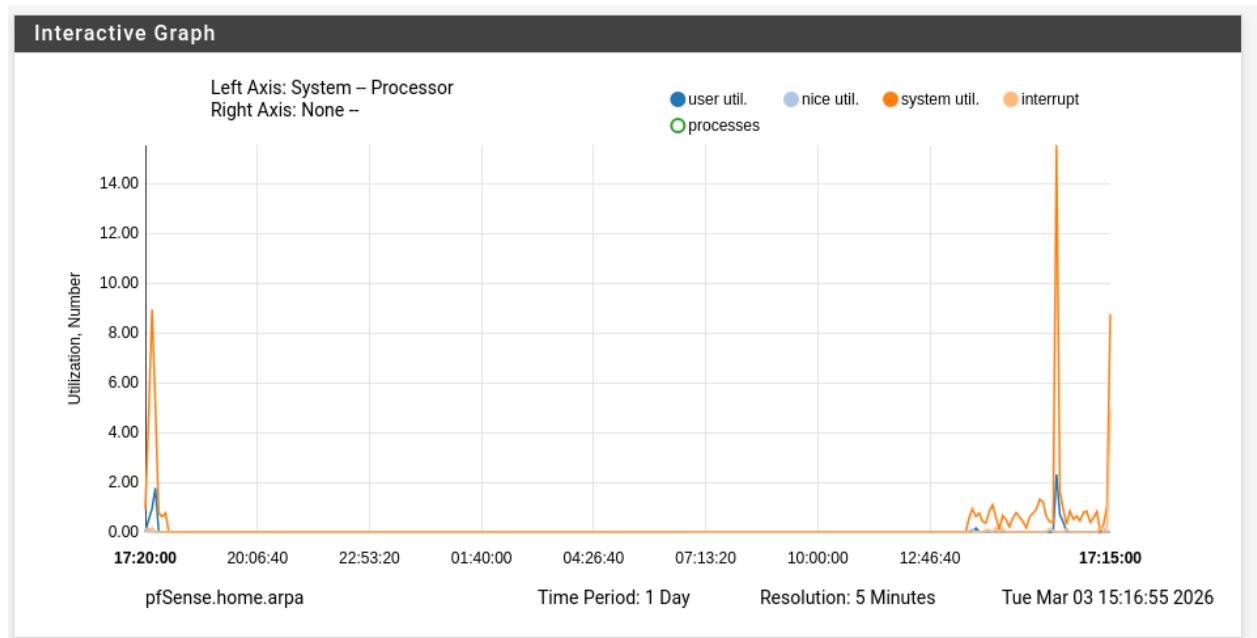
```

kali@kali:~$ sudo hping3 -S --flood -V -p 80 192.168.10.1
[sudo] password for kali:
using eth0, addr: 192.168.10.5, MTU: 1500
HPING 192.168.10.1 (eth0 192.168.10.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
  
```

Fuente: Captura de pantalla Kali Linux.

Figura 3-3 Comando DoS.

Tras realizar la prueba, pfSense respondió correctamente. En la figura 3-4 se puede observar que el uso de sistema subió a 15.54% para procesar y descartar el tráfico malicioso, pero se mantuvo estable sin bloquearse. Esto garantiza que la saturación no afecte la red industrial, permitiendo que los dispositivos sigan operando y comunicándose sin retrasos. Aunque es una simulación en GNS3, el resultado valida que la configuración protege la disponibilidad de los activos críticos ante intentos de sabotaje por saturación.



Fuente: Captura de pantalla pfSense.

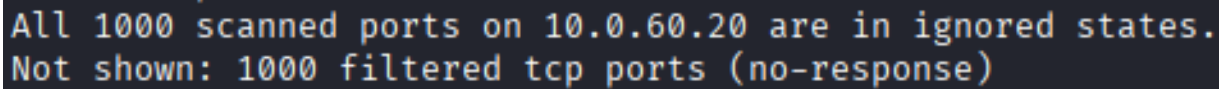
Figura 3-4 Gráfico de uso del sistema.

3.2.3 Prueba de escaneo de huella digital

Los atacantes suelen usar un “escaneo de huella” traducido fingerprinting para saber que versión de software se está ejecutando y de esa forma buscar un fallo específico.

3.2.3.1 Escenario A: Con firewall configurado

Se utiliza el comando “nmap -sV -Pn 10.0.60.20” dirigido al PLC del área de control. Este comando se emplea para analizar un dispositivo específico dentro de la red y obtener información sobre los servicios que tiene activos, en la Figura 3-5 se observa el resultado.



```
All 1000 scanned ports on 10.0.60.20 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)
```

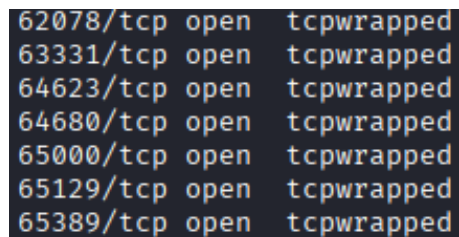
Fuente: Captura de pantalla Kali Linux.

Figura 3-5 Resultado A.

Se puede observar que el firewall bloqueó el escaneo, mostrando los puertos como "filtered" e impidiendo que el atacante obtenga información del sistema. Esto confirma que la red no solo es segura, sino también invisible para herramientas de escaneo avanzado, protegiendo la identidad de los equipos críticos.

3.2.3.2 Escenario B: con regla de acceso total

En el escenario vulnerable presento los resultados de la figura 3-6



```
62078/tcp open tcpwrapped  
63331/tcp open tcpwrapped  
64623/tcp open tcpwrapped  
64680/tcp open tcpwrapped  
65000/tcp open tcpwrapped  
65129/tcp open tcpwrapped  
65389/tcp open tcpwrapped
```

Fuente: Captura de pantalla Kali Linux.

Figura 3-6 Resultado B.

Al permitir acceso total, el comando `nmap -sV` logró alcanzar los puertos del dispositivo. Sin embargo, el resultado arrojó el estado "tcpwrapped". Esto indica que, aunque la conexión llega al destino, el servicio cierra el enlace inmediatamente para evitar la identificación de su versión y software.

3.2.2 Conclusión pruebas Kali Linux

Tras completar las auditorías con Kali Linux, se determinó que, si bien los vectores de ataque pueden ser múltiples y variados (desde saturación por DoS hasta escaneos de reconocimiento), el firewall pfSense se consolida como el elemento más crítico de la arquitectura. Las pruebas demostraron que una configuración de reglas bien definida no solo mitiga el tráfico malicioso, sino que actúa como una barrera de invisibilidad para la red industrial.

La implementación de este perímetro de seguridad es lo que garantiza que los intentos de acceso no autorizado sean bloqueados antes de alcanzar la zona de control. Esto es vital para asegurar la integridad de los computadores, la disponibilidad de los PLCs y, sobre todo, la protección del servidor SCADA, el cual representa el núcleo de la operación. En definitiva, el firewall no solo previene caídas del sistema por saturación, sino que salvaguarda la confidencialidad técnica de los activos, permitiendo que la planta siga operando sin interrupciones incluso bajo condiciones de ataque activo.

3.3 EVALUACIÓN DE COSTOS

La evaluación de costos es un aspecto fundamental en el desarrollo del presente proyecto, ya que permite determinar la viabilidad económica de las soluciones propuestas. No solo se consideran los elementos técnicos, sino también los recursos necesarios para su implementación, tales como equipamiento, tiempo de trabajo, capacitación y mantenimiento.

Los valores presentados en este informe se expresan en pesos chilenos (CLP) y se encuentran estandarizados en Unidad de Fomento (UF). Para efectos de cálculo, se considera el valor de la UF al 4 de marzo de 2026, correspondiente a \$39.813,33 CLP.

3.3.1 Profesionales necesarios

Para la implementación efectiva de la arquitectura de red segura propuesta, se requiere un equipo multidisciplinario con un enfoque especializado en tecnologías de operación (OT). A diferencia de una infraestructura informática convencional, los entornos industriales exigen profesionales que comprendan la criticidad de los procesos en tiempo real.

La implementación integral de la reestructuración de red se estima en un plazo total de 14 semanas, distribuidas de manera estratégica para garantizar la continuidad operacional de la planta. Las primeras 3 semanas se destinan al levantamiento técnico y detección de vulnerabilidades de la red antigua, seguidas de 4 semanas de configuración y validación en entornos de simulación (GNS3/VMware). La fase más crítica, correspondiente a la migración física de los activos y segmentación de VLAN, toma otras 4 semanas programadas para evitar paradas de producción no costeadas, finalizando con 3 semanas de pruebas de intrusión con Kali Linux, marcha blanca y capacitación del personal operativo.

3.3.1.1 Ingeniero en control e instrumentación Industrial

Responsable de la lógica de procesos. Su función es garantizar que la nueva segmentación no interrumpa la comunicación entre los PLCs y el SCADA, gestionando la criticidad de los activos.

3.3.1.2 Ingeniero en redes o ciberseguridad

Encargado de la implementación técnica del firewall pfSense, creación de VLAN y reglas de tráfico, así también como la mantención del firewall.

3.3.1.3 Técnico en telecomunicaciones y redes

Es el encargado de las conexiones físicas entre ellas cableados, canaletas y elaboración de puntos de red y fibra óptica.

3.3.2 Fases y carga horaria

La reestructuración se divide en cuatro fases: Levantamiento (3 semanas), Diseño (4 semanas), Migración (4 semanas) y Validación (3 semanas). Bajo un modelo de dedicación parcial, el Ingeniero en Control lidera con una carga constante de supervisión, intensificándose en la fase inicial y final. El Ingeniero de Ciberseguridad concentra su trabajo en la Fase 2 para la programación lógica del firewall, mientras que el Técnico en Telecomunicaciones interviene exclusivamente en la Fase 3 para la ejecución del montaje físico y cableado. Esta metodología de intervención por hitos permite cumplir el plazo de 14 semanas optimizando el uso de recursos y el presupuesto total en UF. Si se tomara en cuenta desde el 4 de marzo de 2026 de inicio de forma hipotética quedaría de la siguiente forma (ver tabla 3-2).

Tabla 3-2 Carta Gantt

	Fecha inicio	Fecha Final	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6	Semana 7	Semana 8	Semana 9	Semana 10	Semana 11	Semana 12	Semana 13	Semana 14
Fase 1	04-03-2026	24-03-2026														
Fase 2	25-03-2026	21-04-2026														
Fase 3	22-04-2026	20-05-2026														
Fase 4	21-05-2026	10-06-2026														

Fuente: Elaboración propia en Excel.

Se ha planificado una progresión lineal donde cada fase comienza inmediatamente al día siguiente del hito de cierre anterior, garantizando que no existan tiempos muertos en el cronograma y optimizando la disponibilidad de los especialistas según el modelo de dedicación parcial.

Para asegurar la ejecución eficiente, se ha definido un modelo de dedicación parcial orientado a hitos, totalizando 320 horas hombre (HH) distribuidas según las necesidades de cada etapa: el Ingeniero en Control dedica 2,6 horas diarias; el Ingeniero en Redes, 1,1 horas; y el Técnico en Telecomunicaciones, 0,9 horas. Esta modalidad es altamente eficiente para empresas de servicios externalizados, ya que permite que un mismo equipo técnico ejecute múltiples proyectos simultáneamente, optimizando su capacidad instalada y garantizando al cliente expertos de alto nivel sin los costos fijos de una jornada de planta completa.

3.3.3 Costos profesionales

Teniendo en cuenta los puntos anteriores en la tabla 3-3, se detalla el costo estimado por servicios profesionales considerado para el proyecto.

Tabla 3-3 Valor de mercado por hora profesional.

Profesional	Valor Hora (UF)	Horas Proyecto (14 semanas)	Total (UF)
Ing. en Control e Instrumentación	0,2566 UF	180	46,188 UF
Ing. en Redes y Ciberseguridad	0,1983 UF	80	15,864 UF
Técnico en Telecomunicaciones	0,1515 UF	60	9,09 UF
TOTAL, INVERSIÓN RR.HH.	0,6064 UF	320	71,142 UF

Fuente: Elaboración propia en base a requerimientos.

La modalidad de contratación seleccionada es la de Prestación de Servicios Profesionales (Honorarios), con pagos asociados al cumplimiento de hitos específicos por fase. Este modelo garantiza que el desembolso total de 71,142 UF esté sujeto a la entrega de productos tangibles,

optimizando el flujo de caja del proyecto. Los valores presentados corresponden a honorarios brutos, calculados en base al promedio de mercado para profesionales con 3 años de experiencia según la plataforma mifuturo.cl (ver anexo A), considerando que dichas remuneraciones varían significativamente según la especialización y años de experiencia de cada profesional.

3.3.4 Costos de Dispositivos

Se tomará en cuenta solo el mercado nacional debido a los tiempos de implementación calculados para el proyecto (14 semanas) y los tiempos de logística internacional pueden tomar hasta 60 días en aduana también considerando el pago de impuestos correspondiente a internación en Chile es del 6% en el arancel de aduana más el IVA que es de 19%, dando un impuesto de 25%, en la tabla 3-4 se observa el costo, en el anexo B esta adjuntado de donde se obtuvieron cada uno de los costos.

Tabla 3-4 Costos de Dispositivos

Dispositivo	Precio Unidad	Cantidad	Total
Switch Cisco Catalyst 1300	25,1 UF	6	150,6 UF
Netgate 6100 pfSense	39,18 UF	1	39,18 UF
Cable UTP cat6 300m	1,32 UF	1	1,32 UF
500mt 1-Fibra LC-LC Monomodo G657A2	2,70 UF	1	2,70 UF
Gabinete Rack de Pared LINKMADE 12U	3,54 UF	4	14,16 UF
Back-UPS APC BX1200MI-MS	3,66 UF	10	36, 6 UF
Servidor Dell Power Edge R240	29,01 UF	3	58,02 UF
TOTAL, INVERSIÓN DISPOSITIVOS	104,51 UF	26	302,58 UF

Fuente: Elaboración propia en base a requerimientos.

3.3.4.1 Justificación de cada dispositivo

La selección de estos componentes se basa en la creación de una infraestructura robusta para una red industrial, asegurando la segregación de funciones y la alta disponibilidad de los servicios críticos.

- Redes y seguridad

Switch Cisco Catalyst 1300: Se seleccionan por su capacidad de gestión avanzada y soporte de VLAN, permitiendo la segmentación lógica entre las redes de Control (OT) y de Datos (IT).

Netgate 6100 pfSense: Actúa como el núcleo de seguridad perimetral. Su elección se debe a la flexibilidad para gestionar reglas de firewall complejas y su capacidad nativa para actuar como concentrador de VPN, eliminando la necesidad de hardware adicional para acceso remoto seguro.

- Servidores

Servidores Dell PowerEdge R240 (x3): Se optó por una configuración de tres nodos físicos independientes para cumplir con la arquitectura de seguridad del diagrama SW-DMZ-IT.

Nodo 1 (SCADA): Dedicado exclusivamente al control en tiempo real para garantizar latencia cero.

Nodo 2 (Historian): Ubicado en la DMZ OT para el almacenamiento masivo de datos históricos.

Nodo 3 (Servicios WEB/SMTP): Ubicado en la DMZ IT, aislando físicamente los servicios con exposición a redes externas de los sistemas de control críticos.

- Conectividad

Fibra Monomodo G657A2 (500m): Elegida por su baja atenuación a largas distancias y su resistencia a curvaturas, ideal para el despliegue en entornos industriales con ductos complejos.

Cable UTP Cat6: Estándar que asegura velocidades de hasta 1 Gbps para las conexiones de última milla y dispositivos finales.

- Infraestructura y Energía

Gabinete Rack LINKMADE 12U: Proporciona el espacio necesario para albergar los 9U de equipos proyectados, asegurando orden mecánico y flujo de aire.

UPS APC BX1200MI-MS: Garantiza la continuidad operativa ante fallas eléctricas, protegiendo la integridad de las bases de datos del Historian y la disponibilidad del SCADA.

3.3.4.2 Consideraciones de diseño

La presente selección de dispositivos y sus costos asociados en UF constituyen una propuesta técnica de alto rendimiento basada en criterios de segregación de red y disponibilidad industrial. Se debe considerar esta implementación como una referencia hipotética, ya que la configuración final es flexible y admite múltiples alternativas tecnológicas de marcas con equivalencia funcional (como Mikrotik, HP o Fortinet). La elección definitiva de los componentes quedará sujeta a la disponibilidad de stock.

3.3.5 Costos totales

A continuación, se presenta la Tabla 3-5, la cual consolida la valoración económica total de la reestructuración de red propuesta para la planta. Este presupuesto integra de manera detallada los costos de adquisición de hardware activo, la infraestructura física de soporte y la inversión en capital humano especializado para las 14 semanas de ejecución. Se ha incluido, además, un margen del 5% para costos variables, destinado a cubrir herramientas e imprevistos técnicos, asegurando así la integridad financiera del proyecto frente a las condiciones del mercado proyectadas al 4 de marzo de 2026.

Tabla 3-5 Costos totales

Categoría de Inversión	Descripción General	Total (UF)	Total (CLP)
Equipamiento de Red	Switches, Firewall, Fibra, Rack y UPS	244,56 UF	\$9.737.311
Servidores Críticos	3 x Dell PowerEdge R240	87,03 UF	\$3.465.158
Recursos Humanos	Ingeniería y Técnicos (320 hrs)	71,142 UF	\$2.832.400
Costos Variables (5%)	Herramientas, ferretería	20,1366 UF	\$801.704
Imprevistos (10%)	Fallos de equipos o retrasos	40,27 UF	\$1.603.487
TOTAL, INVERSIÓN	Costo Neto del Proyecto	463,1386 UF	\$18.440.060

Fuente: Elaboración propia en base a requerimientos.

3.3.5.1 Análisis de costos totales

El análisis de la Tabla 3-5 revela una inversión estratégica de 463,1386 UF (\$18.440.060 CLP), donde el 52% de los recursos se concentra en robustecer la infraestructura de red y el 18% en la segregación física de servidores (SCADA, Historian e IT) para eliminar puntos únicos de falla y garantizar la ciberseguridad industrial. Esta valoración no solo cubre activos tecnológicos de alto estándar, sino que asegura la viabilidad técnica mediante la asignación de 71,142 UF en capital humano especializado para las 14 semanas de ejecución, junto con un fondo de reserva del 5% para imprevistos operativos y 10% de imprevistos por fallas de hardware o retrasos. Como recomendación crítica, se sugiere que la adquisición de los equipos se realice en una sola etapa para mitigar la volatilidad de precios proyectada al 4 de marzo de 2026 y para asegurar la compatibilidad total de las versiones de firmware entre los switches Cisco y el firewall Netgate desde el día uno de la puesta en marcha.

CONCLUSIONES

La reestructuración de la red planteada en este trabajo no debe interpretarse como un gasto de capital opcional, sino como una inversión crítica de supervivencia operativa. En el contexto industrial actual, mantener una infraestructura deficiente bajo la premisa del ahorro es una negligencia técnica, especialmente al gestionar sistemas SCADA que controlan procesos físicos en tiempo real. La exposición de un servidor de control a redes no segmentadas equivale a comprometer la integridad de la planta; por ello, la adopción de tres nodos físicos independientes (SCADA, Historian e IT) responde a la necesidad de aislar fallas y ataques, garantizando que la producción no se detenga ante un compromiso en el área administrativa.

Esta implementación se alinea estrictamente con los marcos de trabajo de la norma ISA/IEC 62443, cumpliendo con los niveles de seguridad y la segmentación por "zonas y conductos" que el estándar internacional exige para infraestructuras críticas. Mirando hacia el futuro, la convergencia IT/OT amplía la superficie de riesgo de manera exponencial; ante amenazas cada vez más automatizadas, el diseño valorizado en 463,1386 UF establece la línea base necesaria para escalar tecnológicamente sin vulnerar la operación. En definitiva, la ciberseguridad industrial ha dejado de ser una característica deseable para convertirse en el pilar normativo y operativo que sostiene la continuidad de cualquier negocio moderno.

Finalmente, es imperativo reconocer que el perfil del Ingeniero en Control e Instrumentación Industrial ha evolucionado, ya no basta con el dominio de la lógica de control y la instrumentación de campo. Dada la alta vulnerabilidad de los sistemas automatizados actuales al estar integrados en red, es fundamental que el profesional posea conocimientos sólidos en seguridad de datos y protocolos de comunicación. Comprender cómo proteger los activos desde la capa física hasta la lógica es hoy una competencia esencial para salvaguardar los procesos productivos y liderar la transformación digital de manera segura y responsable.

BIBLIOGRAFÍA

-Reporte Minero. (2025, 1 de mayo). Ciberseguridad industrial bajo amenaza: intrusiones en sistemas OT se disparan y lanzan solución para detectarlas en tiempo real.[en línea]. 2026 [consulta en enero del 2026]. Disponible en:

<https://www.reporteminero.cl/noticia/noticias/2025/05/ciberseguridad-industrial-bajo-amenaza>

- Carrasco, G. (2025, 18 de agosto). Los sectores más golpeados por el cibercrimen en Chile durante 2025. Redicom. [en línea]. 2026 [consulta en enero del 2026]. Disponible en:

<https://redicom.cl/blog/los-sectores-mas-golpeados-por-el-cibercrimen-en-chile-durante-2025>

-Fortinet. (s.f.). Norma IEC 62443: Mejora de la Ciberseguridad para los sistemas de automatización y control industrial. [en línea]. 2026 [consulta en enero del 2026]. Disponible en:

<https://www.fortinet.com/lat/resources/cyberglossary/iec-62443>

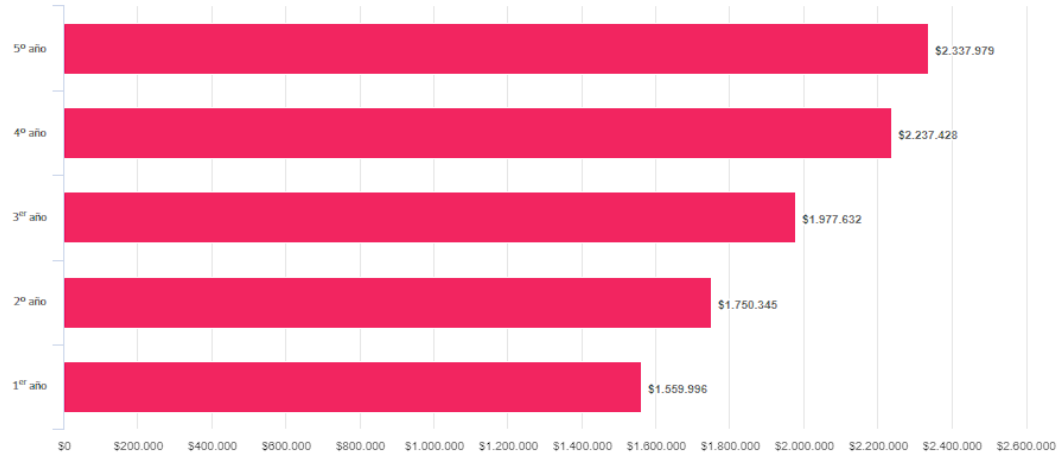
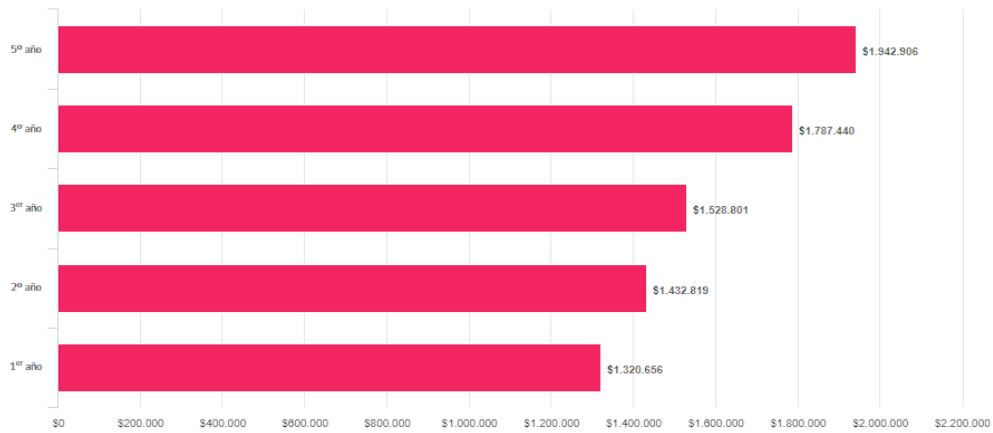
-Netgate. (2026). pfSense Documentación: Firewall Rules and InterVLAN Routing. [en línea].

2025 [consulta en enero del 2025]. Disponible en: <https://docs.netgate.com/pfsense/en/latest/>

-Offensive Security. (2026). Kali Linux Documentation: Network Penetration Testing with Nmap and Metasploit. [en línea]. 2025 [consulta en enero del 2025]. Disponible en:

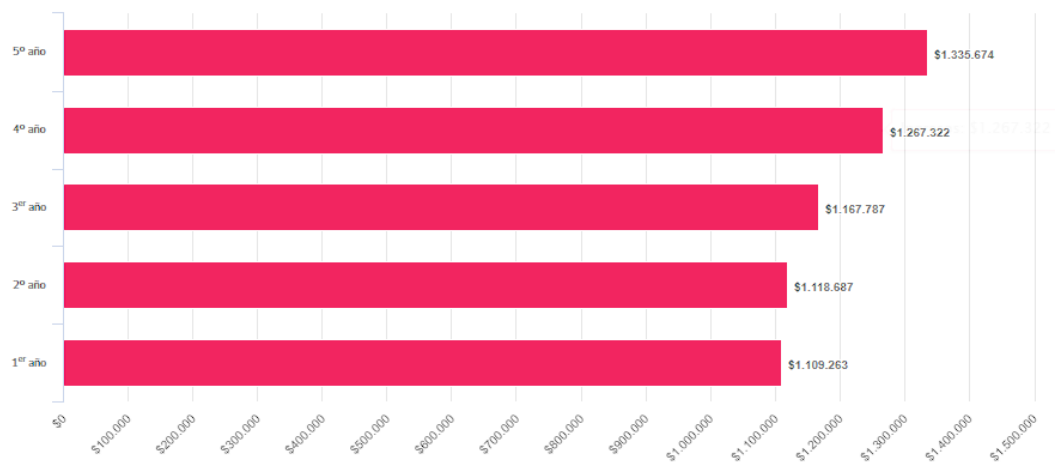
<https://www.kali.org/docs/>

ANEXOS

ANEXO A: SUELDOS PROMEDIO PROFESIONALES MIFUTURO.CL**Ingeniería en Automatización, Instrumentación y Control****Ingresos brutos mensuales (en pesos a septiembre de 2025)****Ingeniería en Conectividad y Redes****Ingresos brutos mensuales (en pesos a septiembre de 2025)**

Técnico en Telecomunicaciones

Ingresos brutos mensuales (en pesos a septiembre de 2025)



ANEXO B: LINKS DE COMPRAS EQUIPOS

Switch Cisco Catalyst 1300:

<https://solucionestcp.cl/product/switch-Cisco-catalyst-c1300-24p-4g-24-puertos-gigabit-poe-4-sfp-1g-administrable/>

Netgate 6100 pfSense:

<https://www.vmcomputing.cl/producto/netgate-sg-6100/>

Cable UTP CAT6:

<https://www.mercadolibre.cl/p/MLC27115242>

Fibra monomodo:

<https://www.spdigital.cl/500mt-1-fibra-lc-lc-monomodo-g657a2-sm-jumper-cableexterior-3mm-gjyfh/>

Gabinete Rack pared:

<https://www.spdigital.cl/60cm-fondo-12u-gabinete-rack-pared-negro-inc-m6-2u/>

UPS:

<https://www.mercadolibre.cl/p/MLC20544713>

Servidor:

<https://www.spdigital.cl/servidor-dell-poweredge-r240-intel-xeon-e-2124-ram-8gb-disco-2tb-sata-hot-plug-sin-so/>