



GRUPO AEGIS TESSERACT:

Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) para
HELIOPOLIS.

INTEGRANTES:

Jair Alejandro Parra Tuzarma.

Diego Sánchez.

Jhon Santos.

Yeison Sánchez.

LÍNEA DE INVESTIGACIÓN SELECCIONADA:

Distribución energética y sistemas de gestión (energía).

EJECUTOR TÉCNICO: ING. ALEXANDER BEJARANO GONZALEZ.

MENTOR: ING. LIGIA STELLA BUSTOS RÍOS.

UNIVERSIDAD DE CALDAS.

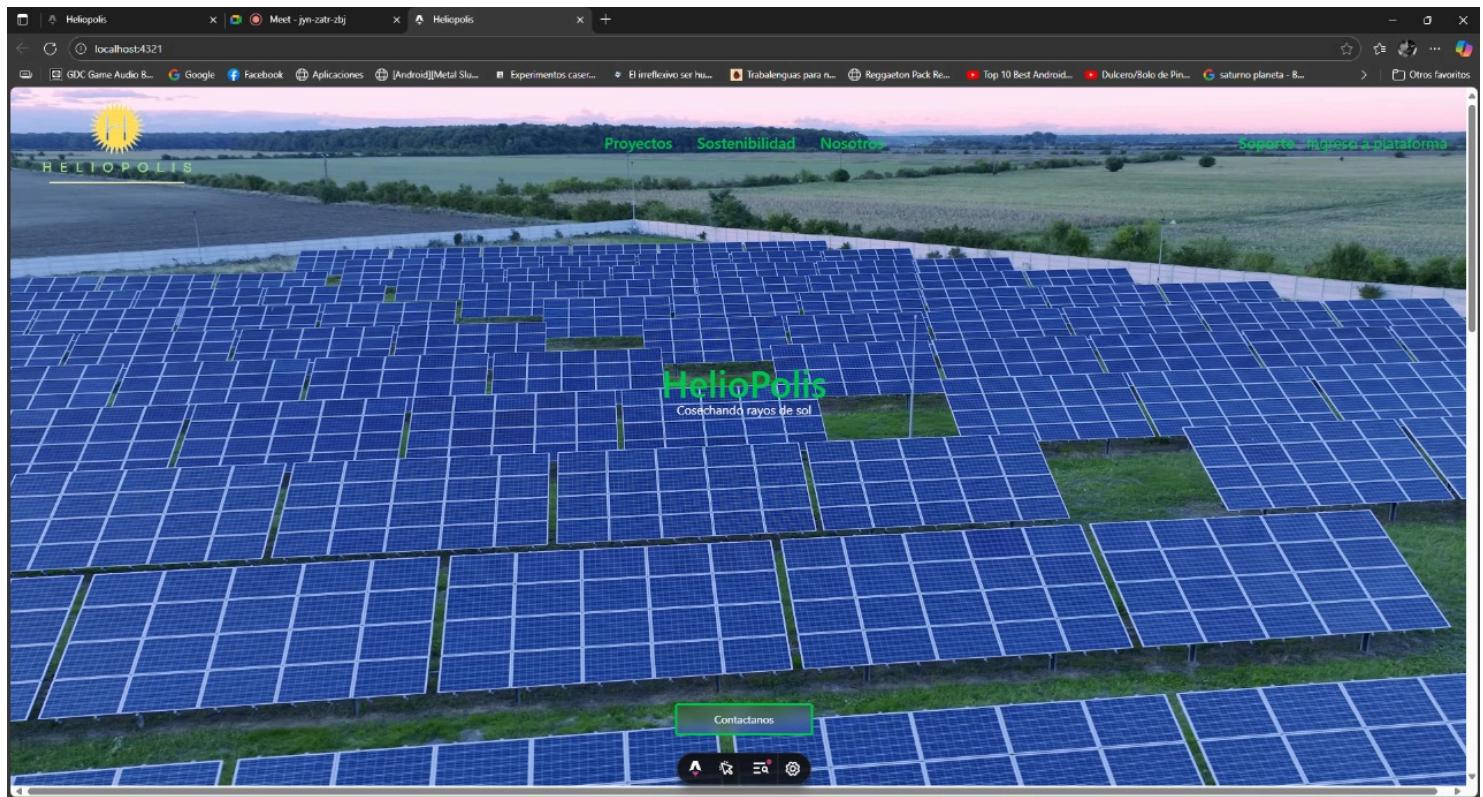
BOOTCAMP DE CIBERSEGURIDAD.

NIVEL EXPLORADOR.

PEREIRA - RISARALDA.

FECHA DE ENTREGA:

02/08/2025



Heliópolis es una empresa dedicada a la distribución de energía solar, a través de una gestión inteligente de consumo energético, supliendo las variables necesidades de nuestros clientes. Impulsamos la sostenibilidad con tecnología y compromiso ambiental.

TABLA DE CONTENIDOS:

GLOSARIO:	5
2. Introducción.....	9
Contexto del proyecto:.....	9
Organigrama:.....	9
Justificación:.....	10
1. Protección de Infraestructura Crítica:.....	10
2. Confidencialidad y seguridad de los datos:.....	10
3. Prevención de ciberataques avanzados (APT, ransomware, etc.):.....	10
4. Cumplimiento normativo y reputación empresarial:.....	11
Objetivos generales y específicos:.....	11
Objetivo General:.....	11
Objetivos Específicos:.....	11
Alcance del Entorno Simulado:.....	12
3. Marco Conceptual y Normativo.....	13
● Ley 1581 de 2012 (Protección de datos personales):.....	13
● Acuerdo CNO (Consejo Nacional de Operaciones) 1960 del 2025 para el SIN (Sistema Nacional Integrado):.....	14
● Implicaciones sectoriales:.....	14
● Referentes internacionales:.....	14
4. Configuración del Entorno Virtual (Inseguro).....	15
● Tabla de IPS (red insegura):.....	15
● Configuración:.....	15
● Herramientas utilizadas:.....	16
● Topología y segmentación:.....	16
● Configuración y evidencias:.....	16
Configuración Proxmox:.....	16
Configuración Firewall Mikrotik:.....	16
4.1. Configuración del Entorno Virtual (Segura).....	17
● Tabla de IPS (red segura):.....	17
● Configuración:.....	17
● Herramientas utilizadas:.....	18

● Topología y segmentación:.....	18
● Configuración y evidencias:.....	18
Configuración de VLANS en Firewall (pfSense):.....	18
Configuración Proxmox:.....	20
Configuración Pfsense:.....	20
VLANS SWITCH:.....	21
5. Diseño de la Red Corporativa.....	21
● Estructura simulada:.....	21
● Topologías:.....	22
Red inicial:.....	22
Red Final:.....	23
● Seguridad lógica:.....	24
6. Políticas de Seguridad de la Información.....	26
● Control de accesos individualizado:.....	26
● Política de contraseñas:.....	27
● Respaldo y disponibilidad:.....	28
● Gestión y registro de incidentes:.....	29
● Alineación a ISO/IEC 27001 y NERC-CIP.....	29
7. Análisis de Riesgos:.....	29
Activos críticos:.....	29
● Principales riesgos identificados:.....	29
● Metodología:.....	29
● Ventajas de MAGERIT:.....	29
● Matriz de amenazas:.....	30
● Vulnerabilidades y controles aplicados:.....	30
❖ Contraseñas en texto plano:.....	30
➤ Control aplicado:.....	30
❖ Sin HTTPS (solo HTTP):.....	30
➤ Control aplicado:.....	30
❖ No hay tokens con firmas o sesiones:.....	30
➤ Control aplicado:.....	30
❖ las rutas sensibles no están protegidas:.....	30
➤ Control aplicado:.....	30
8. Pruebas de Seguridad y Evaluación Técnica.....	30
● Herramientas empleadas:.....	30
● Resultados clave:.....	30
● Análisis:.....	31
9. Controles Técnicos Implementados.....	31
● Monitoreo de logs y alertas:.....	31

10. Gestión de Incidentes.....	31
● Simulación documentada de distintos escenarios de incidentes:.....	31
11. Otras Implementaciones para el SGSI.....	32
● Comité de Seguridad de la Información:.....	32
● Oficial de Seguridad de la Información (CISO):.....	32
● Responsables de Proceso:.....	32
● Política de Control de Personas:.....	32
● Política de USB Cero:.....	32
● Controles Físicos:.....	32
● Capacitación y Concienciación:.....	32
❖ Capacitación General:.....	33
❖ Capacitación Especializada:.....	34
❖ Campañas de Concienciación:.....	34
12. Conclusiones y Recomendaciones.....	34
12. Anexos:.....	35
ANEXO 1 Instalación Hipervisor:.....	36
ANEXO 2 Instalación Firewall Mikrotik:	48
¿Cómo funciona un firewall?.....	48
Tipos de firewalls.....	49
¿Por qué es importante un firewall?.....	49
ANEXO 3 Instalación Firewall Pfsense:.....	58
¿Cómo funciona un firewall?.....	58
Tipos de firewalls.....	59
¿Por qué es importante un firewall?.....	59
ANEXO 4 Política de Control de Acceso:.....	83
ANEXO 5 Instalación Cobian:.....	86
ANEXO 6 Indicadores SGSI Heliópolis:.....	110
ANEXO 7 Matriz Riesgos Heliópolis:.....	112
ANEXO 8 Análisis de vulnerabilidades y mitigación:.....	113
1. Contraseñas en texto plano.....	120
2. Sin HTTPS (solo HTTP).....	120
3. No hay tokens o sesiones.....	120
4. las rutas sensibles no están protegidas.....	121
1) Firmar tokens:.....	121
Poblema sin JWT_SECRET (inseguro):.....	121
1. Uso de dotenv (.env) para ocultar secretos: Se movió la clave secreta JWT fuera del código y se almacenó en un archivo .env..	
122	
ANEXO 9 Monitoreo y logs:.....	136
ANEXO 10 Simulación incidente:.....	139
1. Contexto de la Organización.....	139

2. Descripción del Incidente Simulado.....	139
3. Detalles Técnicos de la Vulnerabilidad:.....	140
5. Conclusión:.....	140
13. Bibliografía y Referencias:.....	141
• International Organization for Standardization. (2022). ISO/IEC 27001:2022:.....	141
• International Organization for Standardization. (2022). ISO/IEC 27002:2022:.....	141
• Congreso de la República de Colombia. (2012). Ley 1581 de 2012:.....	141
• Consejo Nacional de Operación. (2025). Acuerdo CNO 1960 del SIN:.....	141
• North American Electric Reliability Corporation (NERC), NERC-CIP Standards:....	141
• MAGERIT v3.0, Metodología oficial:.....	142
• Archivos técnicos y manuales:.....	142

GLOSARIO:

Glosario de Términos de Seguridad de la Información

A

- **Amenaza:** Cualquier circunstancia o evento con el potencial de causar daño a un activo o a la propia organización. Puede ser intencional o accidental, interna o externa.
- **Análisis de Riesgos:** Proceso sistemático para identificar, evaluar y comprender los riesgos para la seguridad de la información.
- **Antimalware/Antivirus:** Software diseñado para detectar, prevenir y eliminar software malicioso (malware) como virus, troyanos, gusanos, etc.
- **Autenticación:** Proceso de verificar la identidad de un usuario, sistema o entidad.
- **Autorización:** Proceso de otorgar o denegar permiso a un usuario autenticado para acceder a un recurso o realizar una acción específica.
- **Auditoría de Seguridad:** Examen sistemático e independiente para determinar si las actividades y resultados relacionados con la seguridad cumplen con las disposiciones planificadas, son implementados eficazmente y son adecuados para alcanzar los objetivos.
- **Activo de Información:** Cualquier información o sistema relacionado con el procesamiento de información que tiene valor para la organización. Puede ser datos, software, hardware, redes, personal, documentación, etc.

B

- **Backdoor (Puerta Trasera):** Método secreto para eludir la autenticación normal o el cifrado en un producto, sistema operativo o aplicación.
- **Backup (Copia de Seguridad):** Copia de datos o archivos para que puedan ser recuperados en caso de pérdida o corrupción de los datos originales.
- **Brecha de Seguridad:** Incidente de seguridad que resulta en la destrucción, pérdida, alteración, divulgación no autorizada o acceso no autorizado a información transmitida, almacenada o procesada.
- **Brute Force Attack (Ataque de Fuerza Bruta):** Intento sistemático de adivinar una contraseña o clave probando todas las combinaciones posibles hasta encontrar la correcta.

C

- **Cifrado (Encriptación):** Proceso de transformar información en un código para prevenir el acceso no autorizado.
- **Confidencialidad:** Propiedad de la información de no ser puesta a disposición o divulgada a individuos, entidades o procesos no autorizados.
- **Concientización en Seguridad:** Proceso continuo de educar a los empleados sobre los riesgos de seguridad y las mejores prácticas para proteger la información.
- **Control de Acceso:** Medidas técnicas y administrativas que regulan quién o qué puede ver o usar un recurso en un entorno de TI. Puede ser físico o lógico.
- **Controles de Seguridad:** Medidas o salvaguardas que se implementan para reducir un riesgo de seguridad de la información. Pueden ser preventivos, detectivos o correctivos.

D

- **Defensa en Profundidad:** Estrategia de seguridad que implica implementar múltiples capas de controles de seguridad para proteger los activos, de modo que si una capa falla, otras capas pueden proteger el sistema.
- **Disponibilidad:** Propiedad de estar accesible y utilizable bajo demanda por una entidad autorizada.
- **DMZ (Demilitarized Zone - Zona Desmilitarizada):** Red perimetral que se interpone entre una red interna (LAN) y una red externa (Internet), actuando como una zona de seguridad para servidores públicos.

E

- **Educación en Seguridad:** Formación más profunda y estructurada sobre principios y prácticas de seguridad, a diferencia de la concientización.
- **Ethical Hacking (Hacking Ético):** Uso de técnicas de hacking para probar la seguridad de un sistema o red, con el permiso del propietario, para identificar vulnerabilidades.
- **Explotar (Exploit):** Pieza de software, datos o secuencia de comandos que aprovecha una vulnerabilidad para causar un comportamiento inesperado o no deseado en el software, hardware o algo electrónico.

F

- **Falla de Seguridad:** "Brecha de Seguridad".
- **Firewall (Cortafuegos):** Dispositivo de seguridad de red que monitorea y filtra el tráfico de red entrante y saliente basándose en un conjunto definido de reglas de seguridad.

G

- **Gestión de Incidentes:** Proceso de identificar, analizar, priorizar, resolver y documentar incidentes de seguridad de la información.
- **Gestión de Riesgos:** Proceso general de identificación, análisis, evaluación, tratamiento y monitoreo de riesgos.

I

- **Identificación:** Proceso de afirmar una identidad (por ejemplo, nombre de usuario).
- **Incidente de Seguridad:** Evento inesperado que podría comprometer la confidencialidad, integridad o disponibilidad de la información.
- **Integridad:** Propiedad de salvaguardar la exactitud y completitud de los activos.

L

- **Logging (Registro de Eventos):** Proceso de grabar eventos relevantes del sistema o la aplicación para su posterior análisis y auditoría.

M

- **Malware (Software Malicioso):** Término general para cualquier software diseñado para dañar, interrumpir o obtener acceso no autorizado a un sistema informático. Incluye virus, gusanos, troyanos, ransomware, spyware, etc.
- **Métrica de Seguridad:** Medida cuantitativa o cualitativa del estado de la seguridad de la información.
- **Monitoreo de Seguridad:** Supervisión continua de los sistemas y redes para detectar actividades sospechosas o maliciosas.

N

- **Normativa (Regulación):** Leyes, reglas o estándares que una organización debe cumplir en relación con la seguridad de la información (ej. GDPR, HIPAA, Ley de Protección de Datos).

P

- **Parche de Seguridad:** Actualización de software diseñada para corregir una vulnerabilidad o defecto de seguridad.
- **Pentesting (Prueba de Penetración):** Ver "Ethical Hacking". Un ataque simulado a un sistema informático para encontrar debilidades de seguridad, que un atacante podría explotar.
- **Phishing:** Intento de obtener información sensible como nombres de usuario, contraseñas y detalles de tarjetas de crédito (y a veces dinero) haciéndose pasar por una entidad de confianza en una comunicación electrónica.
- **Política de Seguridad de la Información (PSI):** Conjunto de reglas, directrices y procedimientos que rigen cómo se gestiona la seguridad de la información dentro de una organización.
- **Privacidad:** Derecho de los individuos a controlar cómo se recopila, usa y comparte su información personal.
- **Protocolo Seguro:** Conjunto de reglas para la comunicación que incluyen mecanismos de seguridad (ej. HTTPS, SSH, SFTP).

R

- **Ransomware:** Tipo de malware que cifra los archivos de una víctima y exige un rescate a cambio de la clave de descifrado.
- **Respuesta a Incidentes:** Conjunto de procedimientos para manejar incidentes de seguridad desde su detección hasta su resolución y análisis post-incidente.
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos. En seguridad, es la probabilidad de que una amenaza explote una vulnerabilidad, causando un impacto negativo.
- **Riesgo Residual:** El riesgo que permanece después de que se hayan implementado los controles de seguridad.

S

- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además de otras propiedades como la autenticidad, responsabilidad, no repudio y fiabilidad.

- **SIEM (Security Information and Event Management):** Sistema que recopila, normaliza, correlaciona y analiza registros de eventos de seguridad de diversas fuentes para proporcionar una visión consolidada del estado de seguridad.
- **Sistemas de Gestión de Seguridad de la Información (SGSI/ISMS):** Marco de políticas y procedimientos para gestionar los riesgos de seguridad de la información de una organización (ej. ISO 27001).
- **Spoofing:** Creación de una suplantación, especialmente de una dirección IP o de correo electrónico, para engañar a un sistema o usuario.
- **SQL Injection:** Técnica de inyección de código que explota una vulnerabilidad en una aplicación para ejecutar sentencias SQL maliciosas en una base de datos.
- **SSH (Secure Shell):** Protocolo de red criptográfica que permite la operación segura de servicios de red sobre una red no segura.
- **SSL/TLS (Secure Sockets Layer/Transport Layer Security):** Protocolos criptográficos que proporcionan seguridad de las comunicaciones a través de una red informática.

T

- **Troyano:** Tipo de malware que se disfraza como software legítimo, engañando a los usuarios para que lo instalen. Una vez ejecutado, realiza acciones maliciosas sin el conocimiento del usuario.
- **Token:** Pequeño dispositivo de hardware o software que genera un código único para la autenticación, a menudo utilizado en la autenticación de dos factores.

U

- **URL (Uniform Resource Locator):** Dirección web.
- **Usuario Privilegiado:** Usuario con derechos de acceso elevados a sistemas o datos, como administradores.

V

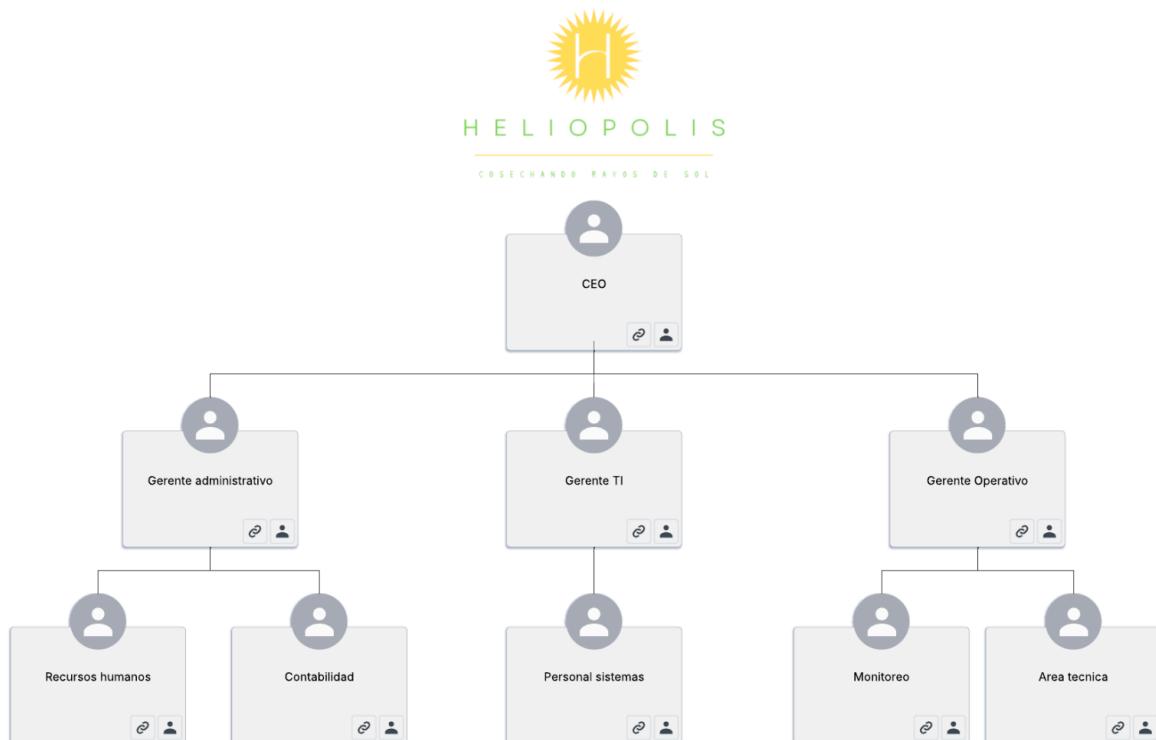
- **Vulnerabilidad:** Debilidad en un sistema, proceso o diseño que podría ser explotada por una amenaza.
 - **Virus:** Tipo de malware que se adjunta a otro programa o archivo y se propaga cuando ese programa o archivo es ejecutado por un usuario.
-

2. Introducción

Contexto del proyecto:

HELIÓPOLIS es una empresa innovadora dedicada a la comercialización de energía limpia y renovable, atendiendo principalmente a EPM, CHEC y ELECTRO CARIBE. Este informe desarrolla el proyecto AEGIS TESSERACT, orientado a la planificación e implementación de un SGSI siguiendo ISO/IEC 27001 e incluyendo controles ajustados al sector energético colombiano. El foco principal es asegurar la confidencialidad, integridad y disponibilidad de todos los activos informáticos y estratégicos, mitigando riesgos asociados a la operación crítica y cumplimiento normativo.

Organigrama:



Justificación:

En el contexto actual de transformación digital y transición energética, las empresas que ofrecen distribución de energía solar y servicios de gestión energética enfrentan una creciente exposición a amenazas cibernéticas. Estos sectores dependen cada vez más de infraestructuras digitales, sensores IoT, sistemas SCADA, redes inteligentes (smart grids) y plataformas de monitoreo remoto, lo que amplía notablemente su superficie de ataque.

La implementación de **estrategias de ciberseguridad sólidas** en este tipo de organizaciones tiene un impacto crítico en varios niveles:

1. Protección de Infraestructura Crítica:

La generación, almacenamiento y distribución de energía solar se apoya en infraestructuras que, si se ven comprometidas, podrían causar interrupciones en el suministro, afectando a clientes residenciales, comerciales e industriales. Un ciberataque dirigido podría provocar sabotajes operativos, apagones o incluso dañar físicamente equipos mediante sobrecargas o manipulaciones de sistemas automatizados.

2. Confidencialidad y seguridad de los datos:

Las empresas de gestión energética recopilan y analizan grandes volúmenes de datos de consumo, eficiencia y comportamiento de los usuarios. La falta de medidas de ciberseguridad adecuadas podría derivar en **violaciones de privacidad**, robo de datos sensibles, o suplantación de identidad digital, afectando la confianza de los clientes y generando consecuencias legales y reputacionales.

3. Prevención de ciberataques avanzados (APT, ransomware, etc.):

Dada su importancia estratégica, estas organizaciones son objetivos potenciales de ataques persistentes avanzados (APT), ataques con motivación financiera (ransomware), o incluso de ciberterrorismo. Asegurar sus activos digitales es crucial para mantener la integridad, disponibilidad y continuidad del servicio.

4. Cumplimiento normativo y reputación empresarial:

La implementación de políticas de ciberseguridad demuestra el cumplimiento de estándares internacionales como ISO 27001, NERC CIP **North American Electric Reliability Corporation** (Corporación de Confiabilidad Eléctrica de Norteamérica) o la IEC 62443 **International Electrotechnical Commission** (Comisión Electrotécnica Internacional) y fortalecer la imagen de la empresa como un proveedor confiable. Esto no solo reduce el riesgo de sanciones legales, sino que también se traduce en una **ventaja competitiva** en un mercado cada vez más consciente de los riesgos tecnológicos.

Objetivos generales y específicos:

Objetivo General:

Implementar un plan integral de ciberseguridad que permita proteger los activos digitales, operativos y de información de una empresa dedicada a la distribución de energía solar y servicios de gestión energética, garantizando la continuidad del servicio, la protección de los datos y la resiliencia ante amenazas ciberneticas.

Objetivos Específicos:

1. **Analizar la infraestructura tecnológica actual** de la empresa para identificar vulnerabilidades en sus sistemas de información, redes, plataformas de monitoreo energético.
2. **Evaluar los riesgos ciberneticos** asociados al sector energético, considerando amenazas específicas como ataques a sistemas SCADA, interrupciones de servicio, ransomware y robo de datos.
3. **Diseñar e implementar políticas de seguridad informática**, incluyendo control de accesos, cifrado de datos, segmentación de red, y mecanismos de autenticación y monitoreo.
4. **Establecer un protocolo de respuesta ante incidentes ciberneticos**, que incluya detección, contención, recuperación y notificación ante posibles ataques.

5. **Fomentar una cultura de ciberseguridad** dentro de la organización, mediante programas de capacitación y concientización para empleados sobre buenas prácticas digitales.
6. **Garantizar el cumplimiento normativo** con estándares y marcos de referencia aplicables (como ISO 27001, NIST o IEC 62443), asegurando la conformidad con los requisitos legales y sectoriales.
7. **Evaluar y probar periódicamente** la efectividad del plan de ciberseguridad a través de auditorías, simulacros de ataque (pentesting) y análisis forense en caso de incidentes.

Alcance del Entorno Simulado:

El entorno simulado de este proyecto busca representar de manera realista la infraestructura tecnológica de una empresa dedicada a la distribución de energía solar y servicios de gestión energética. A través de esta simulación, se evaluarán y aplicarán medidas de ciberseguridad que permitan identificar, mitigar y prevenir amenazas que podrían comprometer la integridad, disponibilidad y confidencialidad de los sistemas críticos.

El alcance del entorno incluye:

- **Simulación de una red corporativa segmentada**, que refleja las distintas áreas operativas de la empresa (administrativa, técnica, control de energía, atención al cliente).
- **Modelado de un sistema SCADA básico**, encargado del monitoreo y control de los dispositivos de distribución de energía solar (inversores, sensores, paneles).
- **Configuración de un servidor web de gestión energética**, donde se centraliza el acceso a datos de consumo, reportes y herramientas de análisis energético.
- **Emulación de ataques comunes** (escaneo de puertos, ataques MITM, inyecciones, ransomware y acceso no autorizado), con el fin de validar las políticas de seguridad implementadas.

- **Implementación de medidas defensivas** como firewalls, VPNs, autenticación multifactor, segmentación de red, cifrado de datos y gestión de usuarios.
- **Simulación de procedimientos de respuesta ante incidentes**, incluyendo detección, contención, análisis forense y recuperación de sistemas.

El entorno simulado se desarrollará utilizando herramientas de ciberseguridad como **Kali Linux**, **Wireshark**, **Nmap**, **Snort**, **Metasploit**, **pfSense** y **GNS3**, permitiendo una aproximación práctica y técnica al proceso de aseguramiento de una infraestructura crítica energética.

3. Marco Conceptual y Normativo

HELIOPOLIS comercializa energía generada en granjas solares y opera un portal web donde sus clientes monitorean y gestionan su consumo energético. Entre los principales riesgos para la continuidad y la reputación empresarial se encuentran:

- Pérdida de acceso al portal por clientes principales, con consecuencias operativas considerablemente graves.
- Manipulación o alteración de la información de monitoreo (impacto legal y reputacional).
- Vulnerabilidades actuales: usuarios compartidos por áreas, servidor único sin segmentación, ausencia de jerarquía y rotación de contraseñas, y carencia de controles de acceso adecuados, contraseñas sin ningún método de encriptación, falta de seguridad en la programación de la página web.

La gestión del SGSI se fundamenta en estándares internacionales, buenas prácticas y regulaciones colombianas, entre ellas:

- **Ley 1581 de 2012 (Protección de datos personales):**

Asegura el tratamiento adecuado de datos sensibles bajo principios de finalidad, libertad, veracidad, transparencia, acceso, circulación restringida, seguridad y confidencialidad, aplicables en todos los procesos con clientes y operaciones internas.

- Acuerdo CNO (Consejo Nacional de Operaciones) 1960 del 2025 para el SIN (Sistema Nacional Integrado):
Considera a HELIÓPOLIS infraestructura crítica cibernetica prioritaria. Exige controles alineados a NERC-CIP: segmentación, autenticación, monitoreo, gestión de incidentes, recuperación y reporte periódico ante autoridades eléctricas.
 - Implicaciones sectoriales:
HELIÓPOLIS debe incorporar controles de continuidad, resiliencia, monitoreo y protección de datos críticos, incluyendo procedimientos para recuperación y reacción ante incidentes, minimizando impactos económicos y sociales.
 - Referentes internacionales:
La arquitectura del SGSI integra los requisitos de ISO/IEC 27001, ISO/IEC 27002 y controles NERC-CIP, asegurando compatibilidad regulatoria y efectividad operativa.
-

4. Configuración del Entorno Virtual (Inseguro)

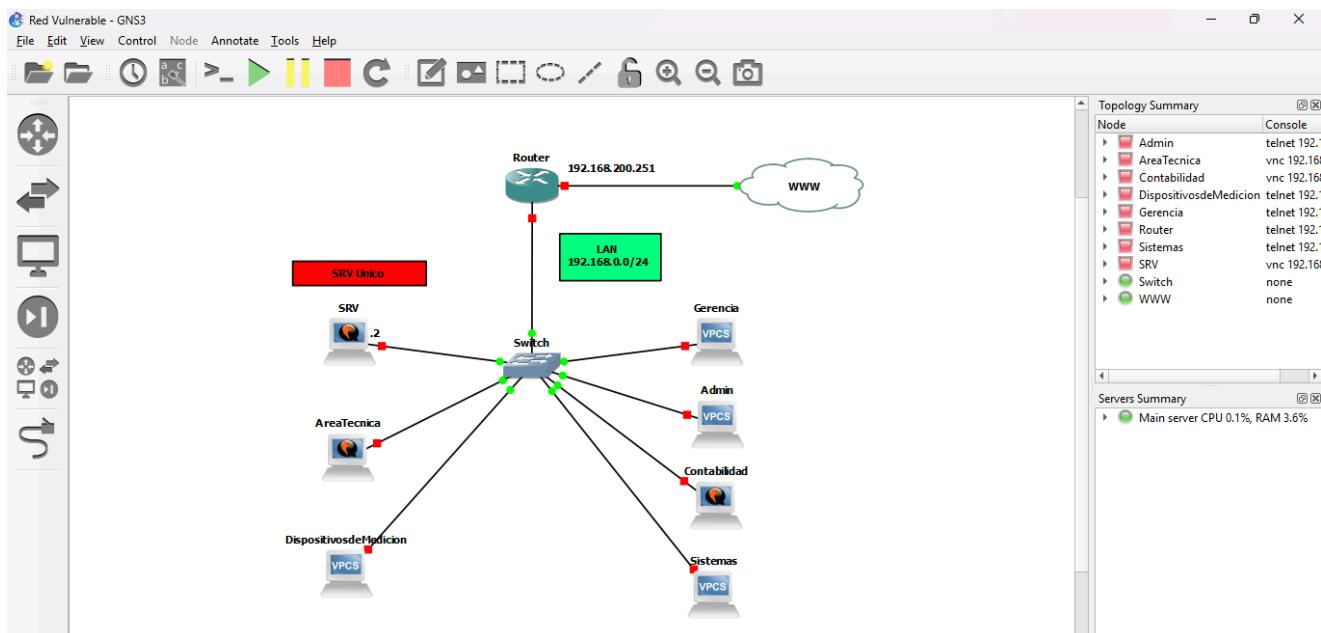
- Tabla de IPs (red insegura):

Heliópolis Red inicial.	
ISP	192.168.200.0/24
Router WAN	192.168.200.251
Router LAN	192.168.0.0/24
LAN	192.168.0.0/24 DHCP
SRV	192.168.0.2/24

- Configuración:

Proxmox, GNS3, MikroTik, servidor en Ubuntu Server GUI ,Kali Linux.

El entorno virtualizado se implementó con un equipo físico con un Hipervisor llamado Proxmox en el cual instalamos GNS3 Server y a su vez el cliente lo instalamos en otra máquina la cual usamos para administrar la topología.



- Herramientas utilizadas:

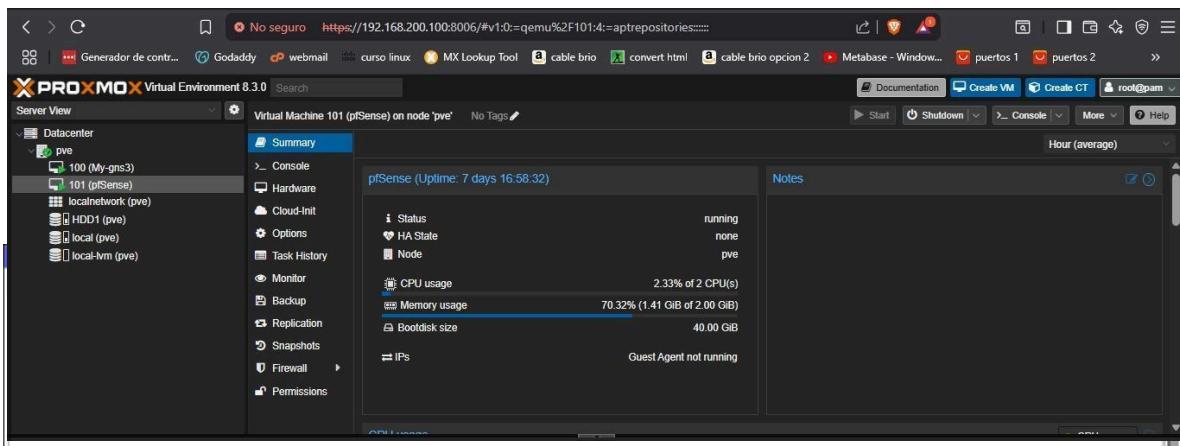
Nmap, Zenmap, Metasploit, Burp Suite, Nessus Essentials, Wireshark.

- Topología y segmentación:

Una única red, router, servidor unificado sin ninguna segmentación.

- Configuración y evidencias:

Configuración Proxmox:



Véase [ANEXO 1 \(Instalación Hipervisor\).](#)

Configuración Firewall Mikrotik:

Véase [ANEXO 2 \(instalación Firewall Mikrotik\).](#)

4.1. Configuración del Entorno Virtual (Segura)

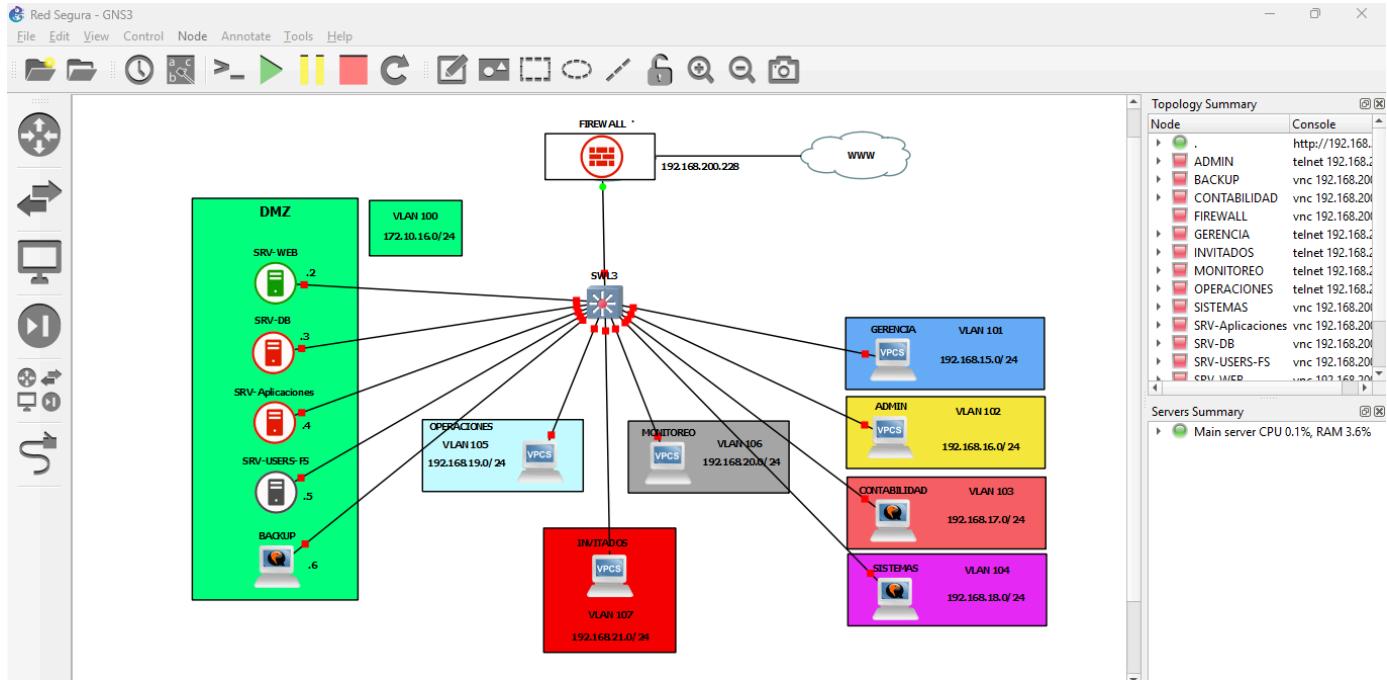
- Tabla de IPs (red segura):

Heliopolis Red Final.	
WAN	192.168.200.0/24
Firewall WAN	192.168.200.228
Firewall LAN	192.168.50.0/24
VLAN 100 DMZ	172.10.16.0/24
VLAN 101 Gerencia	192.168.15.0/24
VLAN 102 Admin	192.168.16.0/24
VLAN 103 Contabilidad	192.168.17.0/24
VLAN 104 Sistemas	192.168.18.0/24
VLAN 105 Operaciones	192.168.19.0/24
VLAN 106 Monitoreo	192.168.20.0/24
VLAN 107 Invitados	192.168.21.0/24

- Configuración:

Proxmox, GNS3, Pfsense, servidor en Ubuntu Server no GUI , Windows server, Windows 10, Kali Linux.

Para la implementación se usó el mismo servidor GNS3 para administrar las máquinas virtuales.



- Herramientas utilizadas:

Nmap, Zenmap, Metasploit, Burp Suite, Nessus Essentials, Wireshark.

- Topología y segmentación:

Firewalls, Switch capa 3, Vlans, servidores independientes.

- Configuración y evidencias:

Configuración de VLANS en Firewall (pfSense):

Interfaces		
WAN	↑ 10Gbase-T <full-duplex>	192.168.200.228
LAN	↑ 10Gbase-T <full-duplex>	192.168.50.1
VLAN100DMZ	↑ 10Gbase-T <full-duplex>	172.10.16.1
VLAN101GERENCIA	↑ 10Gbase-T <full-duplex>	192.168.15.1
VLAN102ADMIN	↑ 10Gbase-T <full-duplex>	192.168.16.1
VLAN103CONTABILIDAD	↑ 10Gbase-T <full-duplex>	192.168.17.1
VLAN104SISTEMAS	↑ 10Gbase-T <full-duplex>	192.168.18.1
VLAN105OPERACIONES	↑ 10Gbase-T <full-duplex>	192.168.19.1
VLAN106MONITOREO	↑ 10Gbase-T <full-duplex>	192.168.20.1
VLAN107INVITADOS	↑ 10Gbase-T <full-duplex>	192.168.21.1

VLANS Firewall

En la anterior imagen se puede observar todas las interfaces de las VLAN ya configuradas con sus respectivas IPs.

Configuración Proxmox:

The screenshot shows the Proxmox interface with the following details:

- Server View:** Datacenter > pve > 101 (pfSense)
- Virtual Machine 101 (pfSense) on node 'pve':**
 - Status:** running
 - HA State:** none
 - Node:** pve
 - CPU usage:** 2.33% of 2 CPU(s)
 - Memory usage:** 70.32% (1.41 GB of 2.00 GB)
 - Bootdisk size:** 40.00 GB
 - IPs:** Guest Agent not running
- Notes:** Hour (average)

Véase [ANEXO 1 \(Instalación Hipervisor\).](#)

Configuración PfSense:

The screenshot shows the pfSense dashboard with the following sections:

- Status / Dashboard:**
 - System Information:**
 - Name: fw.heli.local
 - User: admin@192.168.10.28 (Local Database)
 - System: QEMU Guest
Netgate Device ID: f3f48c2f475002330fdcc
 - BIOS: Vendor: Seabios
Version: rcl-1.16.3-0-ga6ed6b701fa-prebuilt.qemu.org
Release Date: Tue Apr 1 2014
 - Version: 2.7.2-RELEASE (amd64)
built on Tue Mar 5 05:53:00 +05 2024
FreeBSD 14.0-CURRENT
 - CPU Type: QEMU Virtual CPU version 2.5+
2 CPUs, 1 package(s) x 2 core(s)
AES-NI CPU Crypto: Yes (inactive)
QAT Crypto: No
 - Hardware crypto: Inactive
 - Kernel PTI: Enabled
 - MDS Mitigation: Inactive
 - Uptime: 4 Days 16 Hours 17 Minutes 03 Seconds
 - Netgate Services And Support:**
 - Contract type: Community Support
Community Support Only
 - NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
 - If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.
 - You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.
 - Upgrade Your Support
• Community Support Resources
 - Netgate Global Support FAQ
• Official pfSense Training by Netgate
 - Netgate Professional Services
• Visit Netgate.com
 - Interfaces:**

Interface	Description	IP Address
WAN	10Gbase-T <full-duplex>	192.168.200.228
LAN	10Gbase-T <full-duplex>	192.168.50.1
VLAN100DMZ	10Gbase-T <full-duplex>	172.10.16.1
VLAN101GERENCIA	10Gbase-T <full-duplex>	192.168.15.1
VLAN102ADMIN	10Gbase-T <full-duplex>	192.168.16.1
VLAN103CONTABILIDAD	10Gbase-T <full-duplex>	192.168.17.1
VLAN104SISTEMAS	10Gbase-T <full-duplex>	192.168.18.1
VLAN105OPERACIONES	10Gbase-T <full-duplex>	192.168.19.1
VLAN106MONITOREO	10Gbase-T <full-duplex>	192.168.20.1
VLAN107INVITADOS	10Gbase-T <full-duplex>	192.168.21.1
 - Traffic Graphs:**

WAN

wan (in) wan (out)

Graph showing WAN traffic over time, with peaks around 20k, 40k, and 60k bytes.

Véase [ANEXO 3 \(Instalación Firewall PfSense\).](#)

VLANS SWITCH:

VLAN	Name	Status	Ports
1	default	active	Gi3/1, Gi3/2
99	DMZ	active	Gi0/1, Gi0/2, Gi0/3, Gi1/0
101	Gerencia	active	Gi1/1
102	Admin	active	Gi1/2
103	Contabilidad	active	Gi1/3
104	Sistemas	active	Gi2/0
105	Operaciones	active	Gi2/1
106	Monitoreo	active	Gi2/2
107	Invitados	active	Gi2/3
200	VLAN0200	active	Gi3/0
300	VLAN0300	active	
1002	fddi-default	act/unsup	
1003	trcrf-default	act/unsup	
1004	fdnet-default	act/unsup	
1005	trbrf-default	act/unsup	

En la anterior imagen podemos observar las interfaces asignadas a su respectiva VLAN.

5. Diseño de la Red Corporativa

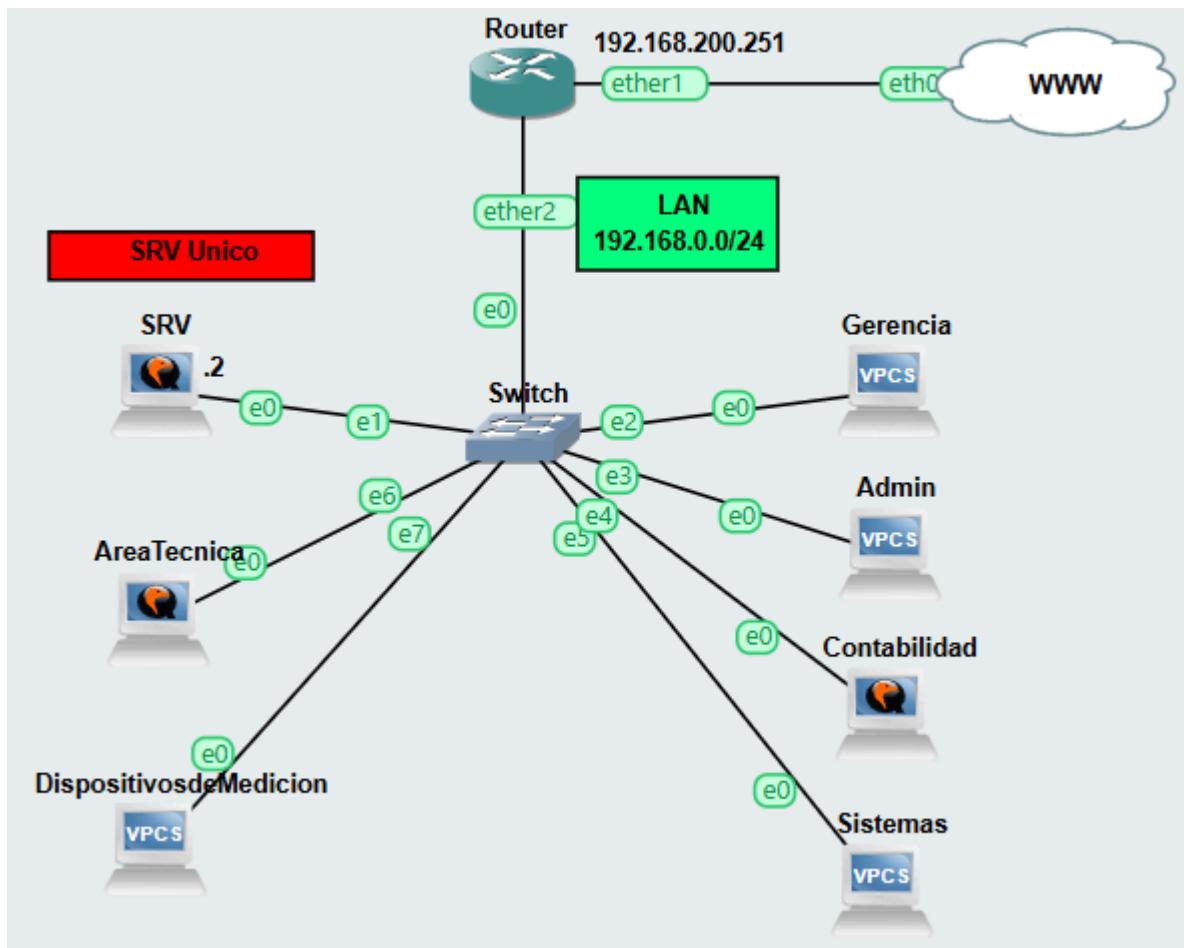
- Estructura simulada:

La empresa está dividida en 8 segmentos, los cuales son:

DMZ, Gerencia, administración, contabilidad, sistemas, operaciones, monitoreo, invitados.

- Topologías:

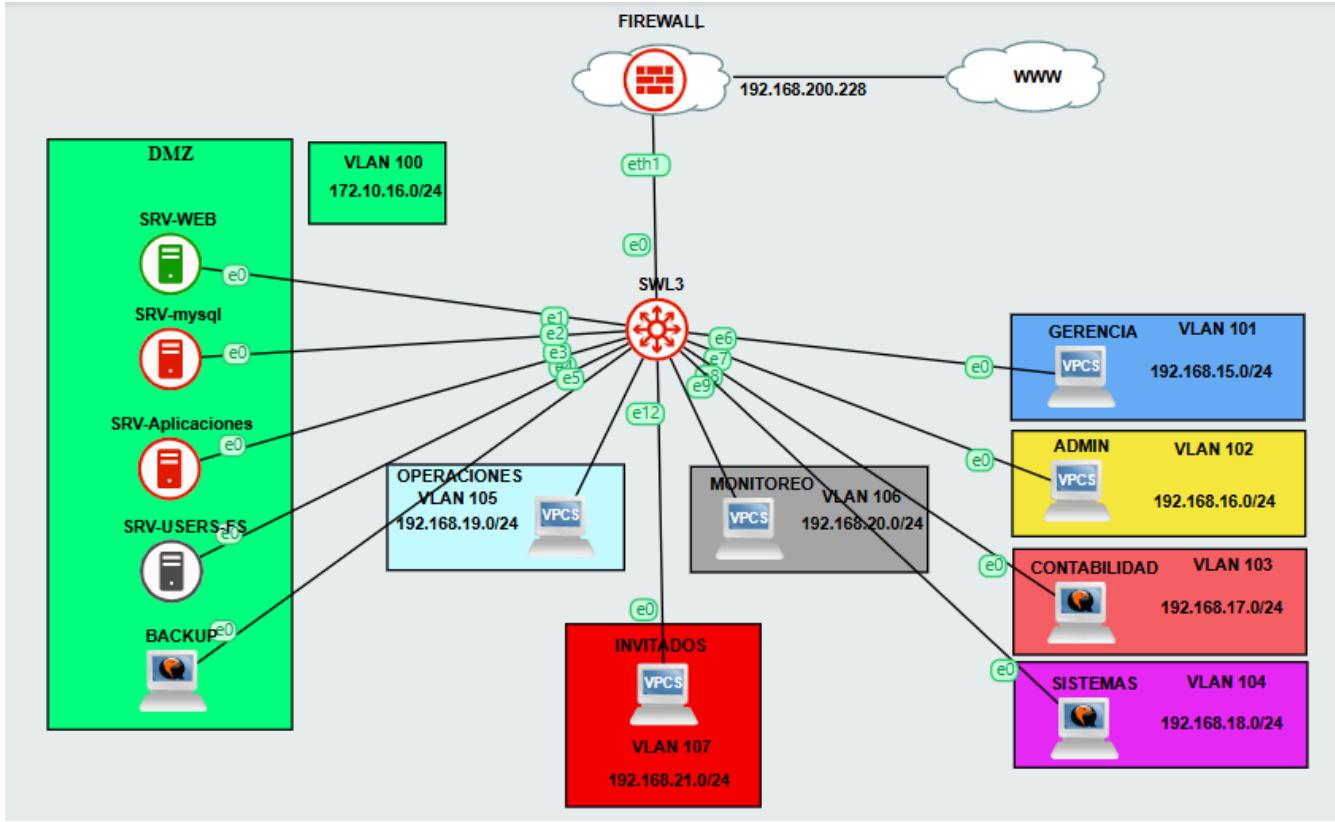
Red inicial:



Red insegura.

Como se puede ver en la topología inicial de la empresa, no había segmentación, tenían una red LAN general en la cual se le tenía una IP fija asignada únicamente al servidor, por lo tanto, con el hecho de que vulneren cualquier dispositivo tendrían fácil acceso a los demás sistemas de la red.

Red Final:



Red segura.

En esta red se puede observar que ya todo está segmentado por procesos con la ayuda de VLANS y se crea una parte (DMZ) donde se divide el único servidor que se tenía en 4 servidores diferentes para no tener todo centralizado y mitigar riesgos.

- Seguridad lógica:

Políticas de ACLs (Access Control List), segmentación, roles y jerarquización.

- ❖ Que toda la red tenga comunicación a ICMP **Internet Control Message Protocol** (Protocolo de Mensajes de Control de Internet) “PING”.

The screenshot shows the pfSense Firewall Rules configuration. The WAN tab is selected. There are three rules listed:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/5 KiB	IPv4 ICMP any	*	*	*	*	*	none		Aceptar ping ✓	
1/12.41 MiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		Aceptar conexiones seguras desde la wan	
2/609.11 MiB	IPv4 *	*	*	*	*	*	none		permitir conexiones fuera de wan	

Buttons at the bottom include: Add, Add, Delete, Toggle, Copy, Save, and Separator.

Regla aceptar ping Pfsense.

- ❖ Que sólo la VLAN del área de SISTEMAS tenga acceso al puerto 443 (servicio HTTPS Hypertext Transfer Protocol Secure) del servidor web que está en el DMZ.

The screenshot shows the pfSense Firewall Rules configuration. The WAN tab is selected. There are four rules listed:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/5 KiB	IPv4 ICMP any	*	*	*	*	*	none		Aceptar ping	
2/12.55 MiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		Aceptar conexiones seguras desde la wan	
0/0 B	IPv4 TCP	VLAN104SISTEMAS subnets	*	*	443 (HTTPS)	*	none		Aceptar conexiones seguras desde Sistemas ✓	
2/613.40 MiB	IPv4 *	*	*	*	*	*	none		permitir conexiones fuera de wan	

Buttons at the bottom include: Add, Add, Delete, Toggle, Copy, Save, and Separator.

Regla acceso al puerto 443 (Area sistemas).

- ❖ Que todas las VLANS tengan acceso a internet ya que por defecto no tienen acceso a internet.

Firewall / Rules / VLAN104SISTEMAS

Floating	WAN	LAN	VLAN100DMZ	VLAN101GERENCIA	VLAN102ADMIN	VLAN103CONTABILIDAD	VLAN104SISTEMAS
VLAN105OPERACIONES	VLAN106MONITOREO	VLAN107INVITADOS					

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input checked="" type="checkbox"/>	0/1.95 GiB	IPv4 *	*	VLAN104SISTEMAS subnets	*	*	*	*	none ✓	Permitir @ vlan 104 sistemas	
<input checked="" type="checkbox"/>	0/0 B	IPv4 ICMP any	*	*	*	*	*	*	none	aceptar ping	
<input checked="" type="checkbox"/>	0/0 B	IPv4 *	*	*	*	*	*	*	none	permitir trafico red fisica	

Add Add Delete Toggle Copy Save Separator

Internet por defecto.

- ❖ Que los puertos 22 (protocolo SSH Secure Shell) de los DMZ únicamente respondan a la VLAN 104 de sistemas.

Floating WAN LAN **VLAN100DMZ** VLAN101GERENCIA VLAN102ADMIN VLAN103CONTABILIDAD VLAN104SISTEMAS

VLAN105OPERACIONES VLAN106MONITOREO VLAN107INVITADOS

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input checked="" type="checkbox"/>	0/14 Kib	IPv4 ICMP any	*	*	*	*	*	none	Aceptar Ping		
<input checked="" type="checkbox"/>	0/3.82 GiB	IPv4 *	*	VLAN100DMZ subnets	*	*	*	*	none	Permitir @ vlan 100 DMZ	
<input checked="" type="checkbox"/>	0/152 B	IPv4 *	*	*	*	*	*	*	none	Permitir desde fuera de la wan	
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	VLAN104SISTEMAS subnets	*	VLAN100DMZ subnets	22 (SSH)	*	none ✓	Permitir ssh a Sistemas		

Add Add Delete Toggle Copy Save Separator

Permitir ssh a DMZ desde sistemas.

- ❖ Que el servidor de base datos únicamente responda al servidor web, de aplicaciones y a Sistemas.

Rules (Drag to Change Order)											Actions
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/14 Kib	IPv4 ICMP	*	*	*	*	*	none		Aceptar Ping	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/3.82 GiB	IPv4 *	VLAN100DMZ subnets	*	*	*	*	none		Permitir @ vlan 100 DMZ	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/152 B	IPv4 *	*	*	*	*	*	none		Permitir desde fuera de la wan	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	VLAN104SISTEMAS subnets	*	172.10.16.3	3306	*	none		Aceptar puerto DB a Sistemas	

Add Add Delete Toggle Copy Save Separator

Aceptar puerto DB a sistemas.

Rules (Drag to Change Order)											Actions
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/14 Kib	IPv4 ICMP	*	*	*	*	*	none		Aceptar Ping	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/3.82 GiB	IPv4 *	VLAN100DMZ subnets	*	*	*	*	none		Permitir @ vlan 100 DMZ	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/152 B	IPv4 *	*	*	*	*	*	none		Permitir desde fuera de la wan	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	VLAN104SISTEMAS subnets	*	172.10.16.3	3306	*	none		Aceptar puerto DB a Sistemas	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	172.10.16.2	*	172.10.16.3	3306	*	none		Permitir DB 3306 De SRV Web	

Add Add Delete Toggle Copy Save Separator

Permitir 3306 de servidor web.

6. Políticas de Seguridad de la Información

- Control de accesos individualizado:

Creación de cuentas únicas por usuario/cliente.

Se creó un servidor active directory y controlador de dominio el cual administra todos los equipos de la red por ende todos los usuarios que van a utilizar los equipos.

Se crean los diferentes departamentos desde la administración de usuarios y equipos de Active Directory, en cada departamento se crean los usuarios respectivos que son los que podrán loguearse en los equipos. Si hay un usuario inexistente no puede hacer uso de ningún equipo de la empresa.

- **Política de contraseñas:**

Rotación periódica de contraseñas para ingresar a los equipos, requisitos de complejidad, prohibiciones de archivos de texto plano que contengan información sensible, para los correos el obligatorio el 2FA, todos los datos sensibles deben pasar por el proceso de hash al momento de registro en la aplicación.

Directiva	Configuración de directiva
Almacenar contraseñas con cifrado reversible	No está definido
Auditoría de longitud mínima de contraseña	No está definido
Exigir historial de contraseñas	2 contraseñas recordadas
La contraseña debe cumplir los requisitos de complejidad	Habilitada
Longitud mínima de la contraseña	10 caracteres
Reducir los límites de longitud mínima de la contraseña	No está definido
Vigencia máxima de la contraseña	90 días
Vigencia mínima de la contraseña	0 días

Configuración directiva para que el usuario cambie la contraseña de usuario cada 90 días, con un mínimo de caracteres de 10 caracteres.

Verificación en dos pasos

Autenticación
Aplicado de forma local

Pide a los usuarios que verifiquen su identidad cuando introduzcan su nombre de usuario y contraseña para añadir una capa de seguridad adicional a sus cuentas. [Más información](#)

Permitir a los usuarios activar la verificación en dos pasos

Implementación obligatoria

Desactivado
 Activado
 Activada desde el 

Plazo para que los nuevos usuarios se registren
Concede a los nuevos usuarios un plazo para registrarse antes de la aplicación obligatoria

1 semana ▾

Frecuencia
Los usuarios no tendrán que repetir la verificación en dos pasos cuando inicien sesión en un dispositivo de confianza. [Más información](#)

Permitir que el usuario confie en el dispositivo

Métodos
Selecciona el método que quieras aplicar de forma obligatoria. [Más información](#)

Cualquiera
 Cualquiera, excepto códigos de verificación a través de mensajes de texto o llamadas telefónicas
 Solo con llave de seguridad

Periodo de gracia de la suspensión de la política de verificación en dos pasos
Permite que los usuarios utilicen temporalmente códigos de verificación, además de sus llaves de seguridad, para iniciar sesión. El periodo de excepción de un usuario comienza cuando se generan los códigos de verificación.

1 día ▾

Configuración del panel admin del servidor de correo la verificación en 2 pasos para que sea obligatoria después de 10 días, si no se realiza el correo automáticamente se bloquea.

Véase [ANEXO 4 \(Políticas de control de acceso\)](#).

- **Respaldo y disponibilidad:**

Para los backups se implementó Cobian el cual es una herramienta gratuita que permite encriptar el archivo final y lo deja en uno solo sin fraccionar, se configura de forma que realice un backup “incremental” diario, y uno “total” semanal.

Aleatoriamente cada 15 días se realiza la revisión de los backups para verificar que no tenga ningún tipo de fallas.

Véase [ANEXO 5 \(Instalacion Cobian\)](#).

- Gestión y registro de incidentes:
Procedimiento de reporte, análisis, respuesta y lecciones aprendidas.
- Alineación a ISO/IEC 27001 y NERC-CIP.

7. Análisis de Riesgos:

Activos críticos:

- Entre los activos críticos se tiene, toda la parte de bases de datos, información del file server, información de acceso como lo son correos electrónicos y contraseñas, usuarios y contraseñas de acceso a los pcs.
- Plataforma de gestión energética, ya que la empresa presta este servicio a cambio de un pago mensual, si se pierde el acceso a la plataforma, no se podría visualizar ni administrar toda la parte de la gestión de energía.

• Principales riesgos identificados:

Inaccesibilidad al portal, manipulación de información crítica, exposición total del servidor, accesos sin restricción y sin monitoreo.

• Metodología:

Se recomienda implementar **MAGERIT** en el futuro para evaluar sistemáticamente los riesgos, aprovechar su soporte documental y priorizar el tratamiento de riesgos en segmento crítico.

• Ventajas de MAGERIT:

Rigurosidad, adaptabilidad, integración con otros marcos, y soporte para toma de decisiones estratégicas.

- Matriz de amenazas:
Véase [ANEXO 6 \(Indicadores SGSI Heliopolis\)](#) y [ANEXO 7 \(Matriz Riesgos Heliopolis\)](#).
- Vulnerabilidades y controles aplicados:
 - ❖ Contraseñas en texto plano:
 - *Control aplicado:*
Firmar tokens.
 - ❖ Sin HTTPS (solo HTTP):
 - *Control aplicado:*
Instalación de certificados SSL/TLS (certbot).
 - ❖ No hay tokens con firmas o sesiones:
 - *Control aplicado:*
Uso de dotenv (.env) para ocultar secretos.
 - ❖ las rutas sensibles no están protegidas:
 - *Control aplicado:*
middleware para rutas protegidas.

8. Pruebas de Seguridad y Evaluación Técnica

- Herramientas empleadas:
Nmap, Nessus, Zenmap, Wireshark.
- Resultados clave:
 - Servicios expuestos (HTTP, Telnet, FTP inseguros).
 - Vulnerabilidades clasificadas por criticidad (ver gráficos de Nessus/escaneos detallados).
 - Tráfico inseguro captado y documentado por Wireshark.

- Análisis:

Véase [ANEXO 8 \(Análisis de vulnerabilidades y mitigación\)](#).

9. Controles Técnicos Implementados

- Individualización y jerarquización de usuarios.
- Cambio y robustez obligatoria de contraseñas.
- Segmentación y políticas de firewall.
- Migración a protocolos seguros (SFTP, HTTPS).

- Monitoreo de logs y alertas:

Implementamos Zabbix para centralizar y optimizar el monitoreo de nuestra infraestructura y la gestión de logs. Con Zabbix, obtenemos una visibilidad completa del rendimiento de nuestros sistemas, redes y aplicaciones, lo que nos permite identificar y resolver problemas de manera proactiva, garantizando la disponibilidad y el correcto funcionamiento de nuestros servicios. Además, su capacidad para recolectar y analizar logs facilita la detección de anomalías y eventos de seguridad, mejorando nuestra capacidad de respuesta ante cualquier incidente. En resumen, Zabbix es nuestra herramienta clave para mantener la estabilidad operativa y reforzar la seguridad de nuestra empresa.

- Procedimientos de respaldo y trazabilidad.

Véase [ANEXO 9 \(Monitoreo y logs\)](#).

10. Gestión de Incidentes

- Simulación documentada de distintos escenarios de incidentes:

Véase [ANEXO 10 \(Simulación incidente\)](#).

- Respuesta y comunicación eficaz entre áreas.
- Plan de recuperación y restauración.
- Mejora continua y retroalimentación estructurada.

11. Otras Implementaciones para el SGSI.

- **Comité de Seguridad de la Información:**

Dirigido por la alta dirección, supervisa la estrategia global de seguridad y asigna los recursos necesarios.

- **Oficial de Seguridad de la Información (CISO):**

Responsable de la coordinación general del SGSI, reporta directamente a la gerencia general y lidera la implementación de controles.

- **Responsables de Proceso:**

Cada área funcional cuenta con un responsable de seguridad que implementa controles específicos y reporta al CISO.

- **Política de Control de Personas:**

Abarcan verificación de antecedentes, capacitación en seguridad, y términos de empleo. Todos los controles han sido implementados dada la criticidad del factor humano en seguridad.

- **Política de USB Cero:**

Es una política de seguridad muy estricta y radical, ya que la seguridad de la información es crítica y las fugas de datos o las infecciones por malware son inaceptables. Se tendrán algunas excepciones, pero solo dispositivos USB propiedad de la empresa, que están gestionados centralmente, cifrados y escaneados.

- **Controles Físicos:**

Incluyen perímetros de seguridad, controles de acceso físico y protección ambiental. Adaptados al centro de datos local.

- **Capacitación y Concienciación:**

El programa de capacitación y concienciación es fundamental para el éxito del SGSI. Se ha desarrollado un plan integral que incluye:

❖ **Capacitación General:**

Todos los empleados reciben formación básica sobre políticas de seguridad, manejo de información confidencial y reconocimiento de amenazas. Esta capacitación se realiza durante la inducción y se actualiza anualmente.

❖ **Capacitación Especializada:**

El personal técnico recibe entrenamiento específico en desarrollo seguro, administración de sistemas y respuesta a incidentes. Esta capacitación incluye certificaciones profesionales y actualización tecnológica continua.

❖ **Campañas de Concienciación:**

Se implementan campañas regulares sobre temas específicos como phishing, ingeniería social, políticas y uso seguro de dispositivos móviles. Estas campañas incluyen simulacros de phishing y comunicaciones internas regulares.

12. Conclusiones y Recomendaciones

En primer lugar, la implementación de las directrices y controles propuestos por el proyecto AEGIS TESSERACT sitúa a **HELIÓPOLIS como un referente de buenas prácticas en SGSI dentro del dinámico sector energético colombiano**. Este enfoque proactivo no solo busca cumplir con las normativas, sino establecer un estándar de excelencia que garantice la confidencialidad, integridad y disponibilidad de sus activos críticos, desde la operación de la granja solar hasta la gestión de la información de sus clientes.

Además, para reforzar aún más la resiliencia y la gestión estratégica de la seguridad, se recomienda **incorporar en el futuro la metodología MAGERIT**. Esta metodología, reconocida por su enfoque sistemático en el análisis y la gestión de riesgos de seguridad de la información, permitirá a HELIÓPOLIS identificar, evaluar y tratar de manera más precisa las amenazas y vulnerabilidades específicas de su infraestructura crítica. La integración de MAGERIT facilitará un cumplimiento más robusto con las regulaciones vigentes y futuras, al proporcionar una visión clara de los riesgos y la efectividad de los controles implementados.

Por otro lado, es crucial **insistir en la obligatoriedad de la capacitación continua del personal, la revisión periódica y la actualización constante de los controles de seguridad**. El panorama de amenazas ciberneticas evoluciona rápidamente, y los requisitos regulatorios se ajustan con la misma celeridad. Por ello, es imperativo que el equipo de HELIÓPOLIS esté siempre al tanto de las nuevas vulnerabilidades y tácticas de ataque, y que los controles implementados sean dinámicos y adaptativos para enfrentar estos desafíos emergentes. La inversión en formación y en procesos de mejora continua será vital para mantener la eficacia del SGSI.

Finalmente, es fundamental mantener una alineación estratégica y operativa con los estándares y normativas clave que rigen la seguridad de la información y la ciberseguridad en el sector energético. Esto incluye:

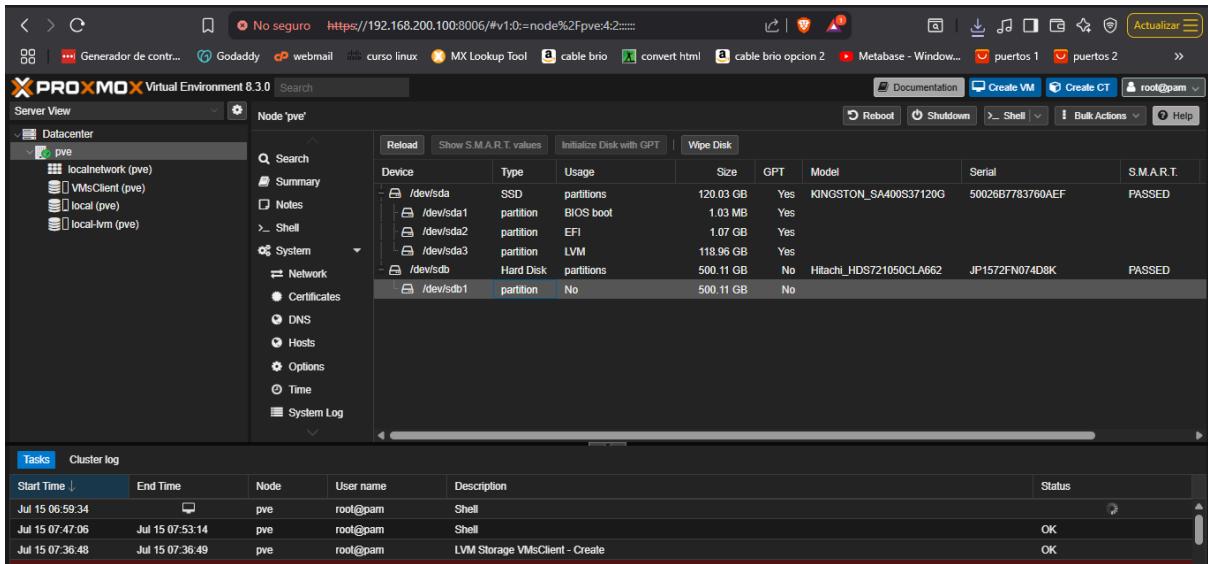
- **ISO/IEC 27001:** Para asegurar una gestión integral y certificable de la seguridad de la información.
- **NERC-CIP (Critical Infrastructure Protection):** Aunque es una normativa estadounidense, sus principios son una referencia global para la protección de infraestructuras críticas en el sector eléctrico, y su estudio puede aportar valor adicional en la protección de sistemas OT/ICS.
- **Acuerdo CNO 1960 de 2025 (o su versión más reciente) y demás directrices del CNO:** Para garantizar el cumplimiento estricto con las regulaciones específicas de ciberseguridad para los agentes del Sistema Interconectado Nacional en Colombia.
- **Ley 1581 de 2012 (Protección de Datos Personales):** Para asegurar el manejo responsable y seguro de toda la información personal de clientes, empleados y proveedores.

12. Anexos:

- [ANEXO 1 \(Instalación Hipervisor\).](#)
- [ANEXO 2 \(instalación Firewall Mikrotik\).](#)
- [ANEXO 3 \(Instalación Firewall Pfsense\).](#)
- [ANEXO 4 \(Políticas de control de acceso\).](#)
- [ANEXO 5 \(Instalacion Cobian\).](#)
- [ANEXO 6 \(Indicadores_SGSI_Heliopolis\).](#)
- [ANEXO 7 \(Matriz Riesgos Heliópolis\).](#)
- [ANEXO 8 \(Análisis de vulnerabilidades y mitigación\).](#)
- [ANEXO 9 \(Monitoreo y logs\).](#)
- [ANEXO 10 \(Simulación incidente\).](#)

ANEXOS

ANEXO 1 Instalación Hipervisor:



Queda la partición con el tamaño total del disco creada en proxmox.

Creamos el volumen lógico:

```
root@pve:~# pvcreate /dev/sdb1
  Physical volume "/dev/sdb1" successfully created.
root@pve:~#
```

Ahora creamos el grupo:

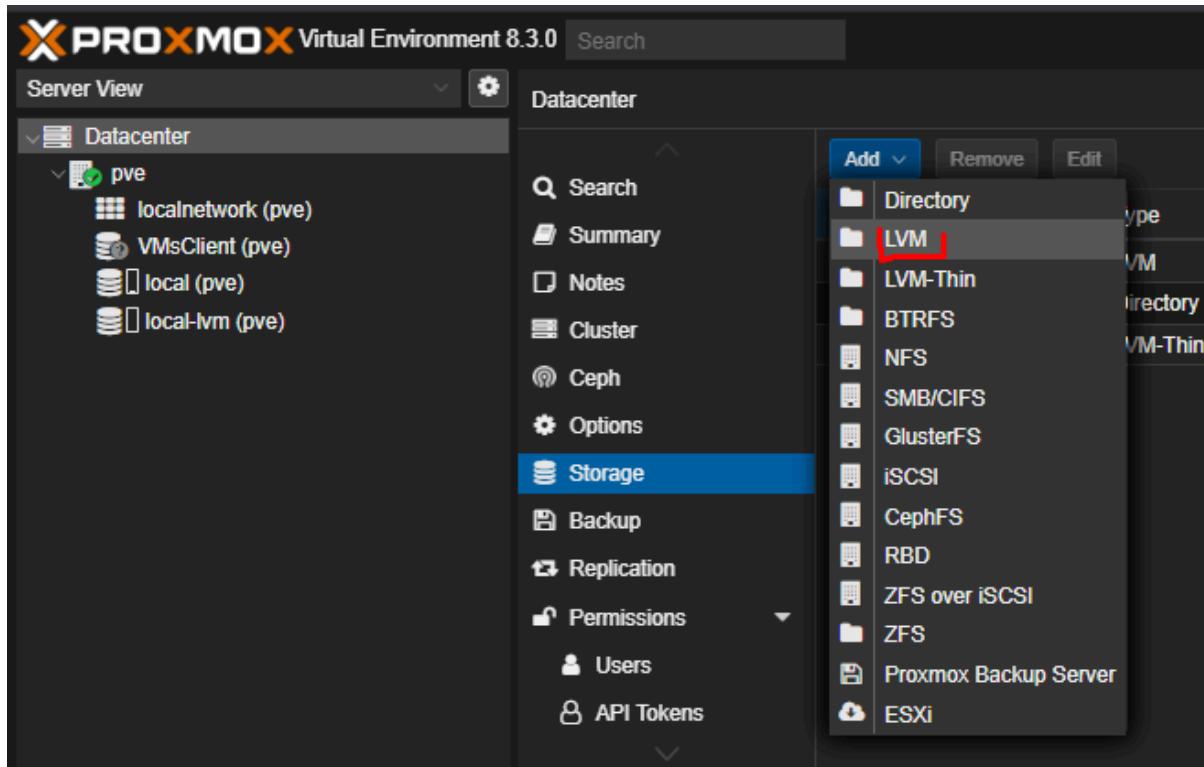
```
root@pve:~# pvcreate /dev/sdb1
Physical volume "/dev/sdb1" successfully created.
root@pve:~# vgcreate HDD01 /dev/sdb1
  Volume group "HDD01" successfully created
root@pve:~#
```

Para montar el disco vamos al panel de Proxmox

Datacenter

Storage

Agregar LVM



Nos aparece el menú de agregar nuevo LVM, en ID ponemos como referencia el mismo nombre manejado para identificar los discos, y el volumen group seleccionamos el grupo creado para este disco que es HDD1.

ID ↑	Type	Content	Path/Targe
VMsClient	LVM	Disk image, Container	
local	Directory	VZDump backup file, ISO image, Cont...	/var/lib/vz
local-lvm	l VM-Thin	Disk image, Container	

En nuestro panel nos debe aparecer el HDD montado.

Device	Type	Usage	Size	GPT	Model
/dev/sda	SSD	partitions	120.03 GB	Yes	KINGSTON_SA400S37120G
/dev/sda1	partition	BIOS boot	1.03 MB	Yes	
/dev/sda2	partition	EFI	1.07 GB	Yes	
/dev/sda3	partition	LVM	118.96 GB	Yes	
/dev/sdb	Hard Disk	partitions	500.11 GB	No	Hitachi_HDS721050CLA662
/dev/sdb1	partition	LVM	500.11 GB	No	

Ya tenemos nuestro sistema listo para crear las VMs, explicaremos la creación de una máquina y sería la guía para crear las que sean necesarias.

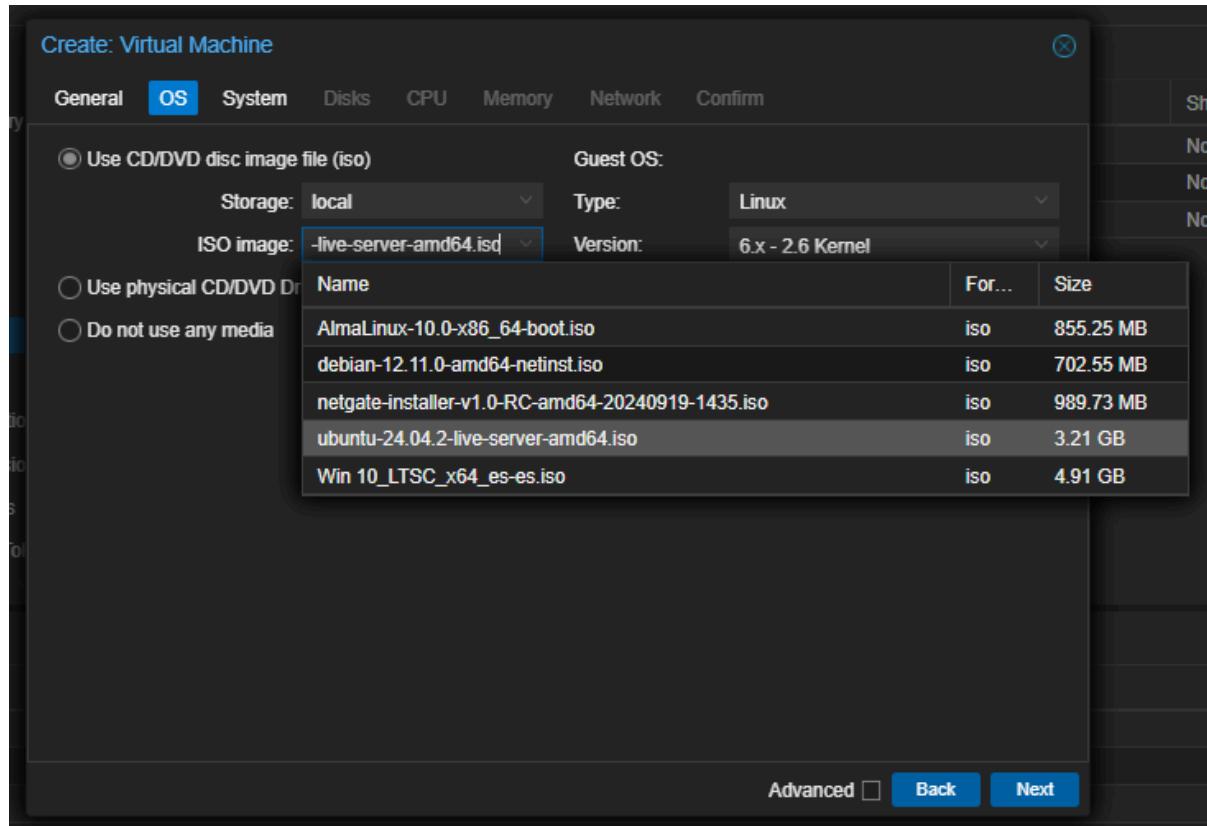
En nuestro panel seleccionamos la opción de crear VM

The screenshot shows the Proxmox VE 8.3.0 interface. At the top, there's a navigation bar with 'Documentation', 'Create VM' (which is highlighted with a red box), 'Create CT', and a user session indicator 'root@pam'. Below the navigation bar is a search bar and a 'Server View' dropdown. The main area is titled 'Datacenter' and contains a tree view under 'pve': 'localnetwork (pve)', 'HDD01 (pve)', 'local (pve)', and 'local-lvm (pve)'. To the right of the tree view is a table with columns: ID, Type, Content, Path/Target, Shared, Enabled, and Bandwidth Limit. The table lists three items: 'local-lvm' (LVM-Thin, Disk image, Container), 'local' (Directory, VZDump backup file, ISO image, Cont... /var/lib/vz), and 'HDD01' (LVM, Disk image, Container). Below the table are buttons for 'Add', 'Remove', and 'Edit'.

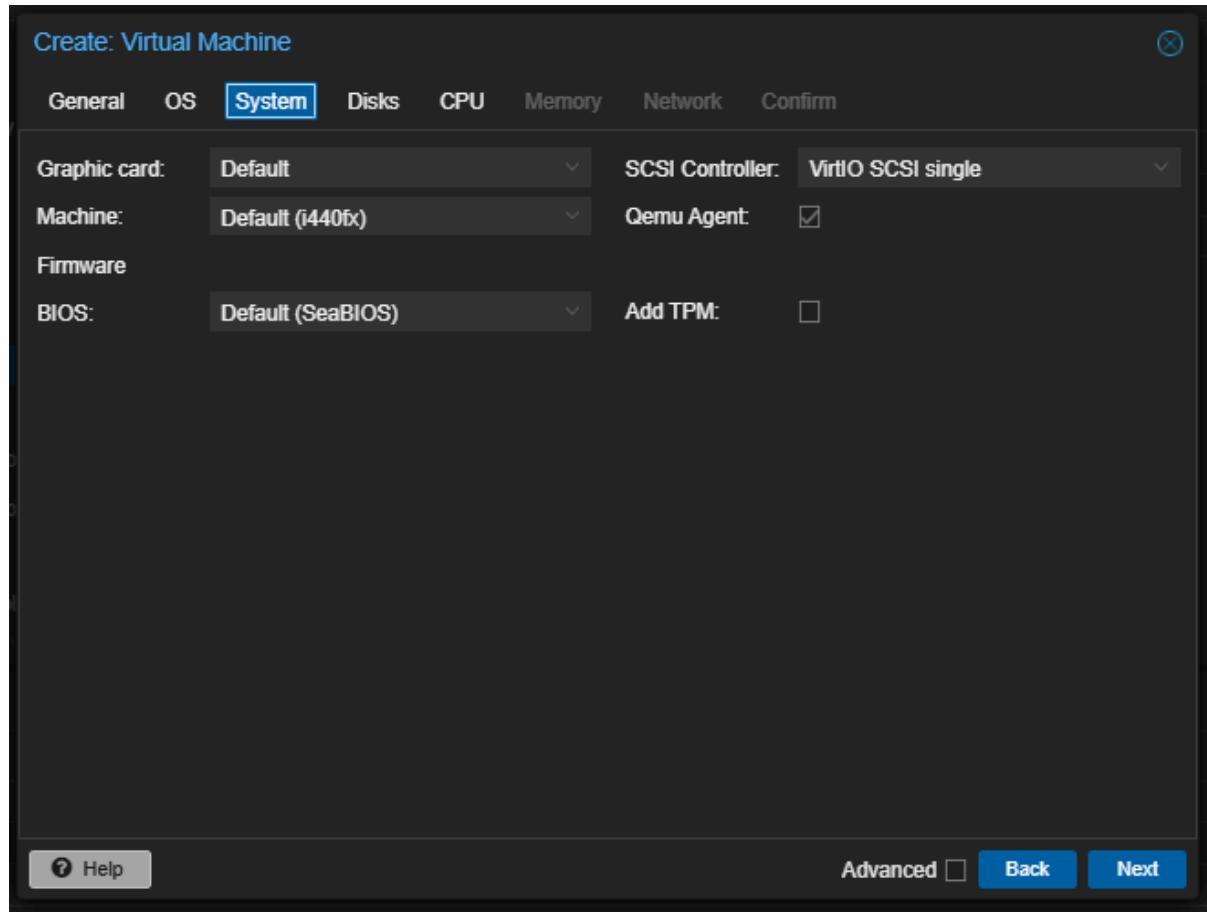
Se abre una ventana emergente e iniciamos la configuración básica, en VM ID ponemos un número para poder identificar el equipo, predeterminado inicia en 100, en Name ponemos el nombre del equipo para poder identificarlo en la red.

The screenshot shows the 'Create: Virtual Machine' dialog box. The 'General' tab is selected. On the left, there are input fields for 'Node' (set to 'pve'), 'VM ID' (set to '100' with a red checkmark), and 'Name' (set to 'SRV0' with a red checkmark). On the right, there is a 'Resource Pool' dropdown menu. At the bottom of the dialog are buttons for '? Help', 'Advanced' (with a checkbox), 'Back', and 'Next'.

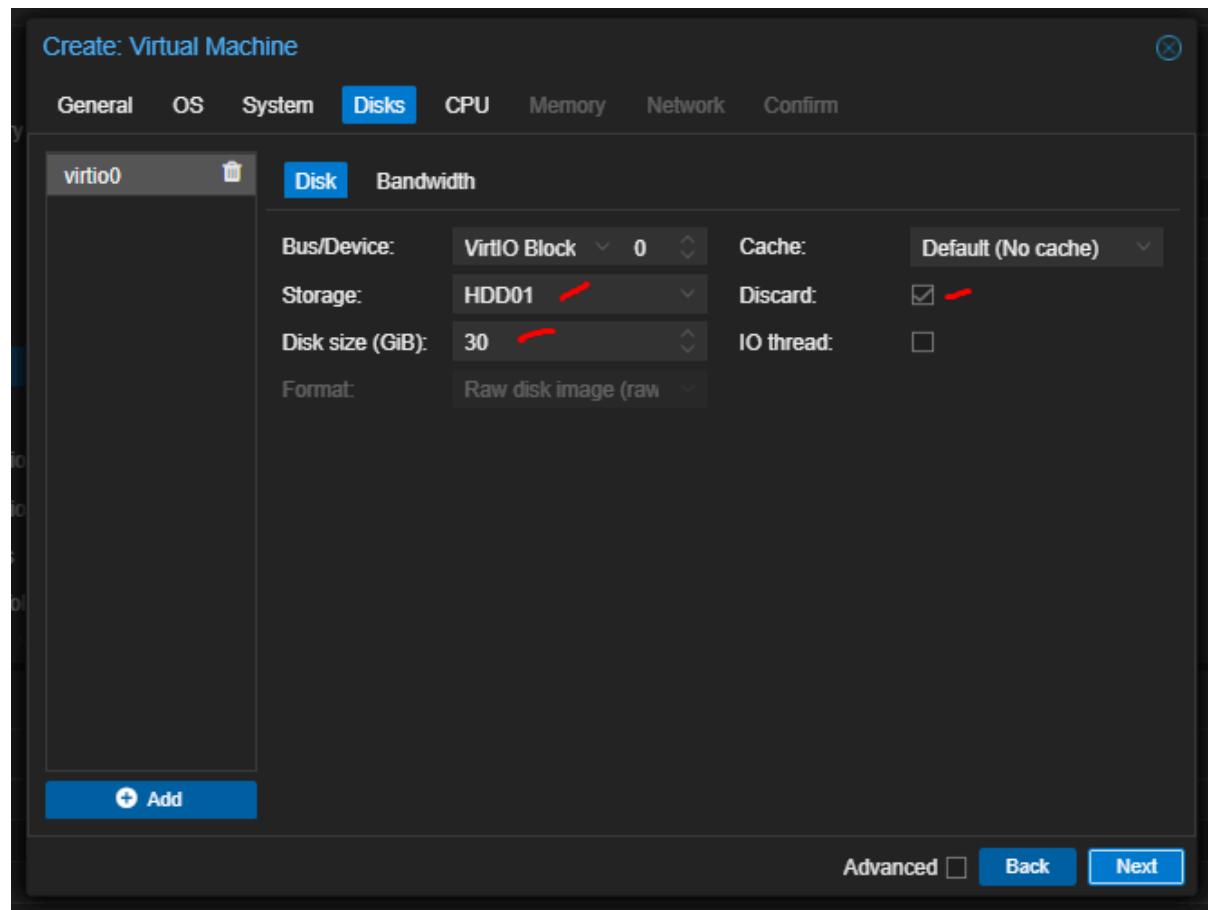
En el siguiente paso seleccionamos la ISO del SO el cual vamos a instalar.



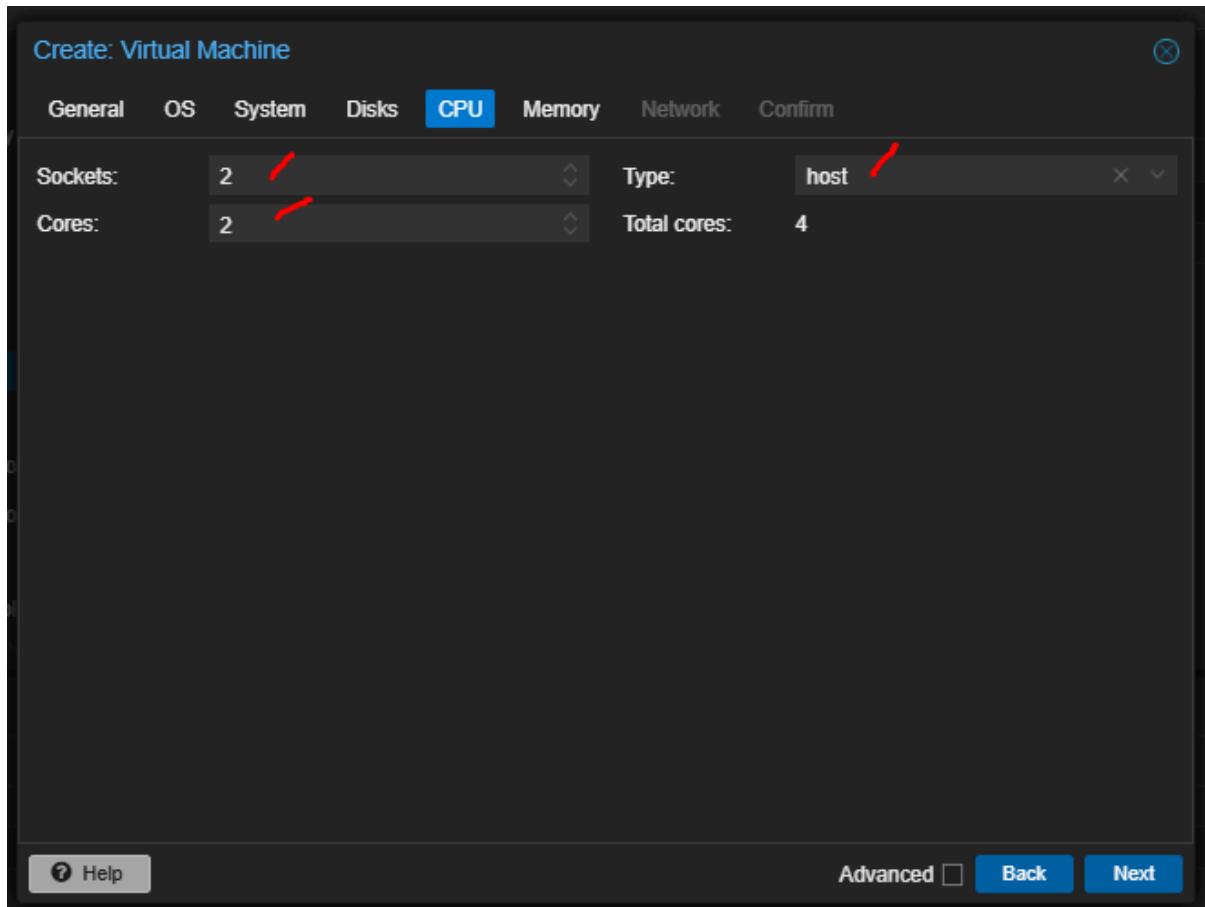
En system dejamos predeterminado.



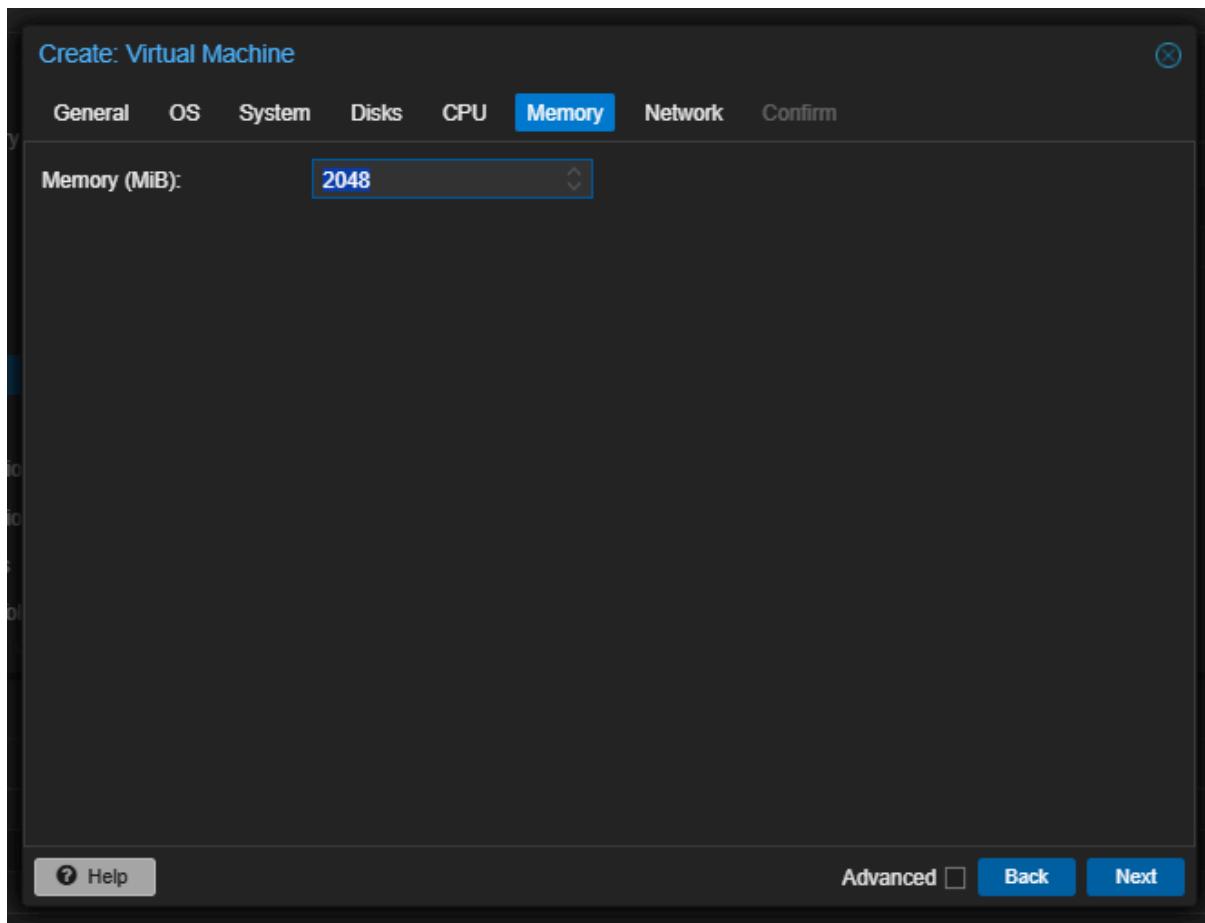
En disk verificamos que tengamos nuestro disco adicional para instalar la máquina y asignamos el tamaño que queramos darle.



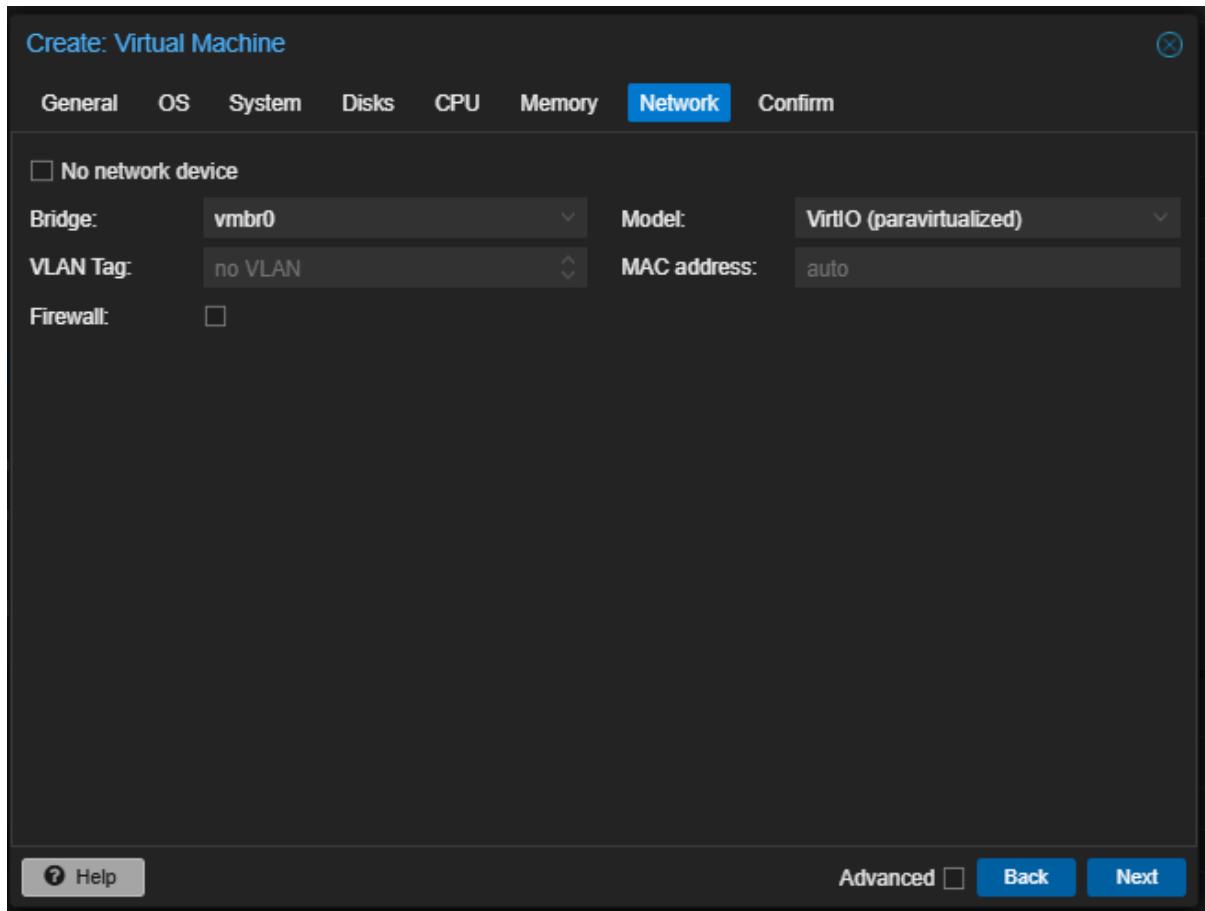
En CPU debemos verificar que esté seleccionado Host para cerciorarnos que asignamos los recursos de la máquina física, asignamos sockets y núcleos según los recursos que se tengan para que no quede saturada la máquina física.



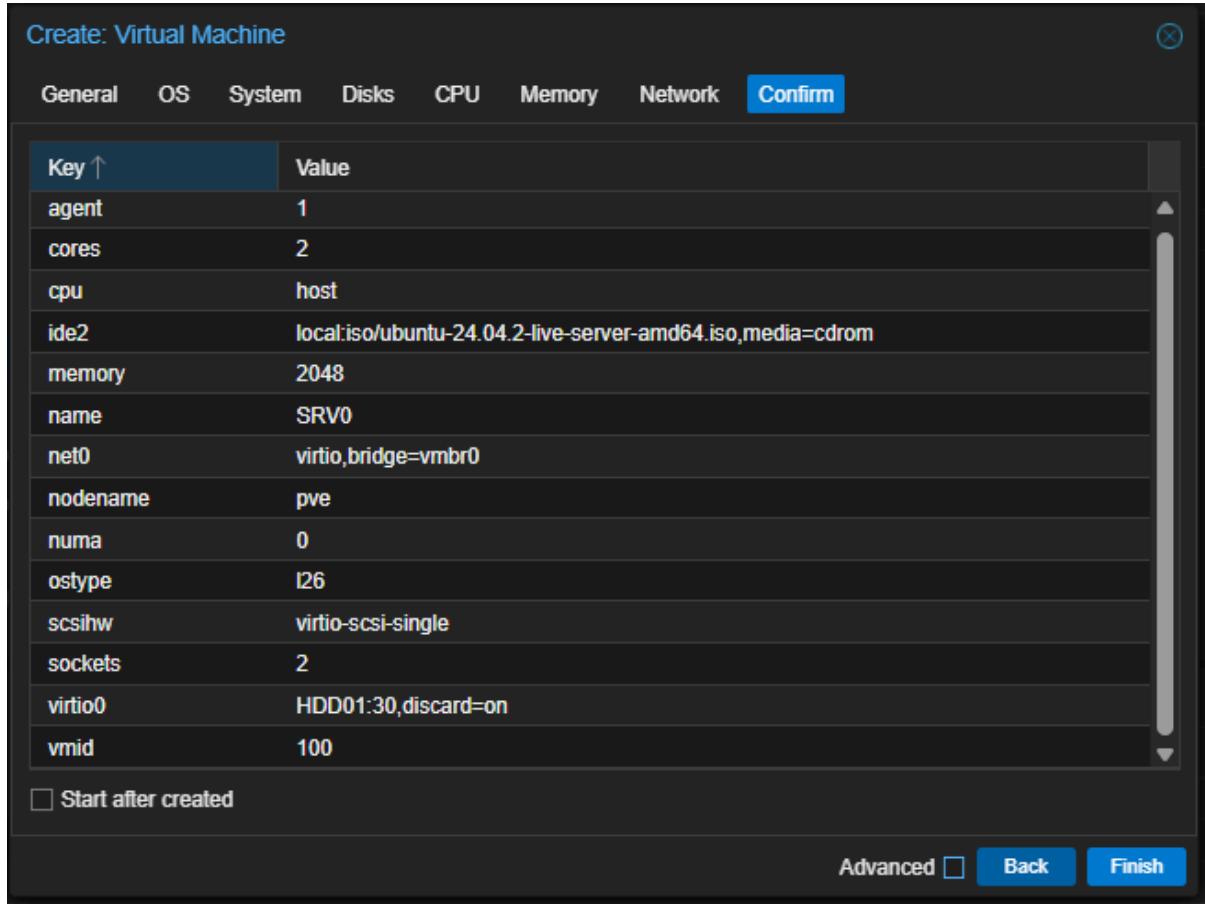
Asignamos la memoria RAM también dependiendo los recursos de la máquina física.



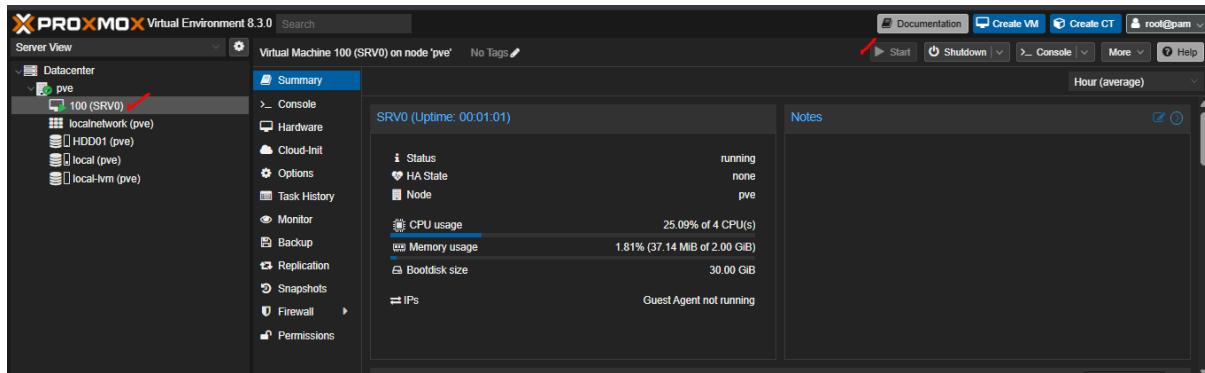
En Red dejamos predeterminado y seguimos.



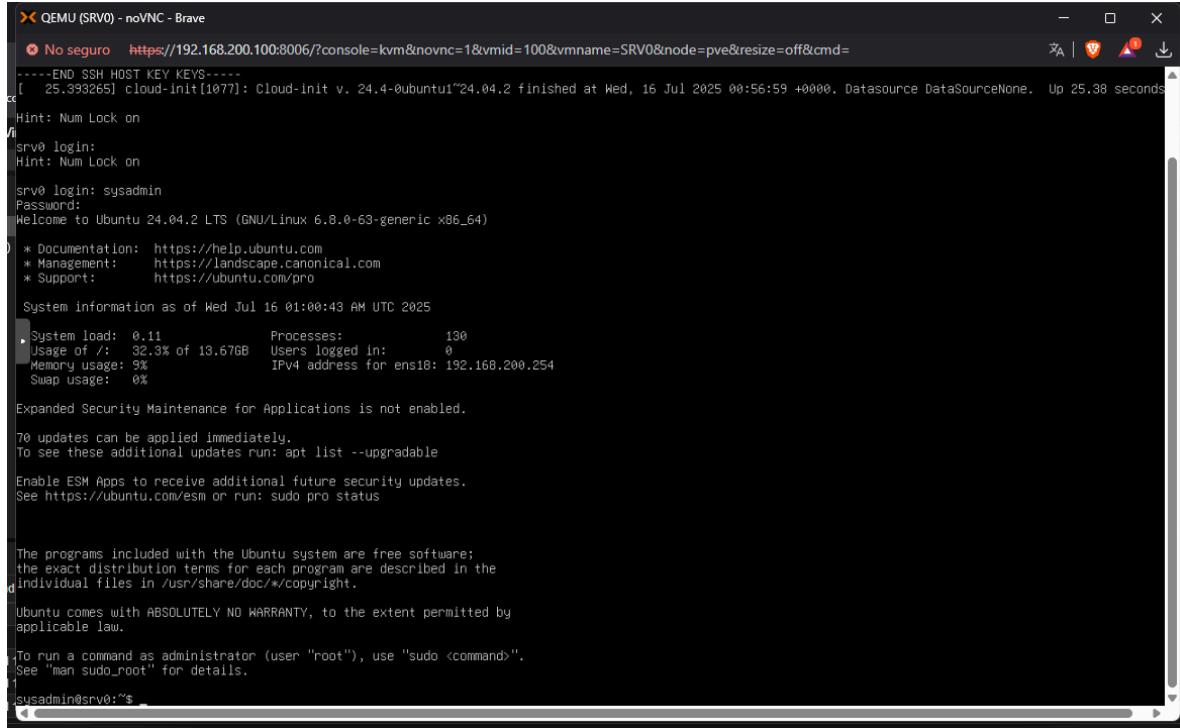
Seguido le damos en confirmar toda la configuración puesta y damos en crear.



Ya en nuestro panel principal nos aparece nuestra máquina creada y lista para ejecutar. Para iniciarla le damos en start y ya inicia normalmente.



Inicia el equipo y ya podemos acceder sin problema.



ANEXO 2 Instalación Firewall Mikrotik:

FIREWALL

Un **firewall** también conocido como cortafuegos es un sistema de seguridad de red que monitorea y controla el tráfico de red entrante y saliente basándose en un conjunto predeterminado de reglas de seguridad. Actúa como una barrera entre una red interna segura y confiable y redes externas no confiables, como internet.

¿Cómo funciona un firewall?

Básicamente, un firewall examina cada paquete de datos que intenta entrar o salir de tu red. Piensa en él como un portero muy estricto que revisa la identificación y el propósito de cada persona que intenta pasar. Si el paquete cumple con las reglas establecidas por el firewall, se le permite pasar; de lo contrario, se bloquea.

Tipos de firewalls

Existen varios tipos de firewalls, cada uno con sus propias características y métodos de funcionamiento:

- **Firewall de filtrado de paquetes:** Es el tipo más básico. Examina los paquetes de datos individualmente, basándose en la dirección IP de origen y destino, el puerto y el protocolo. Si un paquete coincide con una regla, se le permite o se le niega el paso.
- **Firewall con estado (Stateful Inspection Firewall):** Este tipo es más avanzado. No solo examina los paquetes individualmente, sino que también rastrea el estado de las conexiones de red activas. Esto le permite determinar si un paquete es parte de una conexión legítima o si es un intento de intrusión.
- **Firewall de proxy (Proxy Firewall):** Actúa como un intermediario entre la red interna y la externa. Todos los datos de la red pasan a través del proxy. Esto proporciona un alto nivel de seguridad, ya que la red interna nunca se comunica directamente con la red externa.
- **Firewall de próxima generación (Next-Generation Firewall - NGFW):** Combina las funciones de los firewalls tradicionales con otras capacidades de seguridad, como la prevención de intrusiones (IPS), el control de aplicaciones y la inteligencia de amenazas. Son mucho más sofisticados y pueden identificar y bloquear amenazas más complejas.
- **Firewall basado en host:** Se ejecuta en un dispositivo individual (como una computadora) y protege solo ese dispositivo.
- **Firewall basado en red:** Se implementa en el borde de la red y protege todos los dispositivos dentro de esa red.

¿Por qué es importante un firewall?

Los firewalls son esenciales para la seguridad cibernética porque:

- **Protegen contra accesos no autorizados:** Impiden que usuarios no deseados o programas maliciosos accedan a tu red o dispositivos.
- **Previenen ataques de malware:** Ayudan a bloquear la entrada de virus, troyanos, ransomware y otras formas de software malicioso.
- **Controlan el tráfico de red:** Permiten a los administradores de red establecer qué tipo de tráfico está permitido y cuál no, lo que es útil para optimizar el rendimiento y la seguridad.
- **Ofrecen un registro de actividad:** Registran los intentos de acceso, lo que puede ser útil para identificar posibles amenazas o violaciones de seguridad.

Instalacion y configuracion de Firewall básico de Mikrotik



Para realizar la configuración debemos tener un Equipo capa 2 o 3 de Mikrotik el cual es un Switch o un Router desde el más básico nos sirve.

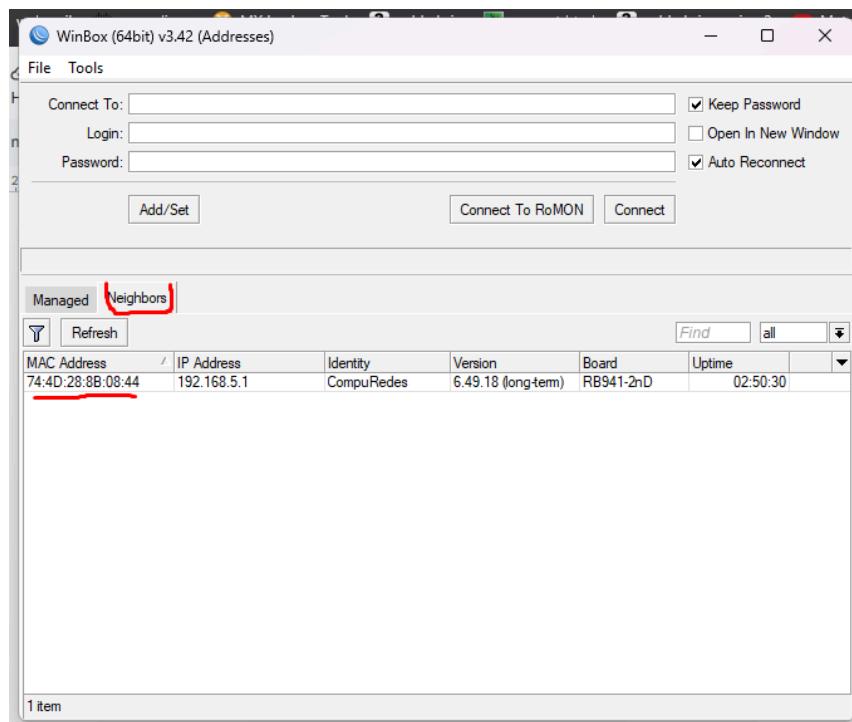
Realizamos la conexión del equipo a nuestro pc.



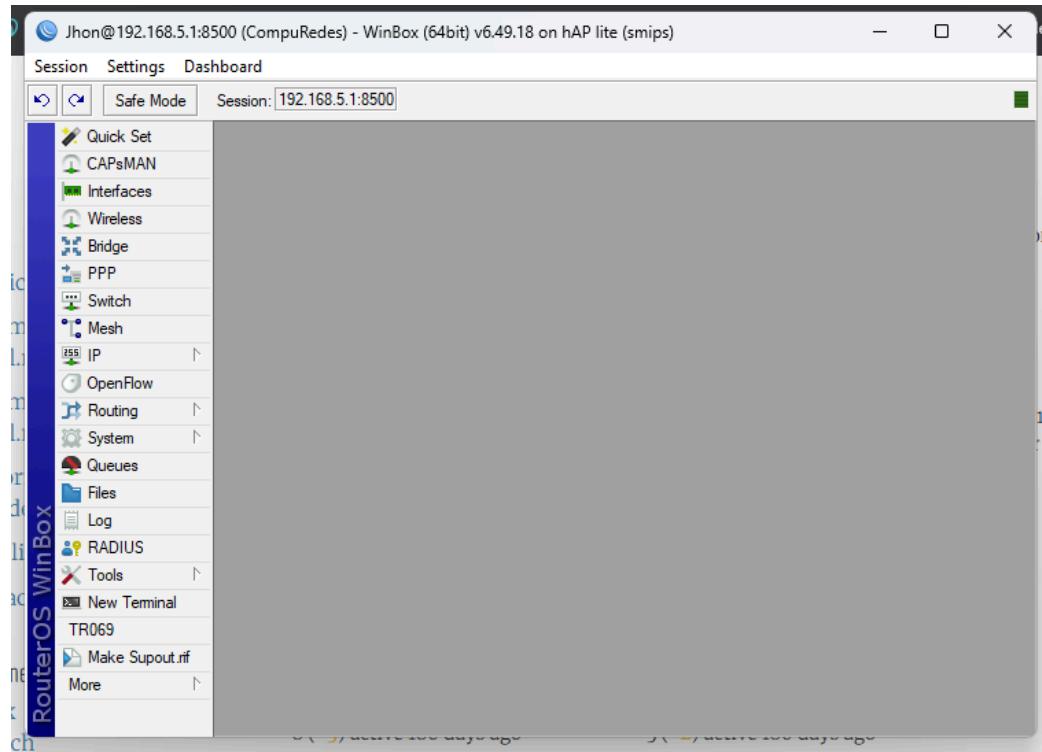
Desde la página de Mikrotik realizamos la descarga del software winbox.

The screenshot shows the MikroTik Software page. At the top, there's a navigation bar with links to Home, About, Buy, Jobs, Hardware, Software (which is underlined), Support, Training, and Account. Below this is a secondary navigation bar with links to Downloads, Changelogs, Download archive, RouterOS, The Dude, Mobile apps, and Back To Home. The main content area has a heading 'Upgrading RouterOS'. It includes instructions for upgrading RouterOS and managing the router using the web interface or WinBox. A sidebar on the left shows download options for WinBox: 'WinBox 4.0beta24' (selected) and 'WinBox 3.42'. To the right, there's an image of a laptop and a smartphone both displaying network management interfaces.

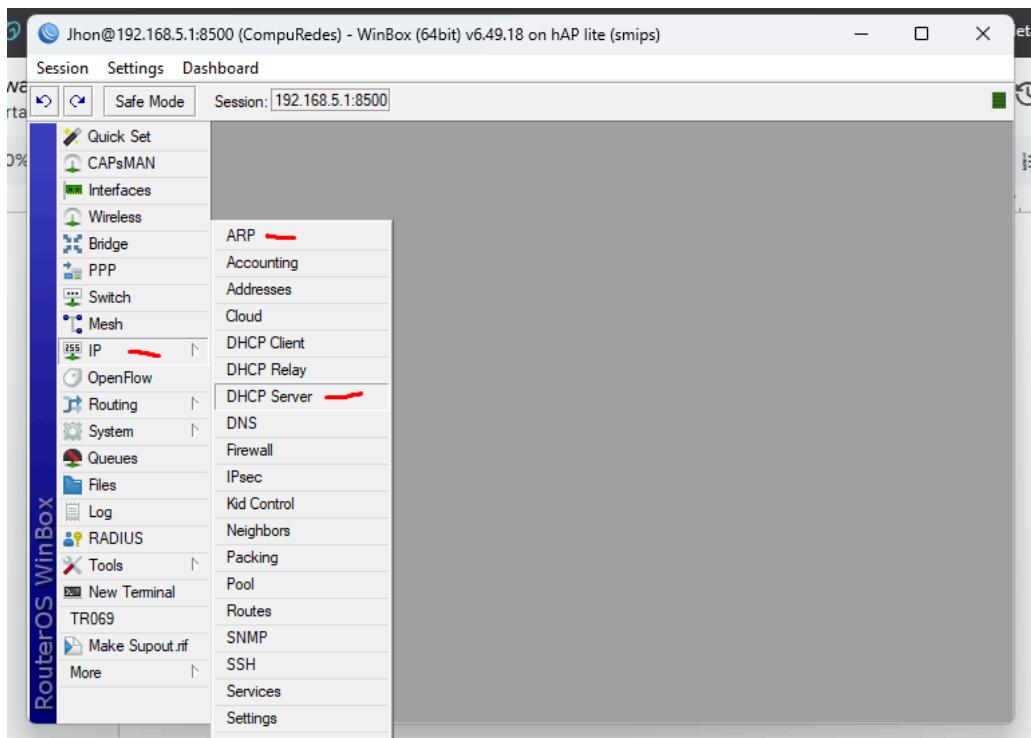
Una vez descargado lo ejecutamos y nos dará el siguiente entorno gráfico el cual clickeamos en neighbor y nos debería mostrar el equipo automáticamente, ingresamos el usuario admin y dejamos la contraseña en blanco y le damos en connect.



Vista principal del router



Revisamos que equipos tenemos conectados a nuestro router en 2 menús diferentes en la tabla ARP y en las direcciones DHCP



The screenshot shows the WinBox interface with the session set to Jhon@192.168.5.1:8500. The 'ARP' option from the previous menu is selected, opening the 'ARP List' window. Below it, the 'DHCP Server' window is also open, showing lease information.

ARP List:

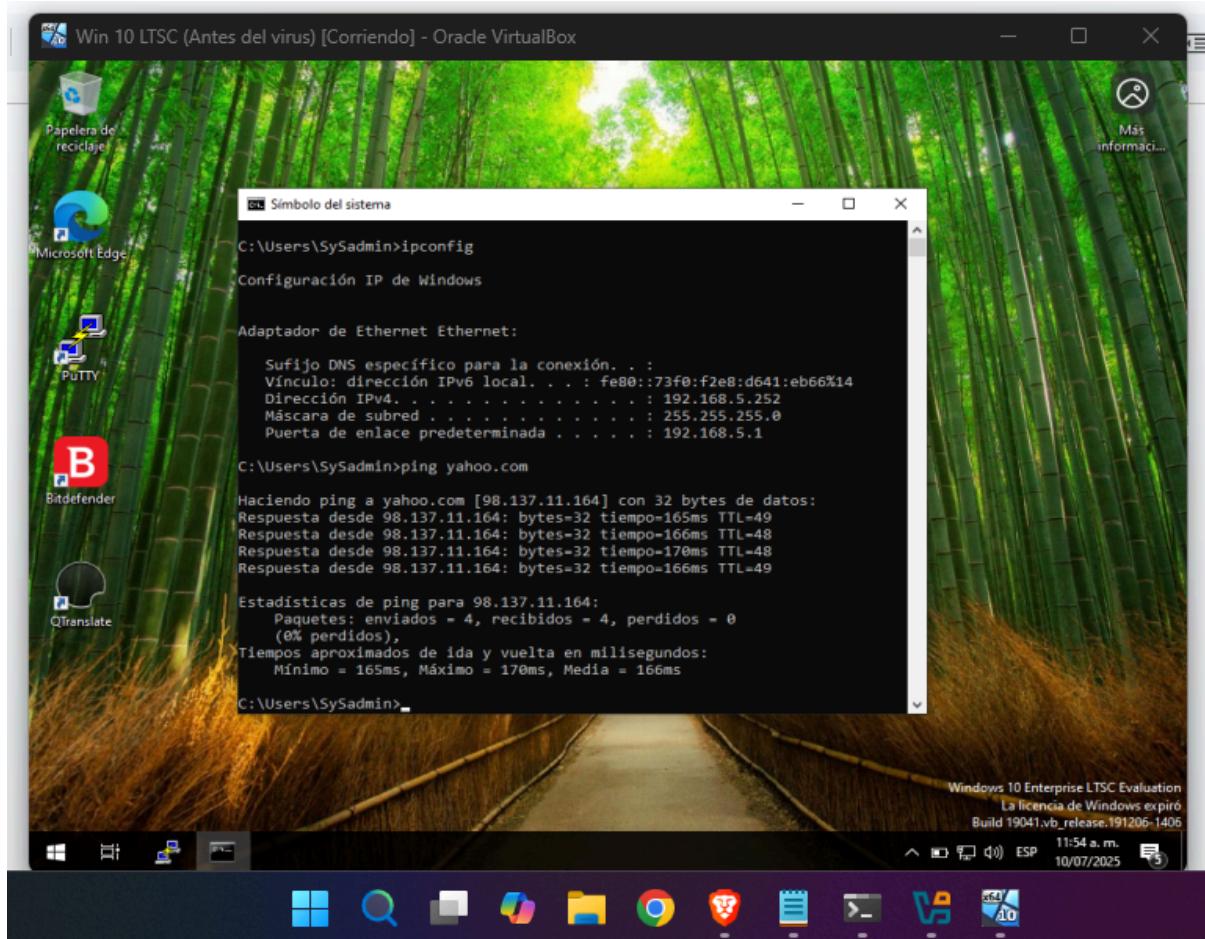
	IP Address	MAC Address	Interface
DC	192.168.5.251	B4:69:21:2B:53:9F	LAN
DC	192.168.5.253	20:4E:F6:85:C4:D9	LAN
DC	192.168.60.1	12:02:00:00:01:01	ether1

DHCP Server:

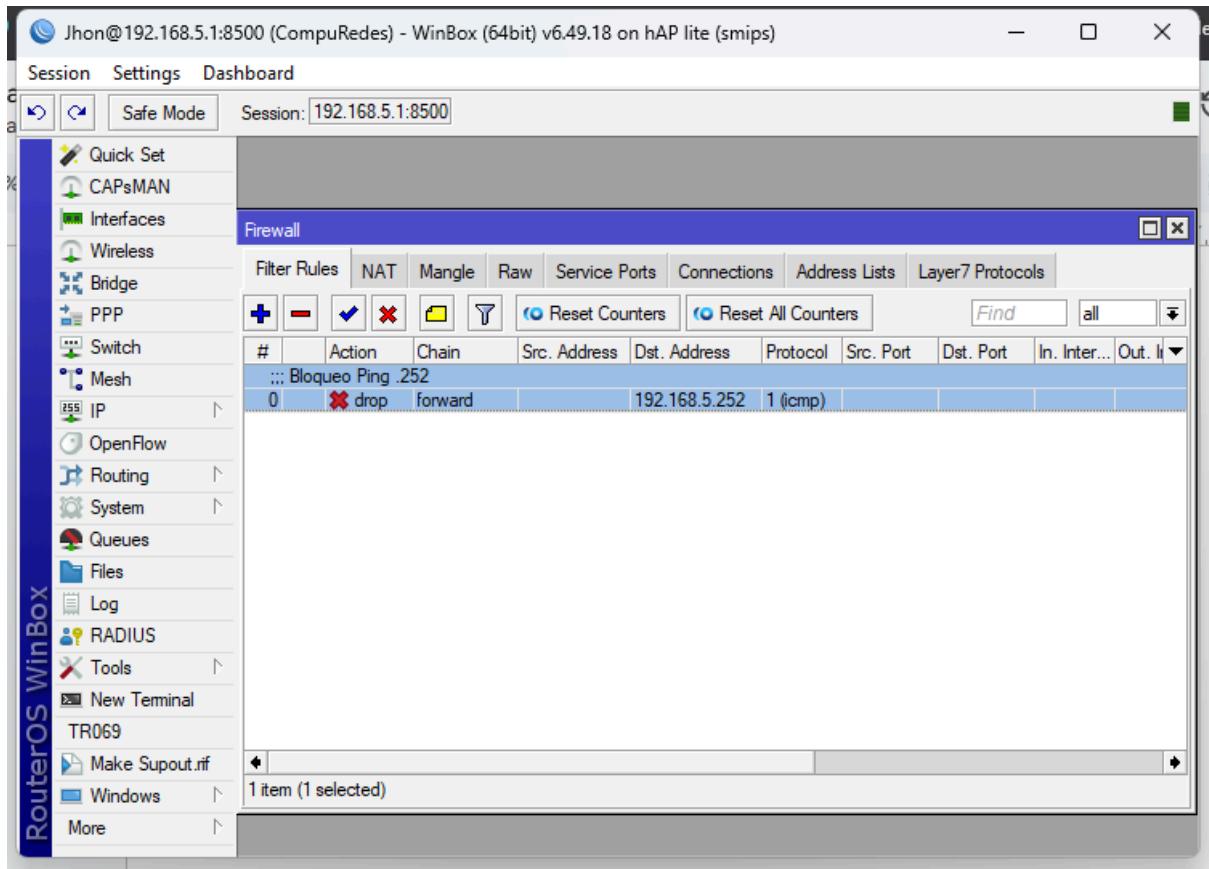
	Address	MAC Address	Server	Active Host Name	Expires After	St
D	192.168.5.251	B4:69:21:2B:53:9F	dhcp1	Precision7520	00:05:30	boun
D	192.168.5.253	20:4E:F6:85:C4:D9	dhcp1	Sistemas	00:06:26	boun

En nuestra práctica vamos a permitir la realización de ICMP (ping) de la máquina virtual con Windows 10 LTSC a cualquier dirección IP o dominio.

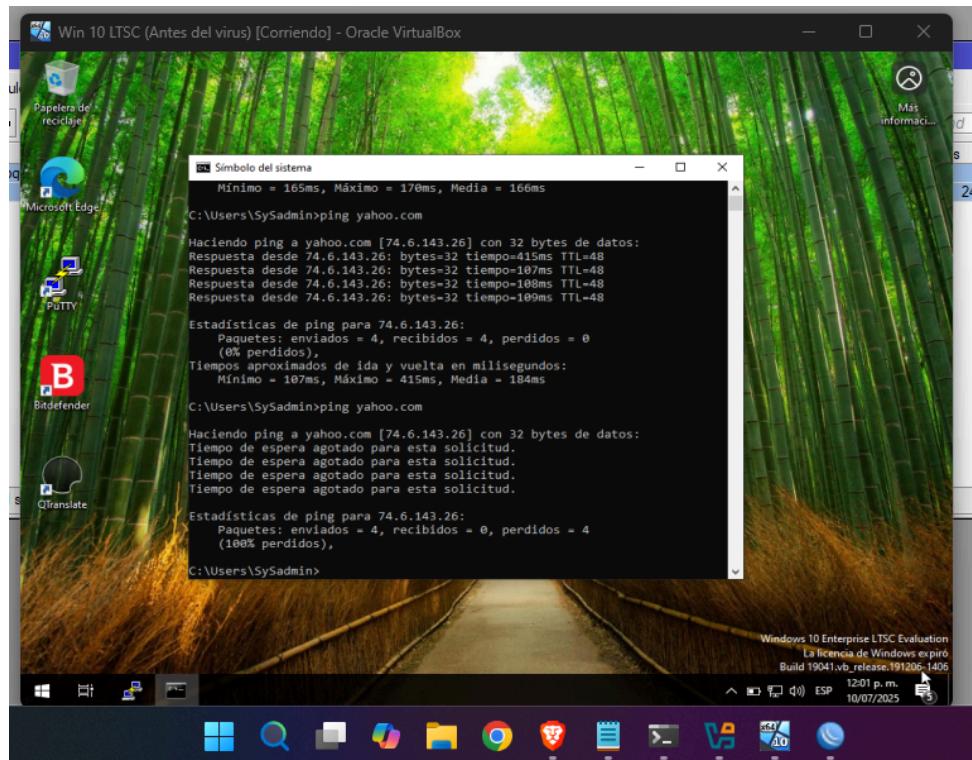
Podemos observar que la maquina tiene la ip 192.168.5.252 y envia ping a yahoo.com obteniendo respuesta,



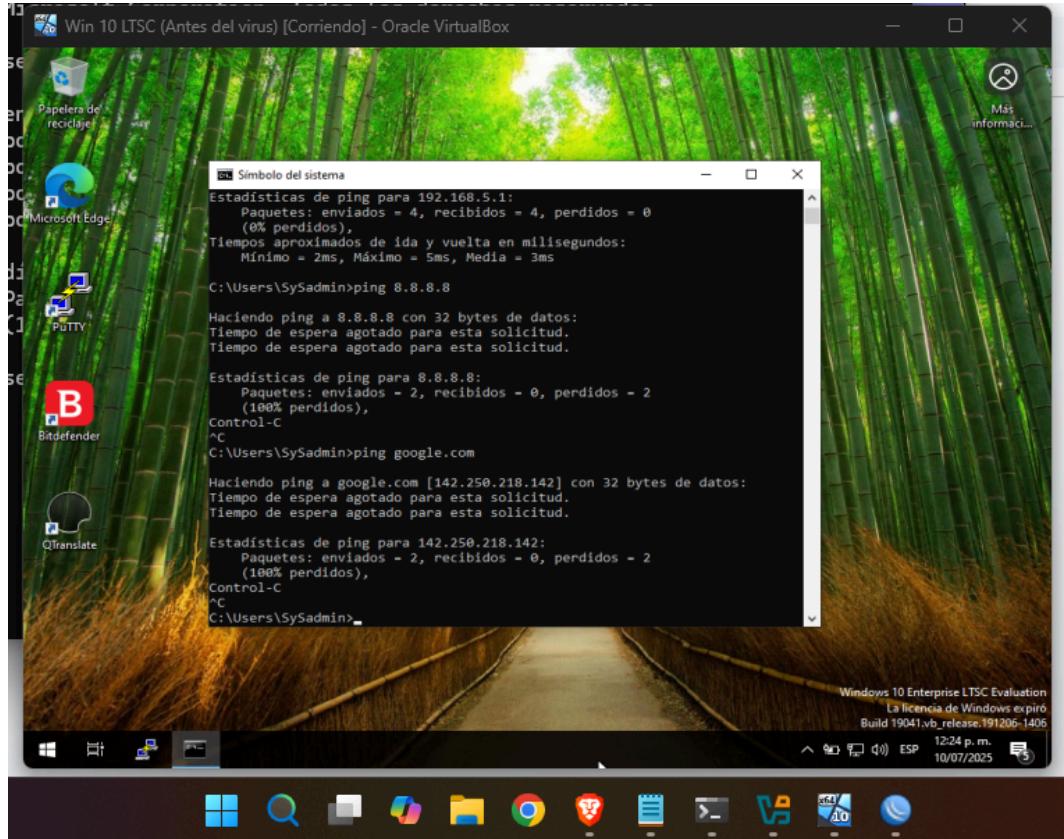
Procedemos a configurar el Firewall indicando como regla que todo lo que pase por el router con protocolo ICMP con destino a la ip del equipo 192.168.5.252 lo bloquee.



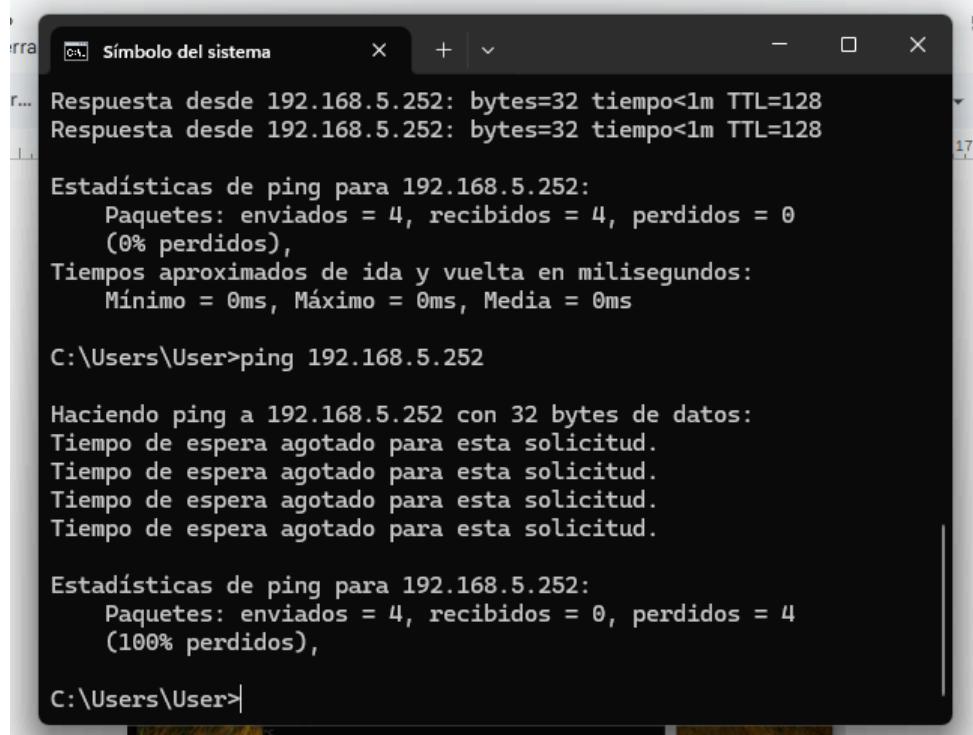
Realizamos nuevamente el ping desde nuestro equipo y efectivamente no se obtiene respuesta del ICMP.



Tratamos de realizar ping a diferentes ip y dominio y no obtenemos respuesta.



Realizamos ping desde la máquina física a la máquina virtual con la ip bloqueada y no tenemos respuesta.



```

r... Respuesta desde 192.168.5.252: bytes=32 tiempo<1m TTL=128
r... Respuesta desde 192.168.5.252: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.5.252:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\User>ping 192.168.5.252

Haciendo ping a 192.168.5.252 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.5.252:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
                (100% perdidos),
C:\Users\User>

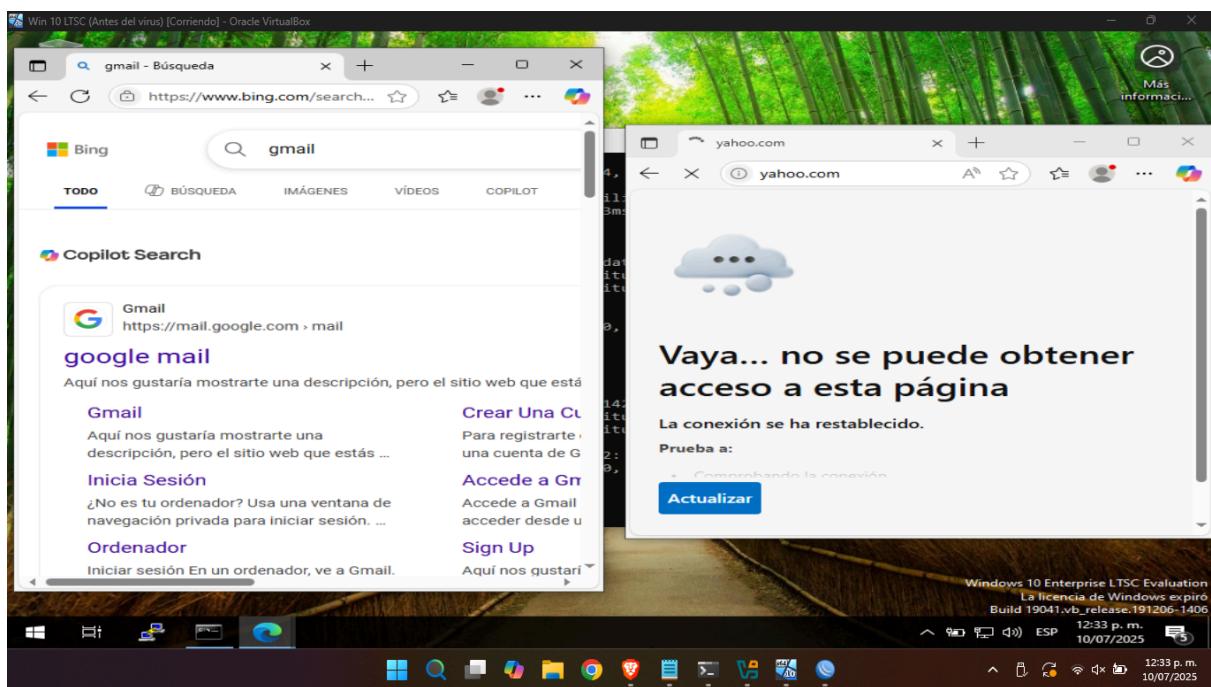
```

Realizamos una nueva regla el cual bloquea la navegación a la pagina yahoo.com

Firewall																
Filter Rules																
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Content	Bytes	Packets
0	drop	forward		192.168.5.252	1 (icmp)										540 B	9
1	drop	forward											yahoo.com		19.8 KB	45

Como podemos observar en el contador de paquetes y de Bytes nos muestra la cantidad y el tamaño de los paquetes bloqueados para cada regla.

Probamos la navegación de nuestro equipo virtual y únicamente no podemos acceder a la página bloqueada.



ANEXO 3 Instalación Firewall Pfsense:

FIREWALL

Un **firewall** también conocido como cortafuegos es un sistema de seguridad de red que monitorea y controla el tráfico de red entrante y saliente basándose en un conjunto predeterminado de reglas de seguridad. Actúa como una barrera entre una red interna segura y confiable y redes externas no confiables, como internet.

¿Cómo funciona un firewall?

Básicamente, un firewall examina cada paquete de datos que intenta entrar o salir de tu red. Piensa en él como un portero muy estricto que revisa la identificación y el propósito de cada persona que intenta pasar. Si el paquete cumple con las reglas establecidas por el firewall, se le permite pasar; de lo contrario, se bloquea.

Tipos de firewalls

Existen varios tipos de firewalls, cada uno con sus propias características y métodos de funcionamiento:

- **Firewall de filtrado de paquetes:** Es el tipo más básico. Examina los paquetes de datos individualmente, basándose en la dirección IP de origen y destino, el puerto y el protocolo. Si un paquete coincide con una regla, se le permite o se le niega el paso.
- **Firewall con estado (Stateful Inspection Firewall):** Este tipo es más avanzado. No solo examina los paquetes individualmente, sino que también rastrea el estado de las conexiones de red activas. Esto le permite determinar si un paquete es parte de una conexión legítima o si es un intento de intrusión.
- **Firewall de proxy (Proxy Firewall):** Actúa como un intermediario entre la red interna y la externa. Todos los datos de la red pasan a través del proxy. Esto proporciona un alto nivel de seguridad, ya que la red interna nunca se comunica directamente con la red externa.
- **Firewall de próxima generación (Next-Generation Firewall - NGFW):** Combina las funciones de los firewalls tradicionales con otras capacidades de seguridad, como la prevención de intrusiones (IPS), el control de aplicaciones y la inteligencia de amenazas. Son mucho más sofisticados y pueden identificar y bloquear amenazas más complejas.
- **Firewall basado en host:** Se ejecuta en un dispositivo individual (como una computadora) y protege solo ese dispositivo.
- **Firewall basado en red:** Se implementa en el borde de la red y protege todos los dispositivos dentro de esa red.

¿Por qué es importante un firewall?

Los firewalls son esenciales para la seguridad cibernética porque:

- **Protegen contra accesos no autorizados:** Impiden que usuarios no deseados o programas maliciosos accedan a tu red o dispositivos.
- **Previenen ataques de malware:** Ayudan a bloquear la entrada de virus, troyanos, ransomware y otras formas de software malicioso.
- **Controlan el tráfico de red:** Permiten a los administradores de red establecer qué tipo de tráfico está permitido y cuál no, lo que es útil para optimizar el rendimiento y la seguridad.
- **Ofrecen un registro de actividad:** Registran los intentos de acceso, lo que puede ser útil para identificar posibles amenazas o violaciones de seguridad.

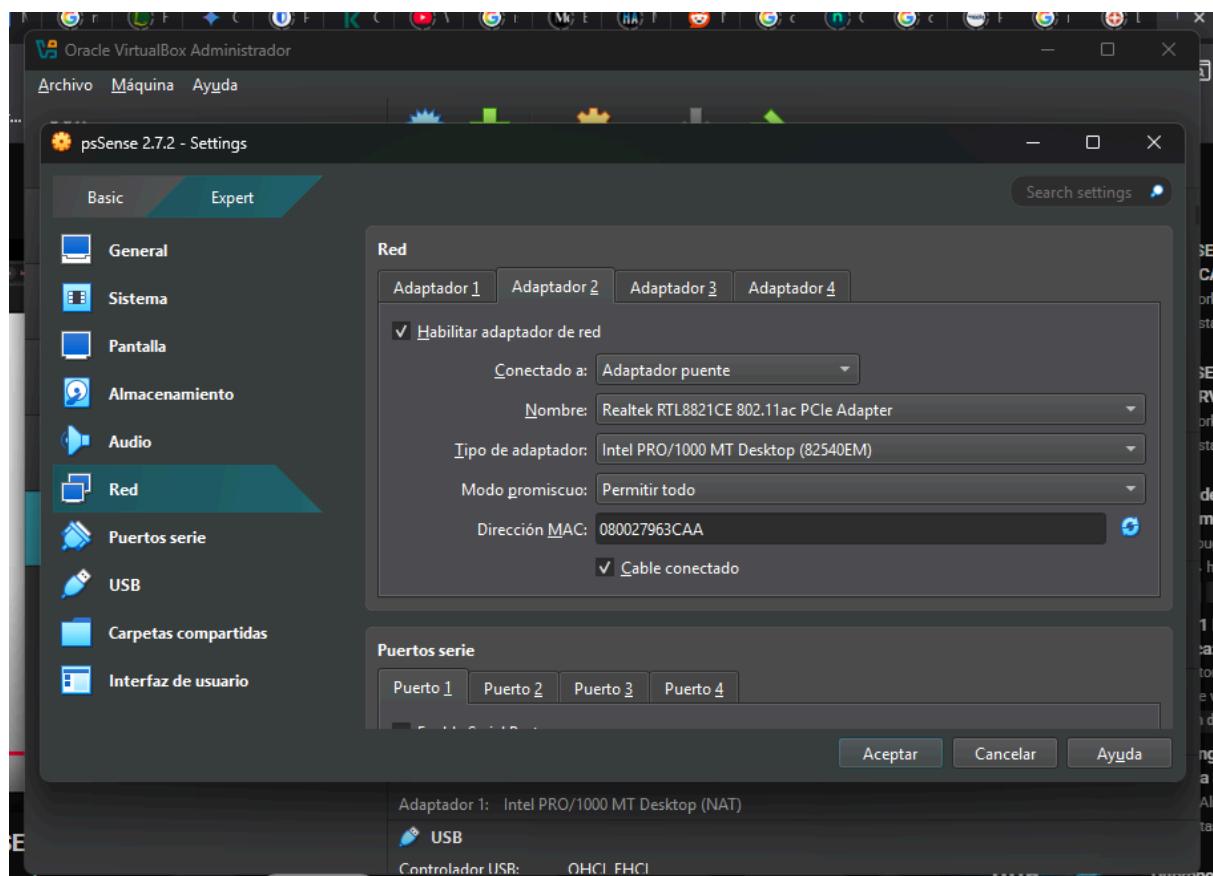
instalación y configuración de Firewall por software pfSense



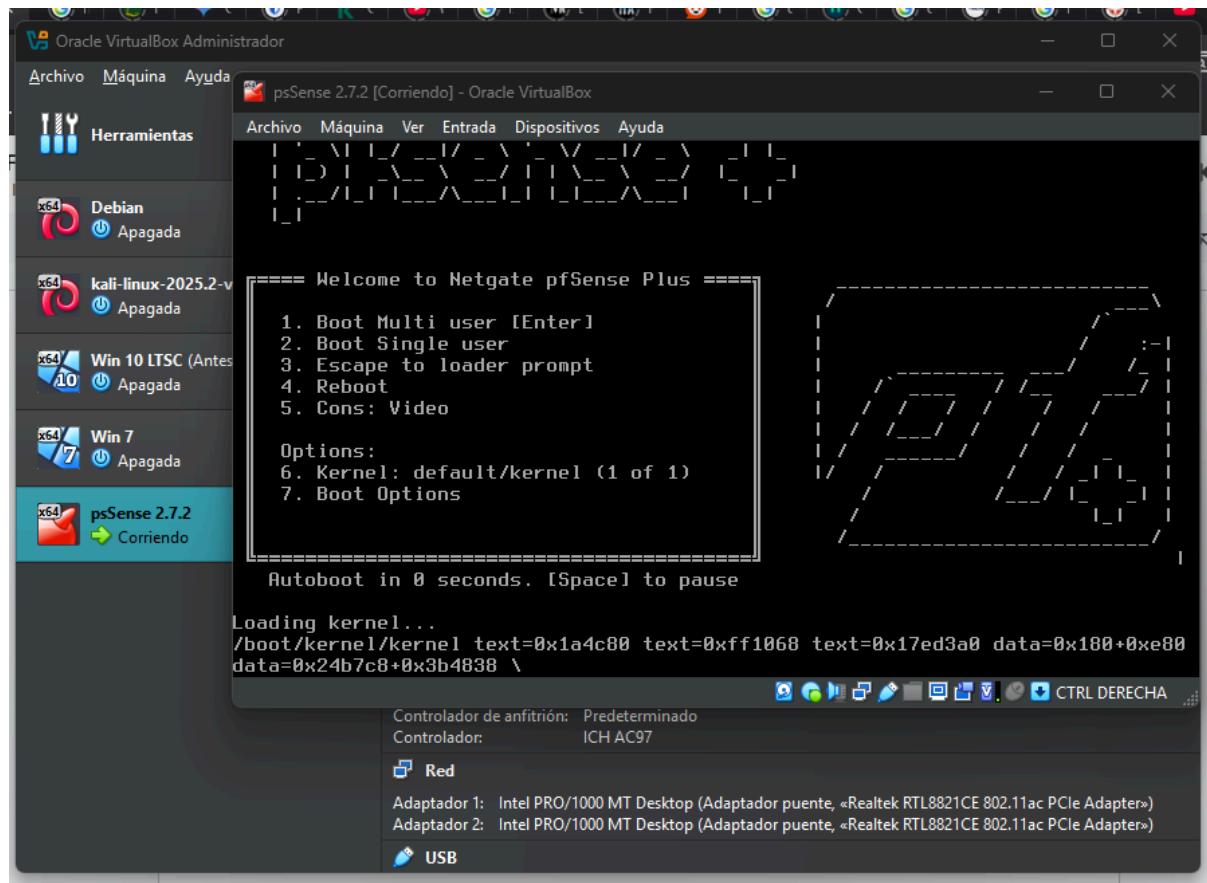
Vamos a realizar pruebas en otro tipo de Firewall el cual es un Firewall por software llamado pfSense

Como primera medida debemos ingresar a la página de pfsense <https://www.pfsense.org/download/>, nos registramos y descargamos la iso que nos permite instalar en una máquina bien sea física o virtual, para nuestro laboratorio lo instalaremos en una máquina virtual.

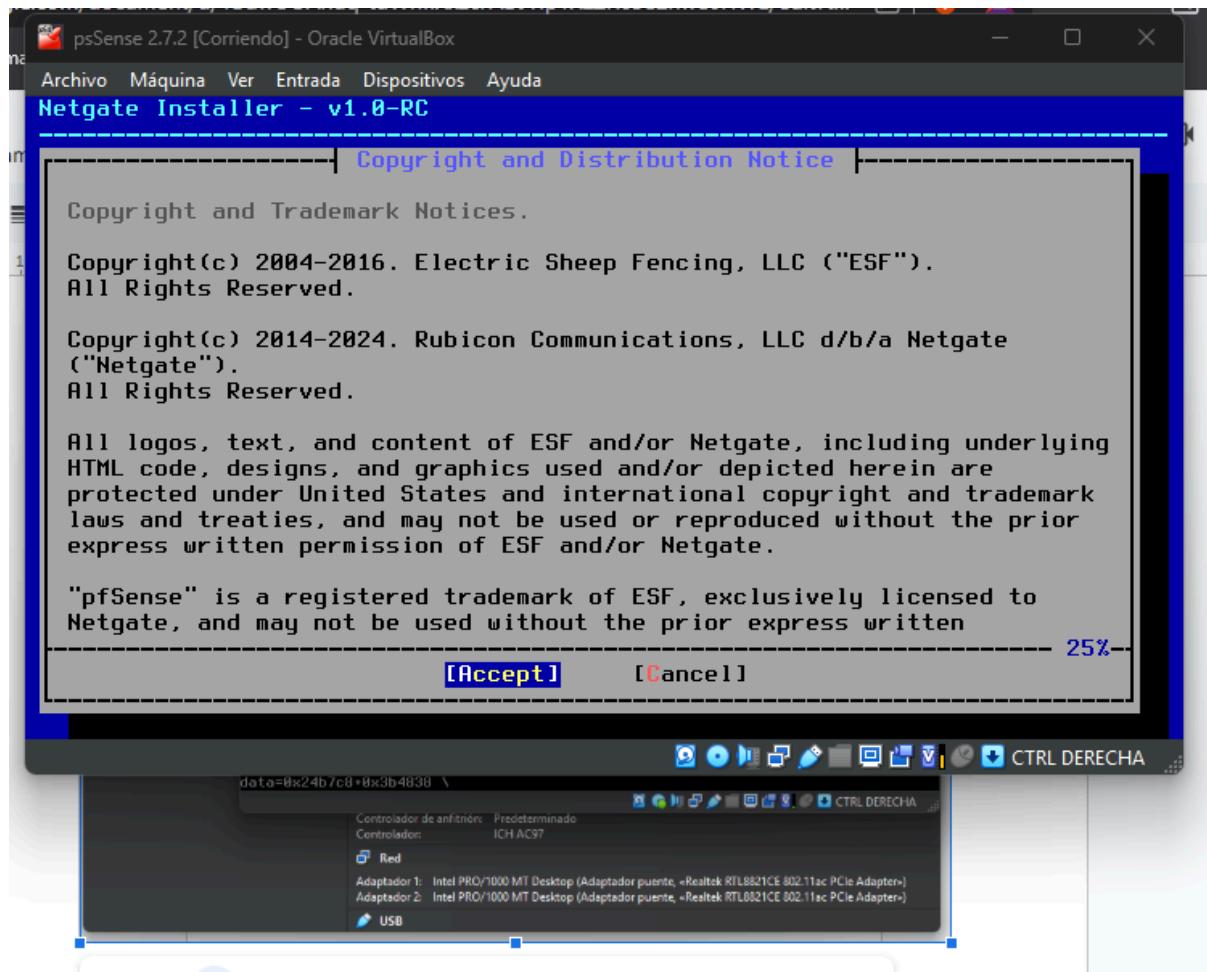
Iniciamos configurando nuestra máquina virtual en Virtualbox.

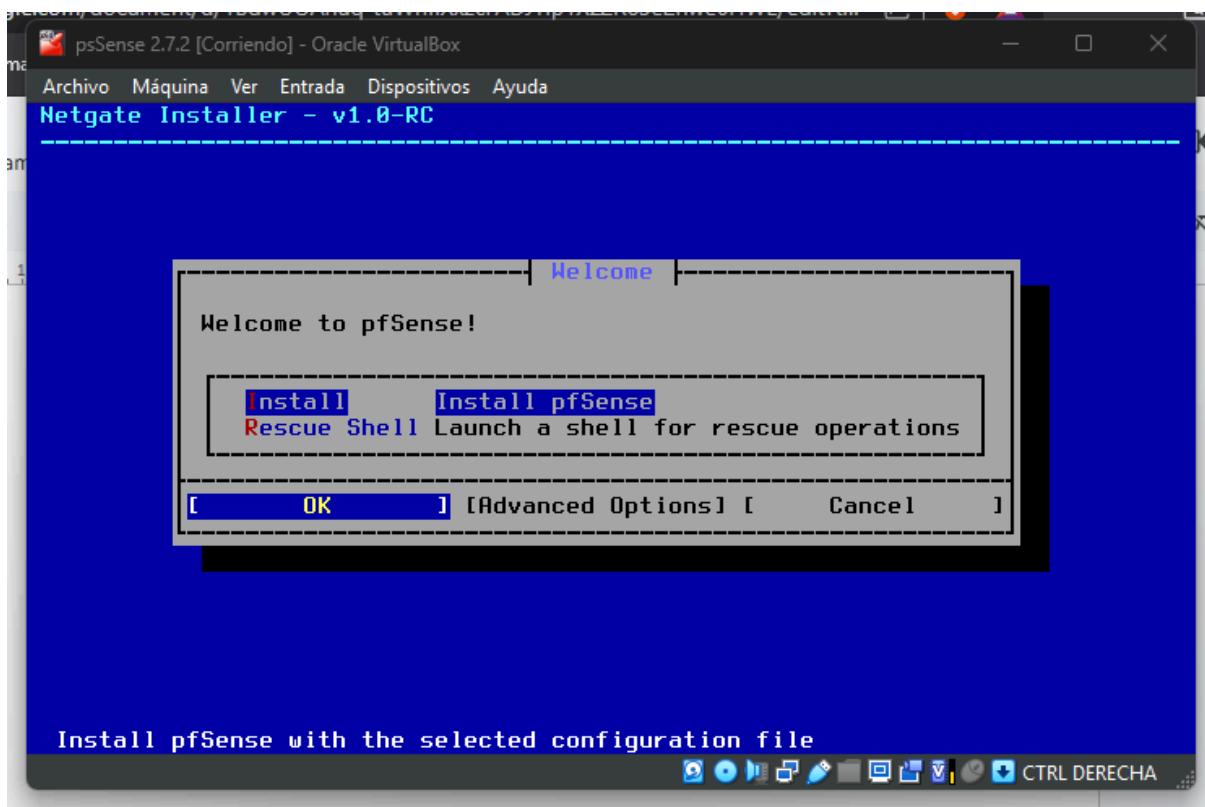


Cuando se enciende la máquina inicia a bootear y esperamos hasta que ya se deba interactuar.

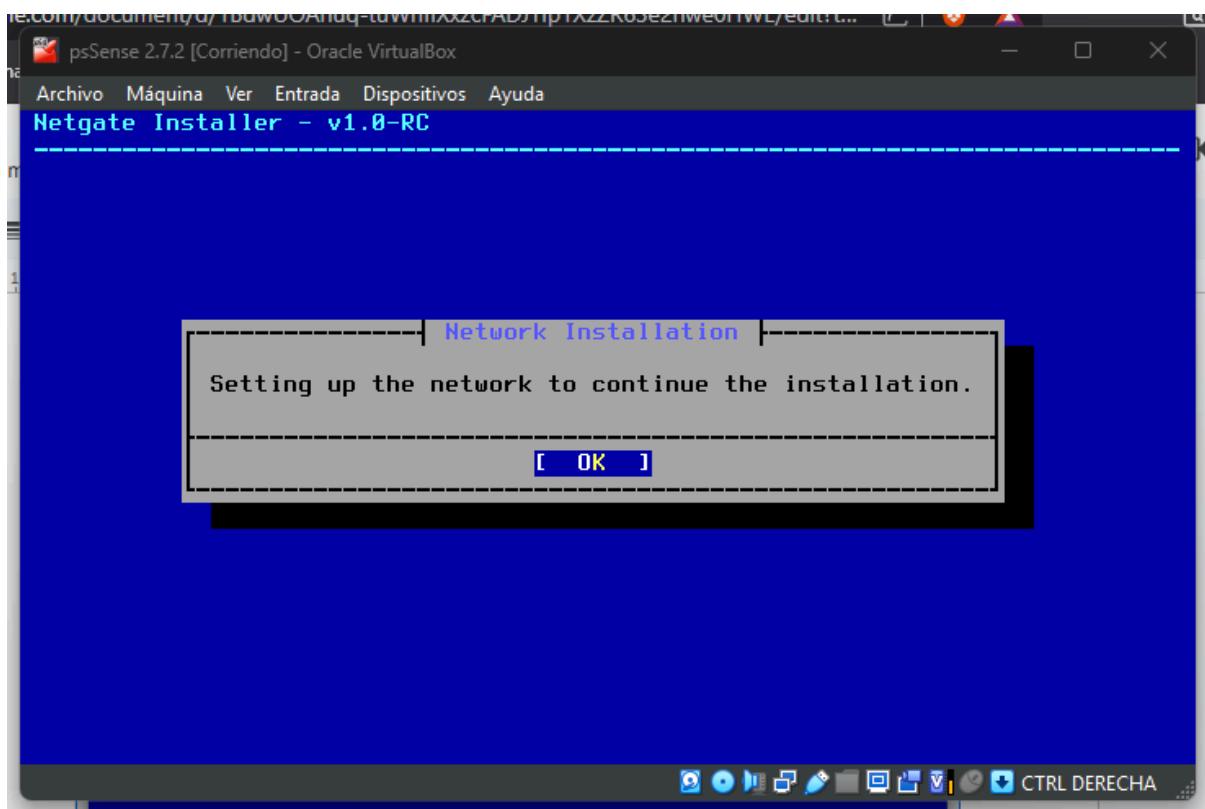


Después de cargar todos los archivos necesarios nos muestra los derechos de autor aceptamos y proseguimos con la instalación.

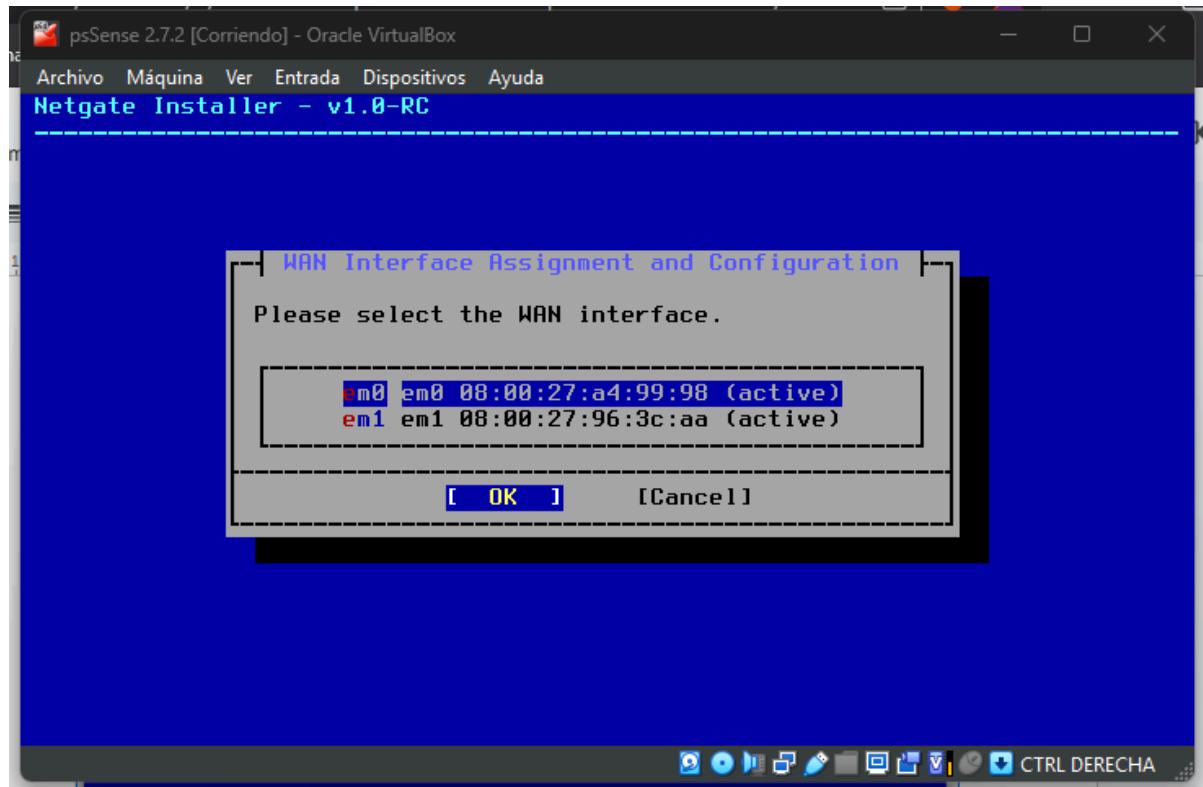




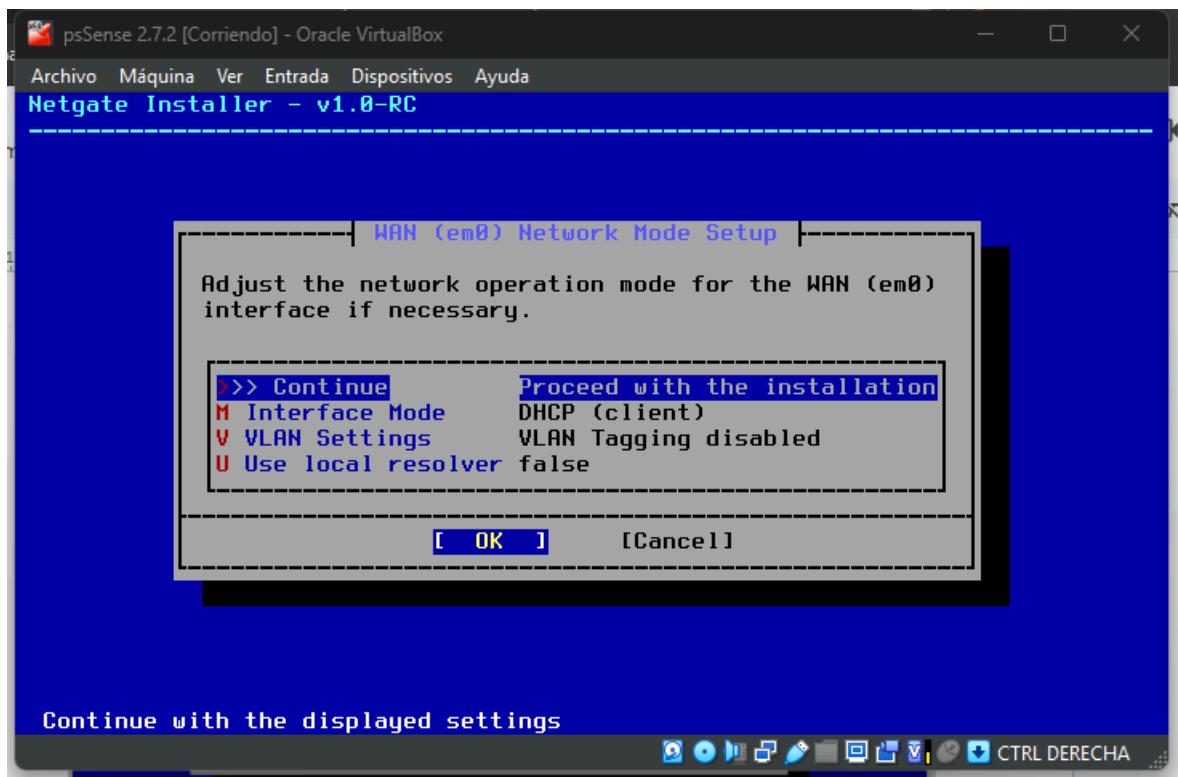
Cuando seleccionamos instalar nos va a pedir configurar la tarjeta de red, sin ello no podemos seguir con la instalación.



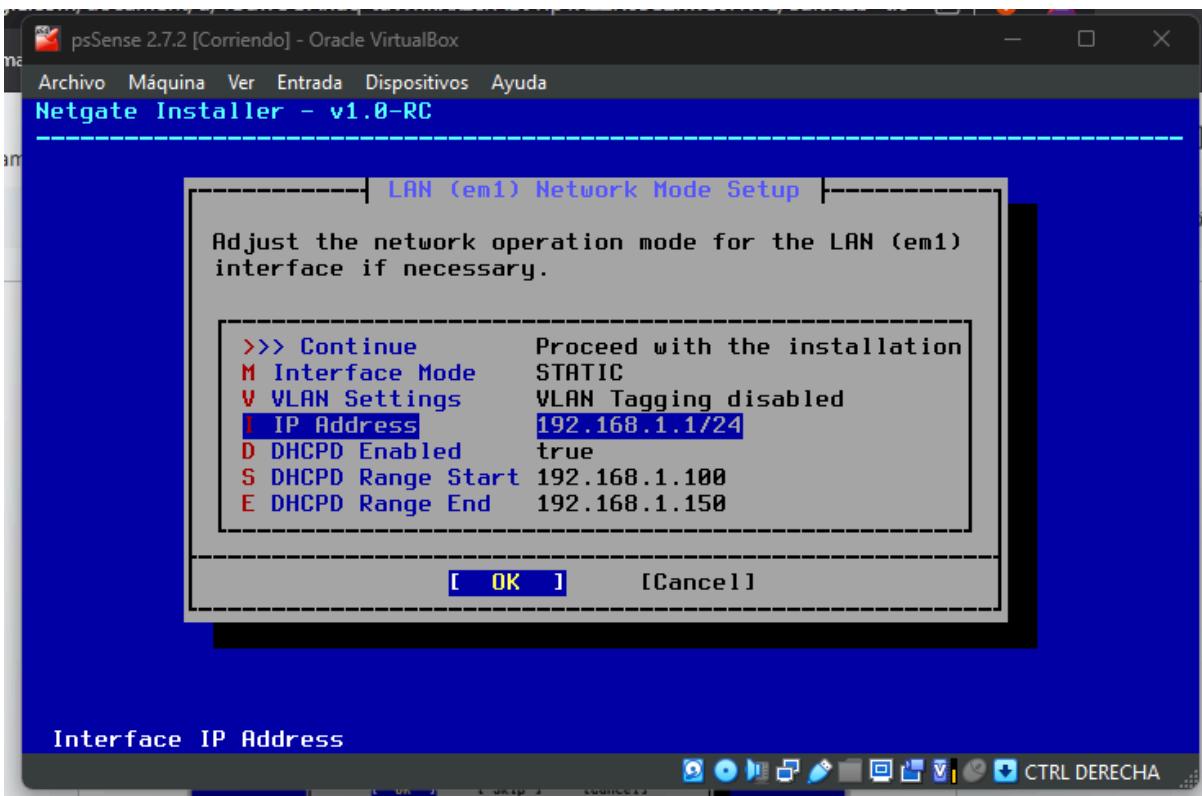
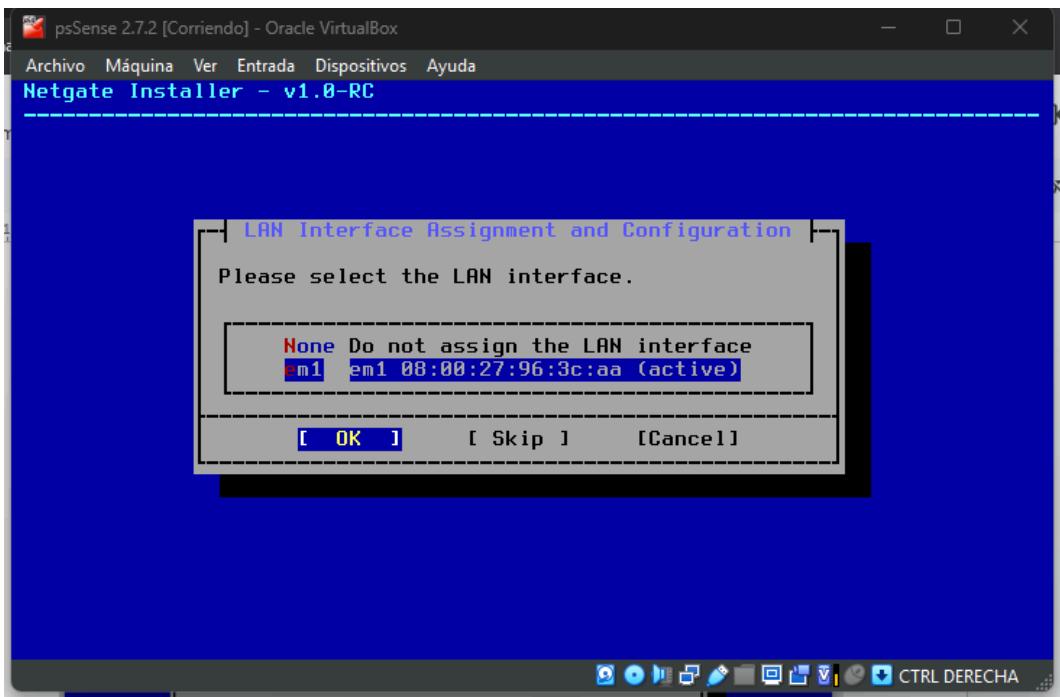
En mi caso configure 2 tarjetas de red y vamos a seleccionar una para que sea configurada como WAN.



Seleccionamos continuar para asignar la tarjeta WAN.

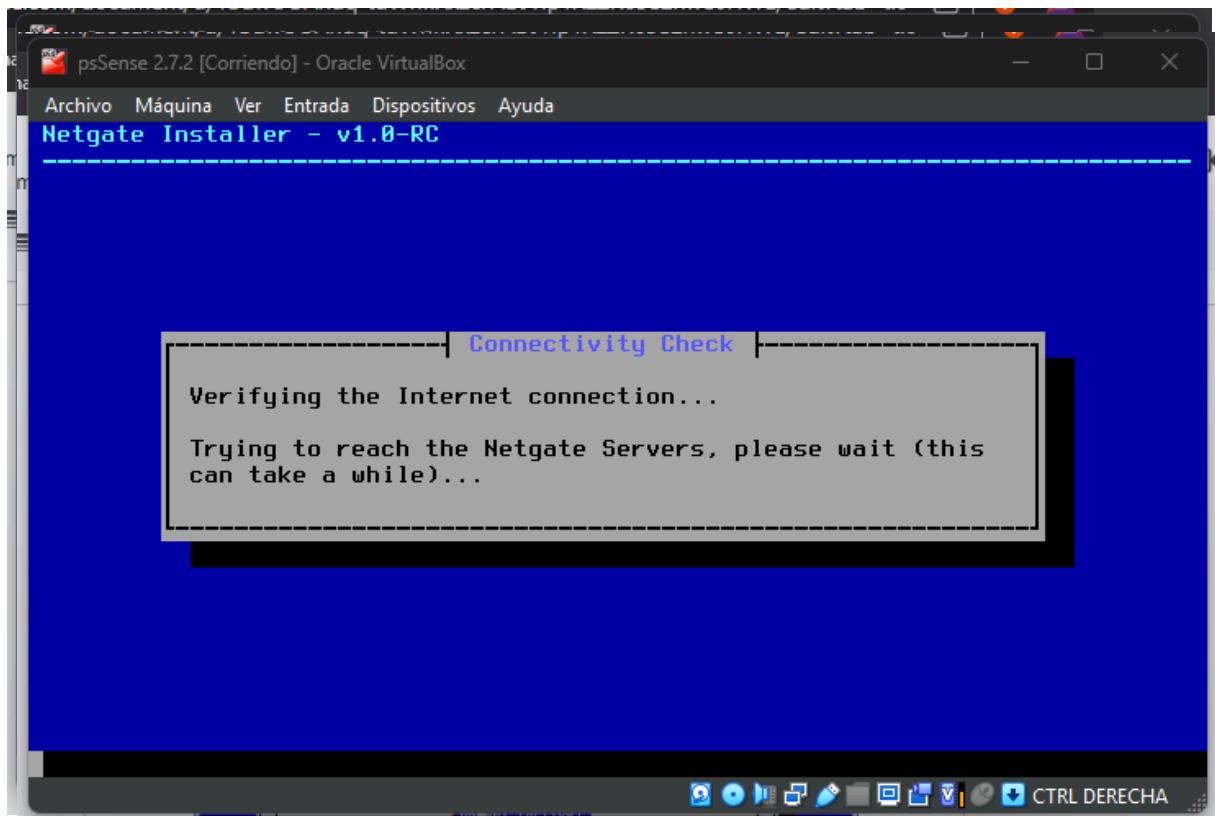


Paso seguido nos pide configurar la interface que vamos a asignar a LAN.

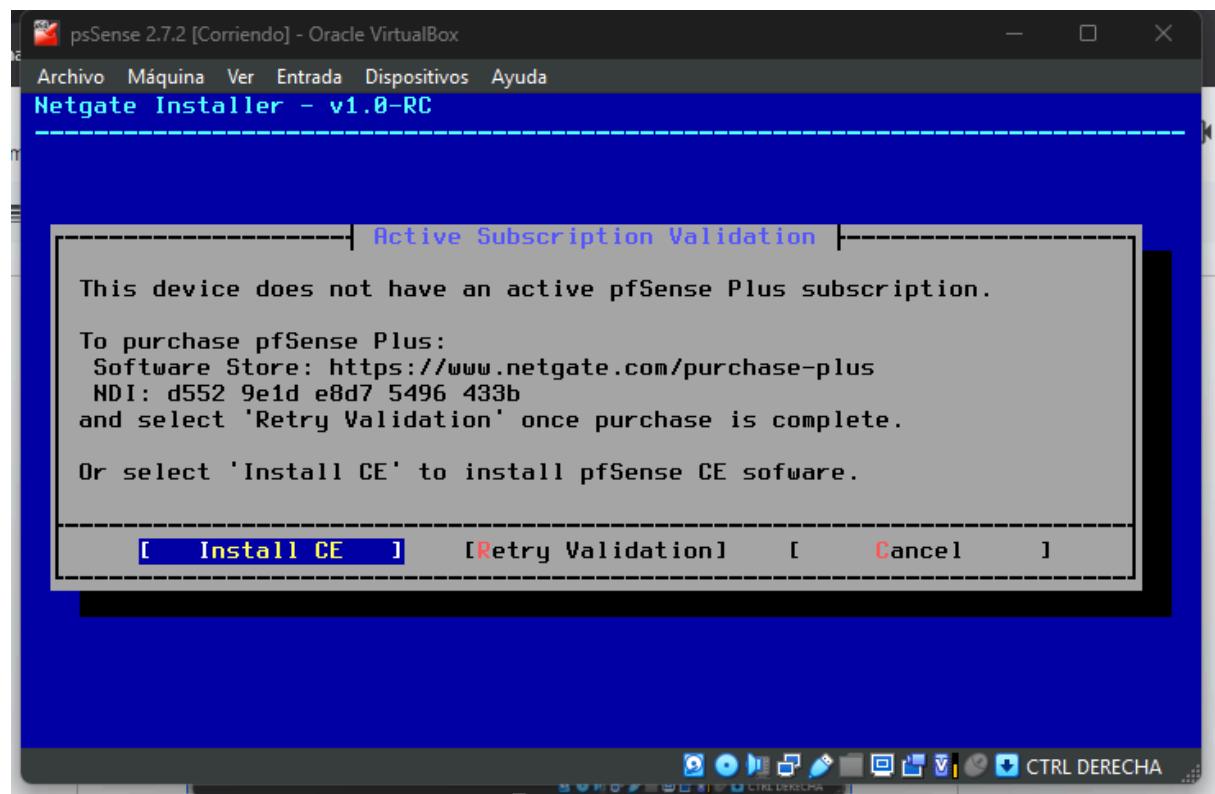


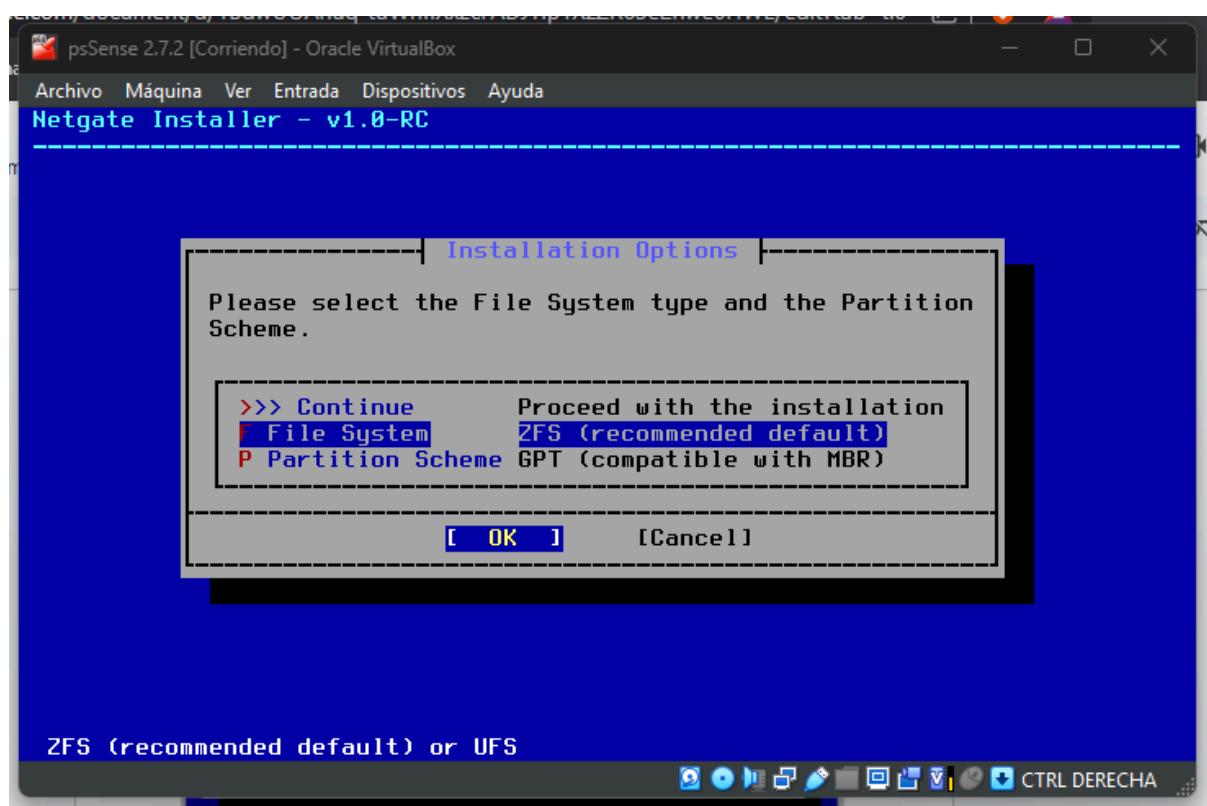
Para configurarla la dejaremos con una ip estática y deshabilitamos el dhcp por ahora.

Una vez configuradas las interfaces de red confirmamos para continuar la instalación.



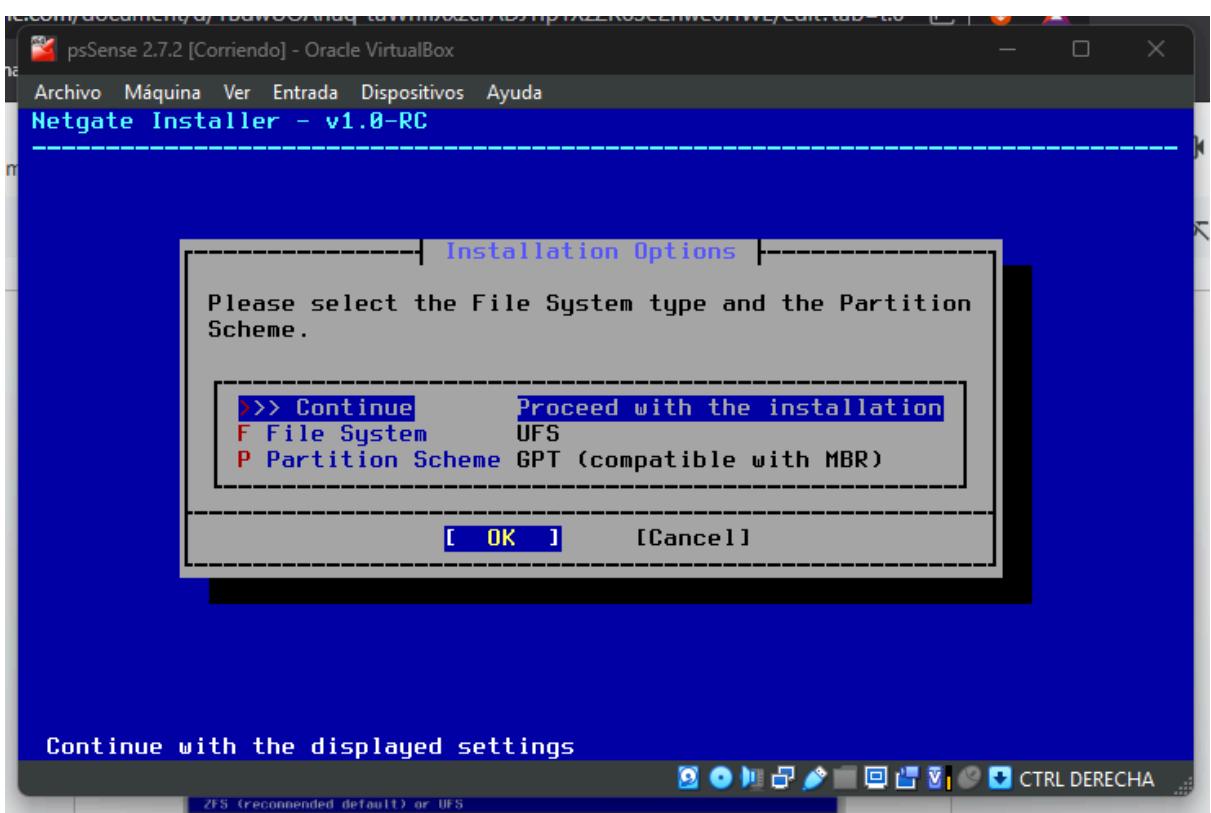
Verifica conexión a internet que todo esté configurado y nos advierte que no tenemos el servicio plus activado pero continuamos con install CE.



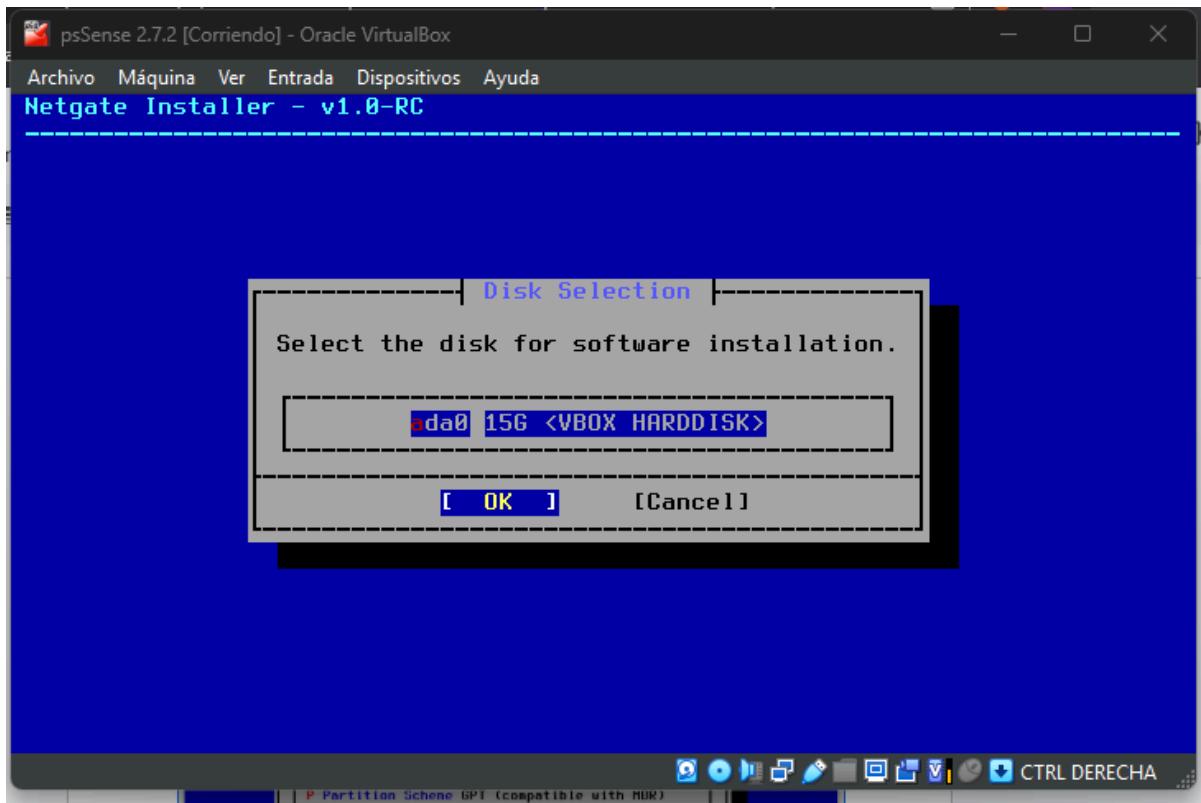


La instalación la hacemos en modo ZFS.

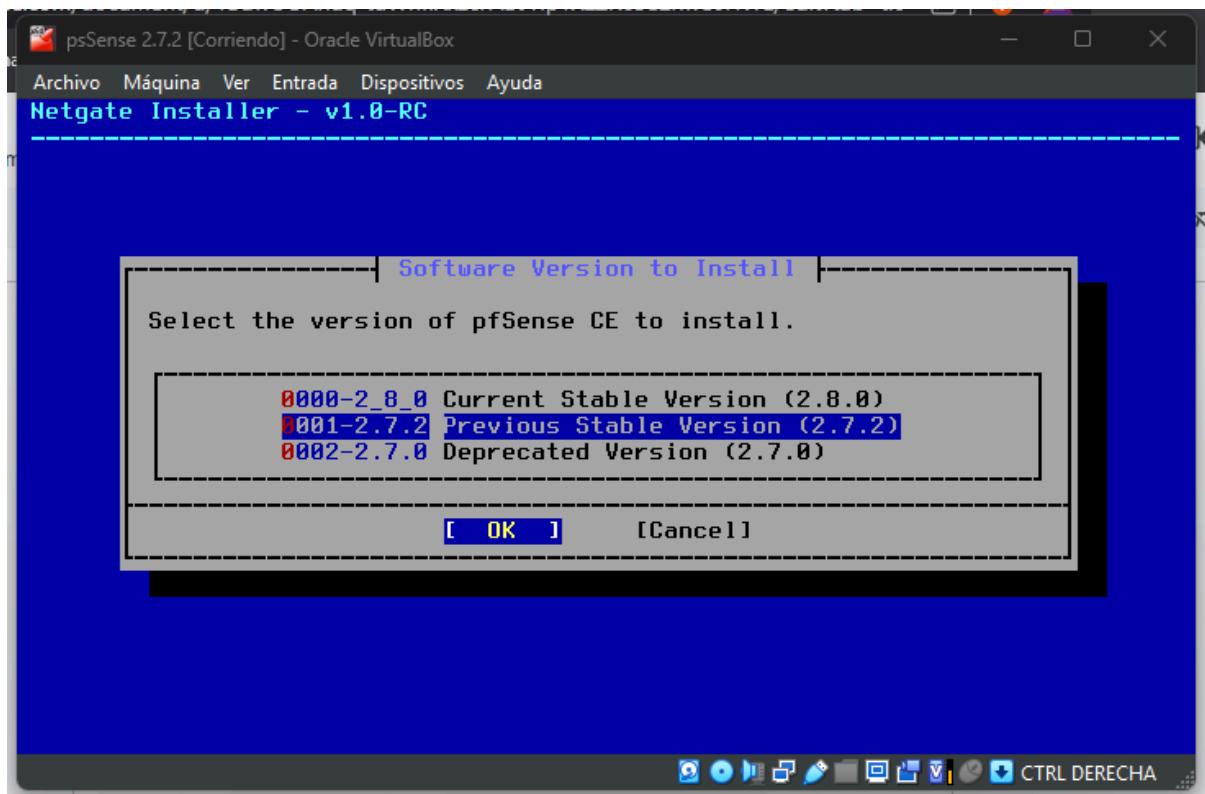
Dejamos el servicio de archivos como está y damos ok.



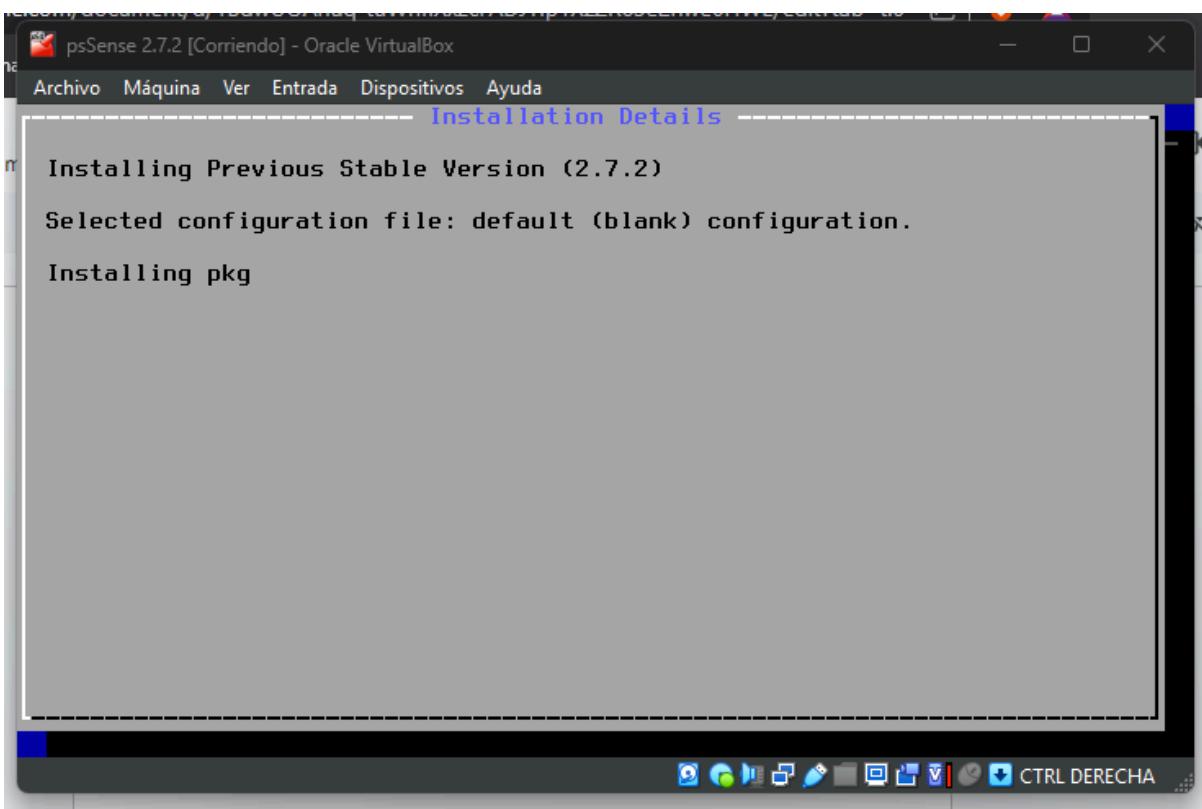
Seleccionamos el disco que creamos para la instalación.



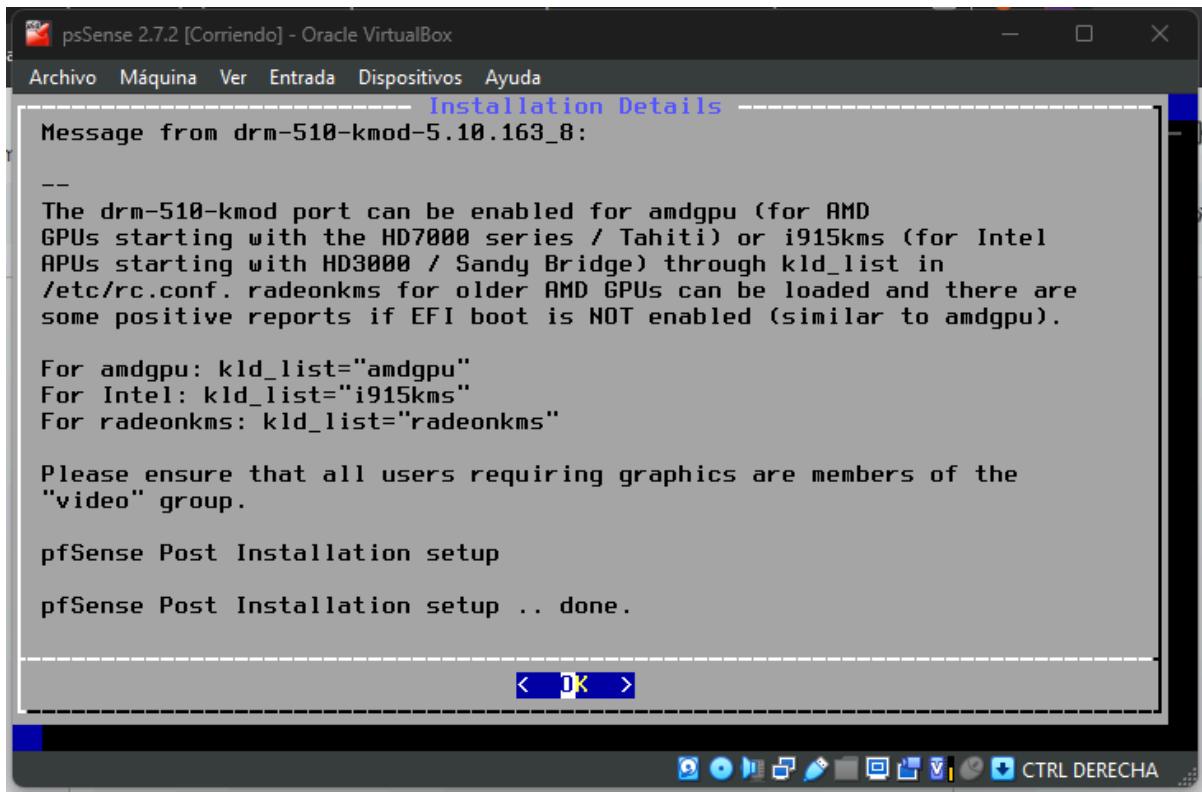
Nos muestra las versiones disponibles a instalar y seleccionamos la 2.7.2

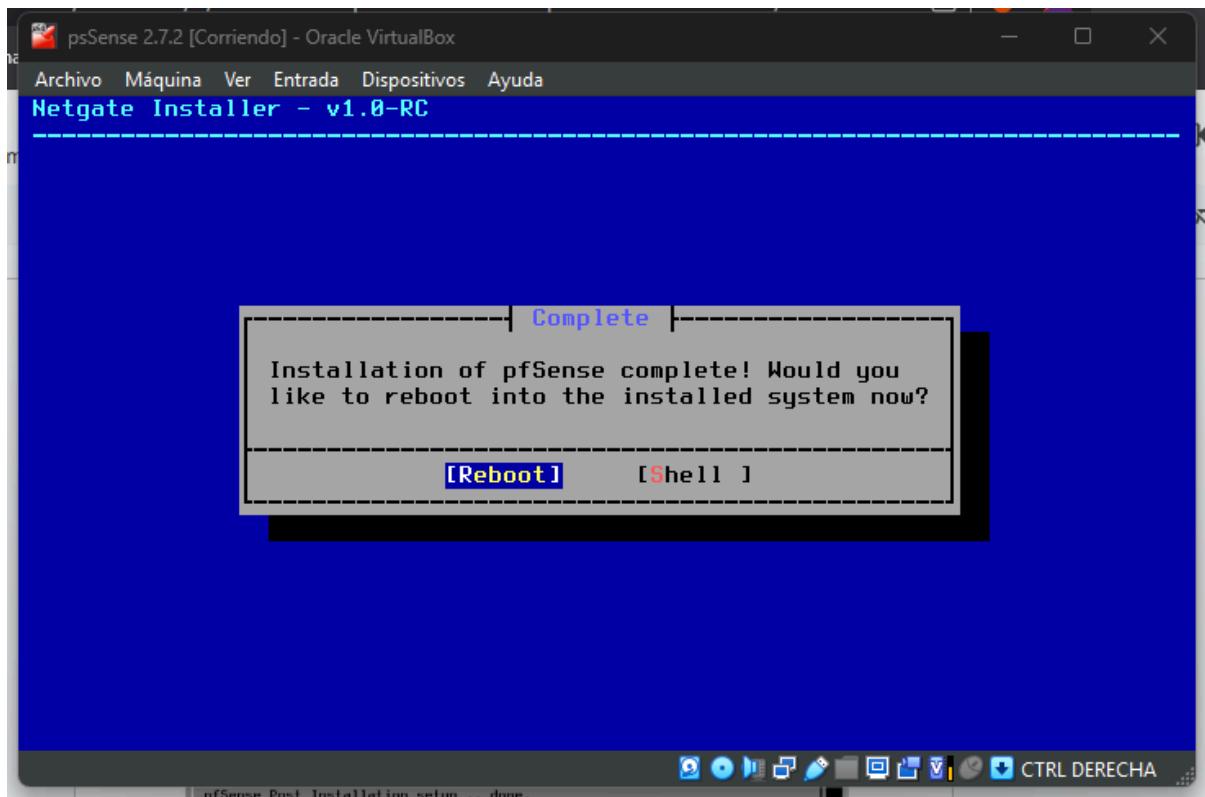


Inicia la instalación y debemos esperar a que instale toda la paquetería necesaria.

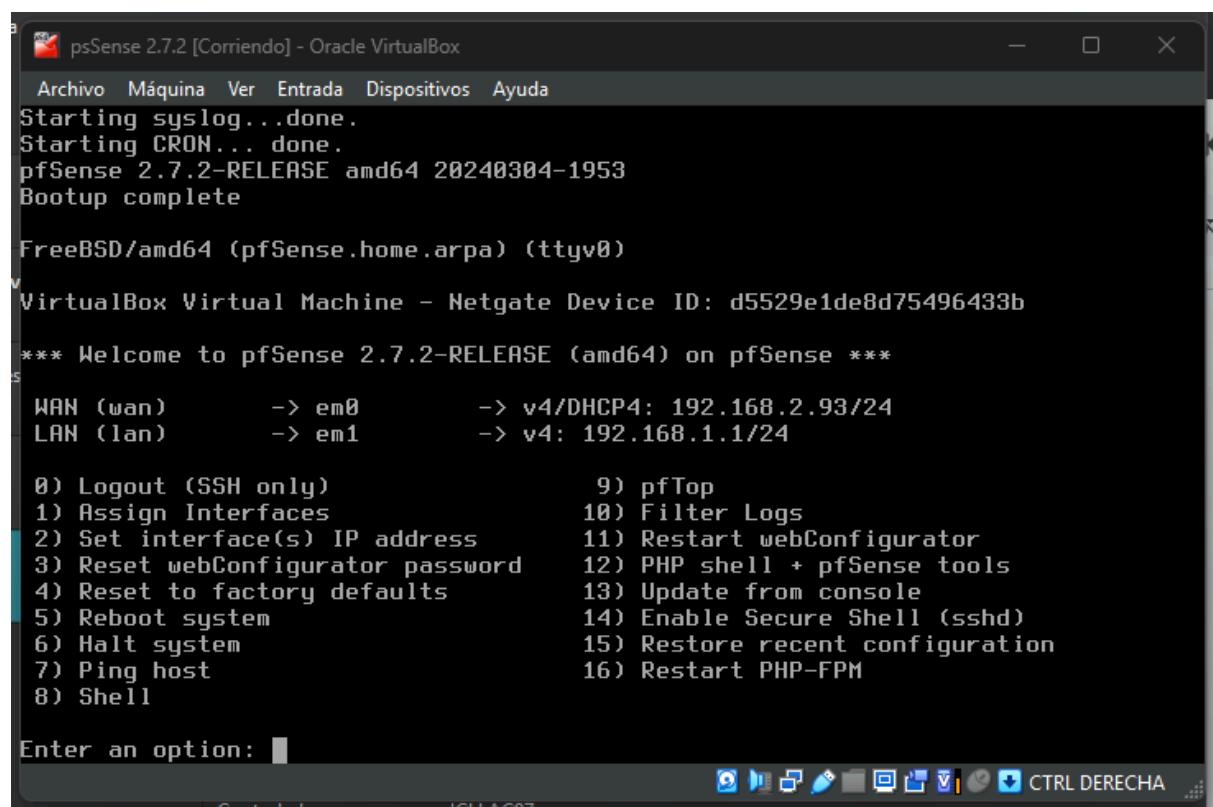


En un punto de la instalación nos pide configurar la tarjeta de video del equipo, damos ok y ya quedaría instalado el servicio.





Se debe quitar la iso configurada de inicio y arrancamos la maquina, esta sería la interface final después de instalar.



Para poder tener comunicación inicialmente debemos desactivar el firewall, seleccionamos la opción 8 y ejecutamos el siguiente comando: pfctl-d

```

psSense 2.7.2 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: d5529e1de8d75496433b

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.2.93/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

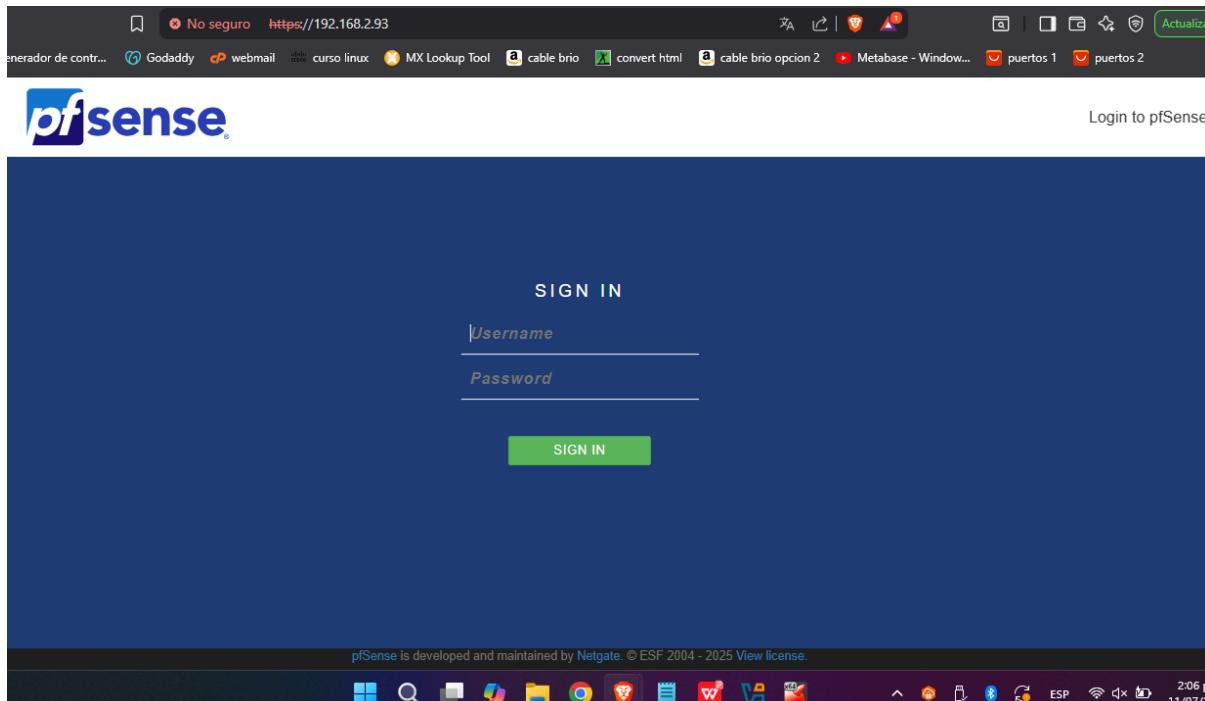
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable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

Enter an option: 8

[2.7.2-RELEASE][root@pfSense.home.arpa]/root: pfctl -d
pf disabled
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:

```

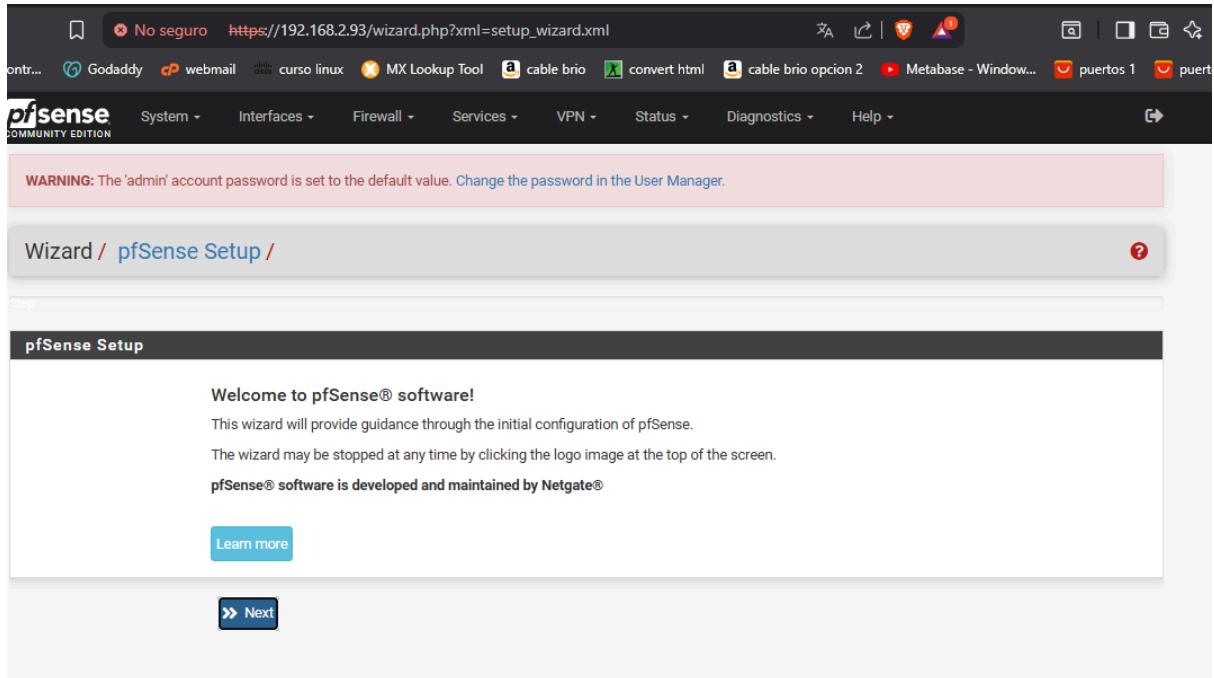
Una vez terminada la instalación y desactivado el firewall ponemos la dirección ip asignada al pfSense en el navegador de preferencia y ya nos cargó el login del entorno gráfico.



User: admin

Pass: pfsense

ya tenemos nuestra primera vista del panel.



Iniciamos la configuración básica de nuestro pfSense, ponemos nuestro nombre del equipo, puede ser cualquiera, seguido del dominio local también puede ser cualquiera y en dns configuramos los que nos dan salida a internet en este caso configuramos los 8.8.8.8 y 1.1.1.1

General Information	
On this screen the general pfSense parameters will be set.	
Hostname	<input type="text" value="pfSense"/>
Name of the firewall host, without domain part.	
Examples: pfSense, firewall, edgefw	
Domain	<input type="text" value="lab.local"/>
Domain name for the firewall.	
Examples: home.arpa, example.com	
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.	
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.	
Primary DNS Server	<input type="text" value="8.8.8.8"/>
Secondary DNS Server	<input type="text" value="1.1.1.1"/>
Override DNS	<input checked="" type="checkbox"/>
Allow DNS servers to be overridden by DHCP/PPP on WAN	
» Next	

En el siguiente paso se procede a configurar las interfaces de red, para nuestra práctica se deja como dhcp para que pueda trabajar en cualquier red.

Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType: **DHCP**

General configuration

MAC Address	<input type="text"/>
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.	
MTU	<input type="text"/>
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.	
MSS	<input type="text"/>
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.	

En la parte final se deseleccionan las 2 últimas casillas para el entorno de pruebas nuevamente.
En el siguiente paso se configura la interface LAN, para nuestro ejemplo configuraremos

RFC1918 Networks

Block RFC1918 Private Networks Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks Block non-Internet routed networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

>> Next

192.168.15.1/24

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address: **192.168.15.1**

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: **24**

>> Next

Con esto configurado ya terminamos lo básico para el nuestro pfSense.

The screenshot shows the final step of the pfSense Setup Wizard. The title bar reads "Wizard / pfSense Setup / Wizard completed." A progress bar at the top indicates "Step 9 of 9". The main content area has a dark header bar with the text "Wizard completed.". Below this, a message says "Congratulations! pfSense is now configured." followed by a note about checking for software updates. A green button labeled "Check for updates" is visible. Another message encourages users to remember they're here to help, with a link to learn about Netgate support services. A section titled "User survey" asks users to help improve pfSense software by taking a short survey, with a link to an anonymous user survey. A "Useful resources" section lists links to the website, store, forum, and newsletter. At the bottom, a blue "Finish" button is visible.

Reiniciamos la máquina, desactivamos nuevamente el firewall e ingresamos nuevamente por interfaz web, aceptamos términos y condiciones y listo ya tenemos nuestro panel principal.

No seguro https://192.168.2.93

Godaddy webmail curso linux MX Lookup Tool cable brio convert html cable brio opcion 2 Metabase - Window...

pfSense COMMUNITY EDITION

Copyright and Trademark Notices.

Copyright® 2004-2016, Electric Sheep Fencing, LLC ("ESF"). All Rights Reserved.
 Copyright® 2014-2025, Rubicon Communications, LLC d/b/a Netgate ("Netgate"). All Rights Reserved.

All logos, text, and content of ESF and/or Netgate, including underlying HTML code, designs, and graphics used and/or depicted herein are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of ESF and/or Netgate.

"pfSense®" is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All other trademarks shown herein are owned by the respective companies or persons indicated.

pfSense® software is open source and distributed under the Apache 2.0 license. However, no commercial distribution of ESF and/or Netgate software is allowed without the prior written consent of ESF and/or Netgate.

ESF and/or Netgate make no warranty of any kind, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. ESF and/or Netgate shall not be liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of any software, information, or material.

Restricted Rights Legend.

No part of ESF and/or Netgate's information or materials may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of ESF and/or Netgate. The information contained herein is subject to change without notice.

Use, duplication or disclosure by the U.S. Government may be subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance.

The export and re-export of software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, Licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government's Enemies List; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign

No seguro https://192.168.2.93

Godaddy webmail curso linux MX Lookup Tool cable brio convert html cable brio opcion 2 Metabase - Window... puer...

pfSense COMMUNITY EDITION

Status / Dashboard

System Information

Name	pfSense.lab.local
User	admin@192.168.2.104 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: d5529e1de8d75496433b
BIOS	Vendor: innoteck GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.2-RELEASE (amd64) built on Mon Mar 4 14:53:00 -05 2024 FreeBSD 14.0-CURRENT
CPU Type	Intel(R) Core(TM) i3-1005G1 CPU @ 1.20GHz 2 CPUs: 1 package(s) x 2 cache groups x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	01 Hour 21 Minutes 13 Seconds
Current date/time	Fri Jul 11 15:25:24 -05 2025

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- [Upgrade Your Support](#)
- [Community Support Resources](#)
- [Netgate Global Support FAQ](#)
- [Official pfSense Training by Netgate](#)
- [Netgate Professional Services](#)
- [Visit Netgate.com](#)

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your Netgate Device ID (NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#).

Los primeros pasos a realizar sería agregar un usuario y deshabilitar el administrador.

The screenshot shows the pfSense Community Edition interface. In the top navigation bar, 'System' is selected. Under 'System Info', there is a table with various system details. The 'User Manager' link is highlighted with a red box.

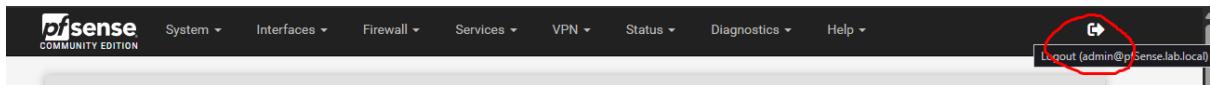
	Name	User	System	BIOS	Version
Name	pfSense	Register	Machine	Update	built on Mon Mar 4 14:53:01 2019 (d64)
User	Administrator	Logout			
System	pfSense				
BIOS	5529e				
Version	c 1.200				

The screenshot shows the 'User Manager / Users' page. The 'Users' tab is selected. A table lists the users, showing one entry for 'admin' with the status '✓' and group 'admins'. At the bottom right, there are 'Add' and 'Delete' buttons.

Username	Full name	Status	Groups	Actions
admin	System Administrator	✓	admins	

Se ingresan los datos requeridos, usuario y password, los demás campos se dejan como están. Cerrado el nuevo usuario nos deslogueamos y nos logueamos con el nuevo usuario.

The screenshot shows the 'User Properties' form. The 'Defined by' field is set to 'USER'. The 'Username' field is filled with 'sysadmin'. The 'Password' field contains two masked password entries. The 'Full name' field is empty. The 'Expiration date' field is also empty. The 'Custom Settings' checkbox is unchecked. In the 'Group membership' section, the 'Not member of' list is empty and the 'Member of' list contains 'admins'. At the bottom, there are buttons for 'Move to "Member of" list' and 'Move to "Not member of" list'.



Una vez logueado con el usuario nuevo vamos a usuarios nuevamente y seleccionamos la opción de usuario no puede loguearse.

User Properties	
Defined by	SYSTEM
Disabled	<input checked="" type="checkbox"/> This user cannot login
Username	admin
Password	Password
Full name	System Administrator User's full name, for administrative information only

Administrativamente ya estaría configurado, ahora vamos a iniciar con las reglas de firewall, vamos a crear una regla para que las ips de la red wan se puedan conectar sin necesidad de desactivar el firewall.

Ingresamos a firewall - rules - y seleccionamos la interface wan.

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
No rules are currently defined for this interface All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.											
<input style="border: 2px solid red; color: red; background-color: #fff; border-radius: 5px; padding: 5px; margin-right: 5px;" type="button" value="Add"/> <input style="color: green; background-color: #fff; border-radius: 5px; padding: 5px;" type="button" value="Add"/> <input style="color: red; background-color: #fff; border-radius: 5px; padding: 5px;" type="button" value="Delete"/> <input style="color: blue; background-color: #fff; border-radius: 5px; padding: 5px;" type="button" value="Toggle"/> <input style="color: cyan; background-color: #fff; border-radius: 5px; padding: 5px;" type="button" value="Copy"/> <input style="color: blue; background-color: #fff; border-radius: 5px; padding: 5px;" type="button" value="Save"/> <input style="color: orange; background-color: #fff; border-radius: 5px; padding: 5px;" type="button" value="Separator"/>											

Edit Firewall Rule

Action	Pass		
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.			
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	WAN		
Choose the interface from which packets must come to match this rule.			
Address Family	IPv4		
Select the Internet Protocol version this rule applies to.			
Protocol	TCP		
Choose which IP protocol this rule should match.			
Source			
Source	<input type="checkbox"/> Invert match	WAN subnets	Source Address
Display Advanced			
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.			
Destination			
Destination	<input type="checkbox"/> Invert match	This Firewall (self)	Destination Address
Destination Port Range	HTTPS (443)	From	To
Custom Custom			
Specify the destination port or port range for this rule. The 'To' field may be left empty if only filtering a single port.			
Extra Options			
Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).		

Se habilita nuevamente el firewall con el comando pfctl -e y ya podemos conectarnos normalmente.

```

pfSense 2.7.2 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
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: 8

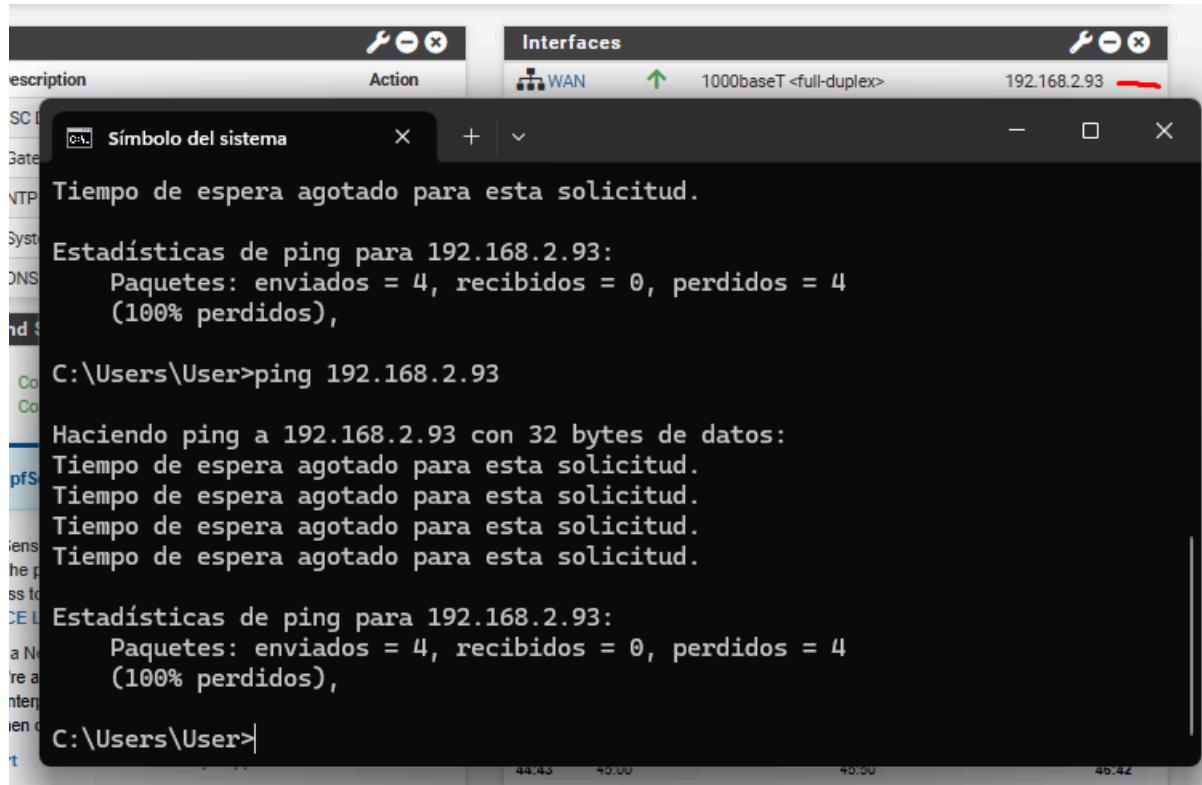
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: pfctl -d
pf disabled
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
Message from syslogd@pfSense at Dec 25 10:29:21 ...
php-fpm[394]: /index.php: Successful login for user 'admin' from: 192.168.1.161
(Local Database)

[2.7.2-RELEASE][root@pfSense.home.arpa]/root: pfctl -d
pf disabled
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
Message from syslogd@pfSense at Dec 25 10:35:02 ...
php-fpm[73933]: /index.php: Successful login for user 'clockworker' from: 192.168.1.161
(Local Database)

[2.7.2-RELEASE][root@pfSense.home.arpa]/root: pfctl -e
pfctl: pf already enabled
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: 

```

Vamos a configurar una nueva regla de firewall que habilite el ICMP (ping), como es un firewall todo queda desactivado, la ip del firewall 192.168.2.93



The screenshot shows a terminal window with the title "Símbolo del sistema". The window displays the following text:

```
Tiempo de espera agotado para esta solicitud.  
Estadísticas de ping para 192.168.2.93:  
Paquetes: enviados = 4, recibidos = 0, perdidos = 4  
(100% perdidos),  
C:\Users\User>ping 192.168.2.93  
  
Haciendo ping a 192.168.2.93 con 32 bytes de datos:  
Tiempo de espera agotado para esta solicitud.  
Estadísticas de ping para 192.168.2.93:  
Paquetes: enviados = 4, recibidos = 0, perdidos = 4  
(100% perdidos),  
C:\Users\User>
```

Vamos nuevamente a firewall - rules - wan y creamos la nueva regla.

Edit Firewall Rule

Action	Pass	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.	
Interface	WAN	Choose the interface from which packets must come to match this rule.	
Address Family	IPv4	Select the Internet Protocol version this rule applies to.	
Protocol	ICMP	Choose which IP protocol this rule should match.	
ICMP Subtypes	any Alternate Host Datagram conversion error Echo reply	For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.	
Source			
Source	<input type="checkbox"/> Invert match	WAN subnets	Source Address
Destination			
Destination	<input type="checkbox"/> Invert match	This Firewall (self)	Destination Address

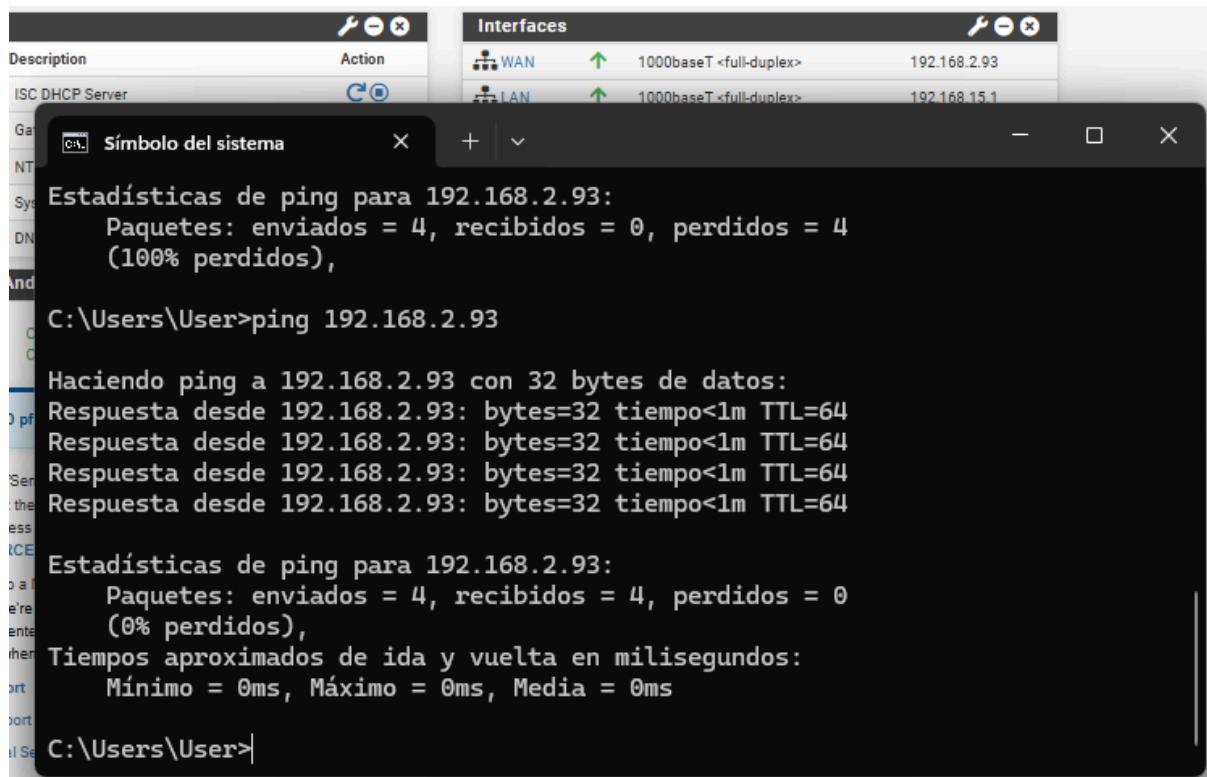
Ya podemos observar las 2 reglas creadas hasta el momento.

Firewall / Rules / WAN

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Floating	WAN	LAN																																				
Rules (Drag to Change Order) <table border="1"> <thead> <tr> <th></th> <th>States</th> <th>Protocol</th> <th>Source</th> <th>Port</th> <th>Destination</th> <th>Port</th> <th>Gateway</th> <th>Queue</th> <th>Schedule</th> <th>Description</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>✓ 0/0 B</td> <td>IPv4 ICMP</td> <td>WAN subnets</td> <td>*</td> <td>This Firewall (self)</td> <td>*</td> <td>*</td> <td>none</td> <td></td> <td></td> <td> </td> </tr> <tr> <td><input type="checkbox"/></td> <td>✓ 2/304 KiB</td> <td>IPv4 TCP</td> <td>WAN subnets</td> <td>*</td> <td>This Firewall (self)</td> <td>443 (HTTPS)</td> <td>*</td> <td>none</td> <td></td> <td></td> <td> </td> </tr> </tbody> </table>				States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	<input type="checkbox"/>	✓ 0/0 B	IPv4 ICMP	WAN subnets	*	This Firewall (self)	*	*	none				<input type="checkbox"/>	✓ 2/304 KiB	IPv4 TCP	WAN subnets	*	This Firewall (self)	443 (HTTPS)	*	none			
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions																											
<input type="checkbox"/>	✓ 0/0 B	IPv4 ICMP	WAN subnets	*	This Firewall (self)	*	*	none																														
<input type="checkbox"/>	✓ 2/304 KiB	IPv4 TCP	WAN subnets	*	This Firewall (self)	443 (HTTPS)	*	none																														
<input type="button" value="Add"/> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Toggle"/> <input type="button" value="Copy"/> <input type="button" value="Save"/> <input type="button" value="Separator"/>																																						

Realizamos la prueba nuevamente de ping y el resultado es exitoso.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Símbolo del sistema". It displays the output of a ping command to 192.168.2.93, showing 4 packets sent, 4 received, and 0 lost (0% loss). It also shows statistics for the connection. Above the terminal, there is a "Interfaces" window showing two network interfaces: "WAN" (1000baseT <full-duplex>) with IP 192.168.2.93 and "LAN" (1000baseT <full-duplex>) with IP 192.168.15.1.

```
Estadísticas de ping para 192.168.2.93:
  Paquetes: enviados = 4, recibidos = 0, perdidos = 4
              (100% perdidos),
C:\Users\User>ping 192.168.2.93

  Haciendo ping a 192.168.2.93 con 32 bytes de datos:
  Respuesta desde 192.168.2.93: bytes=32 tiempo<1m TTL=64
  Respuesta desde 192.168.2.93: bytes=32 tiempo<1m TTL=64
  Respuesta desde 192.168.2.93: bytes=32 tiempo<1m TTL=64
  Respuesta desde 192.168.2.93: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.2.93:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\User>
```

ANEXO 4 Política de Control de Acceso:

Política de Control de Acceso – Gestión de Contraseñas

1. Propósito

Establecer lineamientos que aseguren el acceso autorizado y seguro a la información mediante una gestión adecuada de contraseñas.

2. Alcance

Aplica a todos los usuarios, sistemas, aplicaciones, dispositivos y redes que requieran autenticación dentro de la organización.

3. Roles y Responsabilidades

Rol	Responsabilidad
Usuarios	Crear, proteger y actualizar contraseñas según esta política.
TI	Configurar y administrar controles técnicos.
Responsable SGSI	Auditar y actualizar la política periódicamente.

4. Normas de Contraseña

- Longitud mínima: **10 caracteres**.
- Requisitos de complejidad: combinación de letras (mayúsculas y minúsculas), números y símbolos.
- Reutilización: no repetir las últimas 2 contraseñas.
- Caducidad: renovar cada 90 días.
- Almacenamiento: cifrado seguro; nunca en texto plano.

5. Autenticación

- Autenticación Multifactor - MFA obligatorio para accesos al correo corporativo.
- Bloqueo automático tras 5 intentos fallidos consecutivos.

6. Uso Seguro

- No compartir contraseñas por canales no seguros.
- Usar gestores de contraseñas validados por TI.
- Cambiar la contraseña inmediatamente ante sospecha de exposición.
-

7. Concientización

- Capacitación anual.
- Difusión de buenas prácticas en la gestión de credenciales.

8. Revisión y Actualización

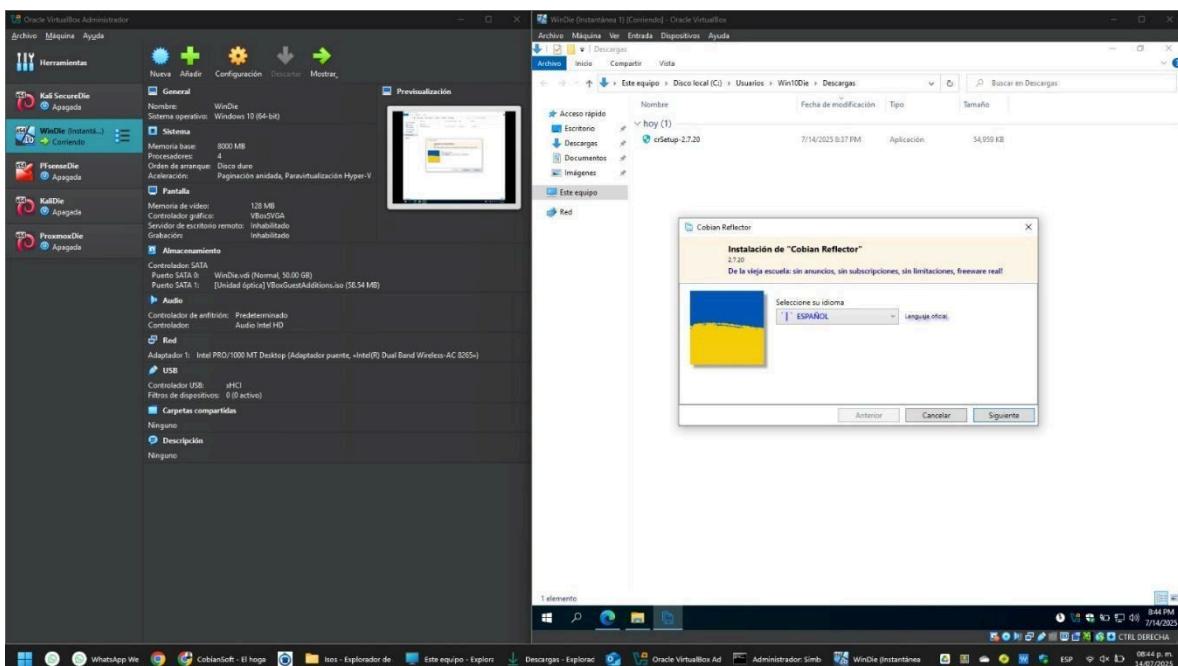
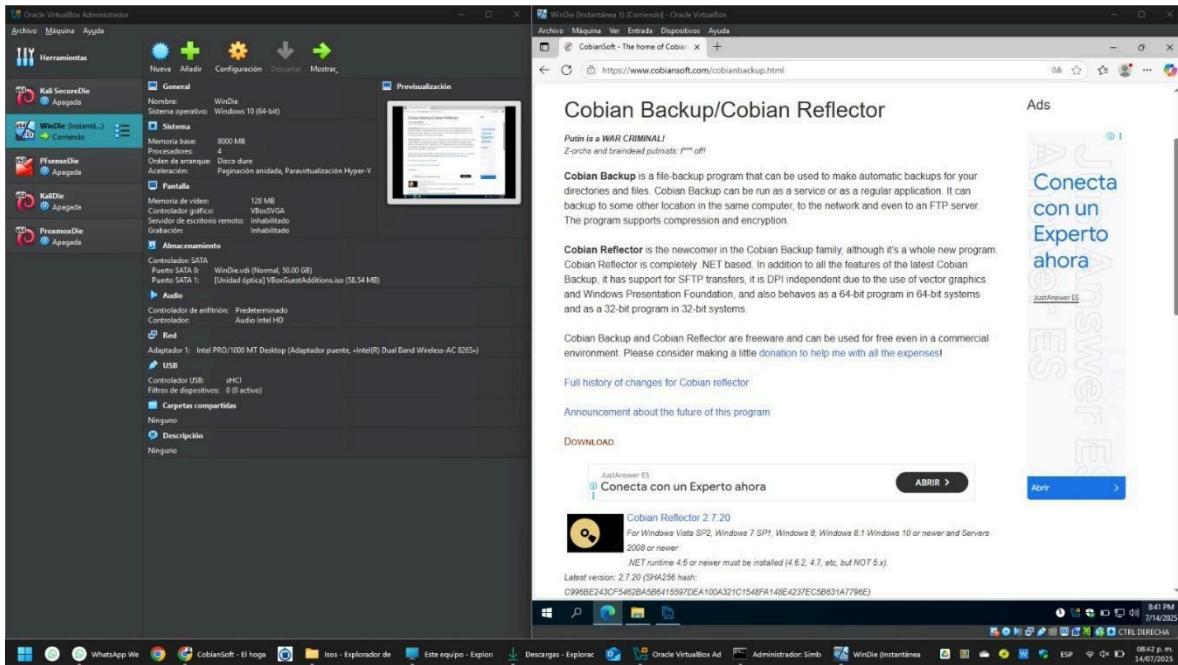
- Frecuencia: semestral.
 - Consideraciones: nuevas amenazas, tecnologías emergentes, auditorías SGSI.
-

ANEXO 5 Instalación Cobian:

BACKUP en WINDOWS con COBIAN REFLECTOR

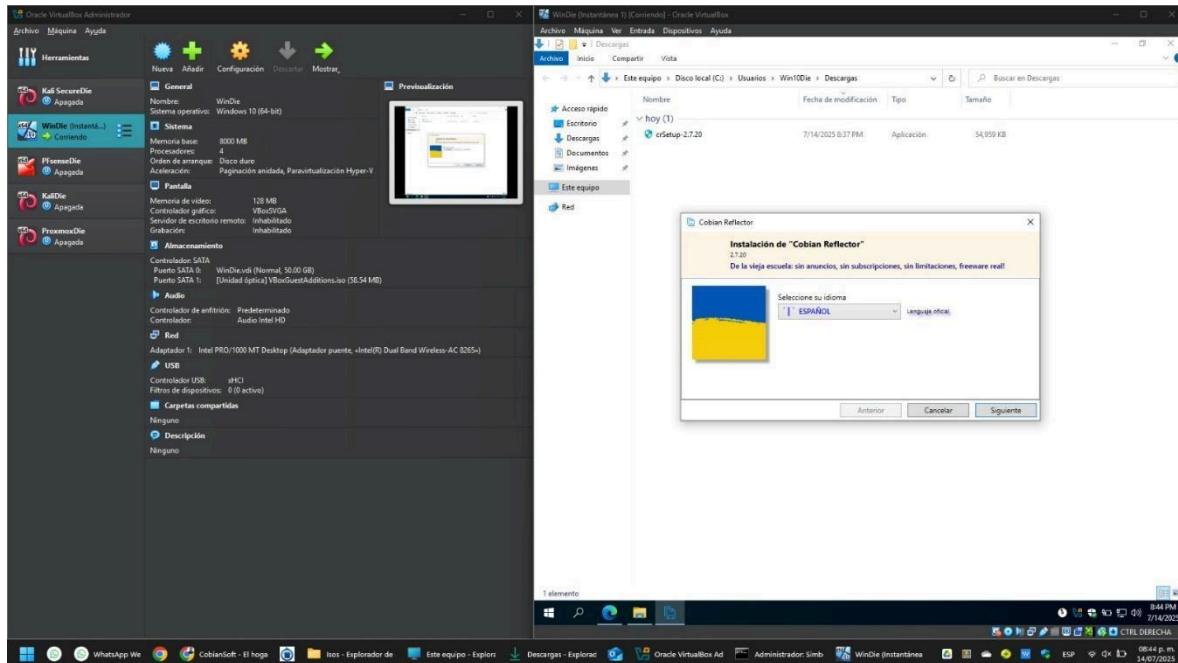
Cobian Reflector es una herramienta gratuita para realizar copias de seguridad en Windows que permite crear distintos tipos de respaldos: completos, incrementales y diferenciales. A continuación, se detalla el procedimiento para configurar cada tipo de copia de una carpeta de datos.

Descarga e instala Cobian Reflector desde la web oficial (cobiansoft.com).

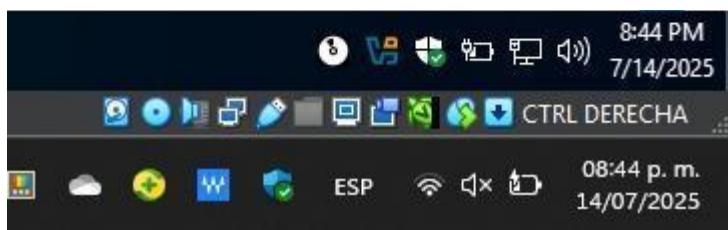




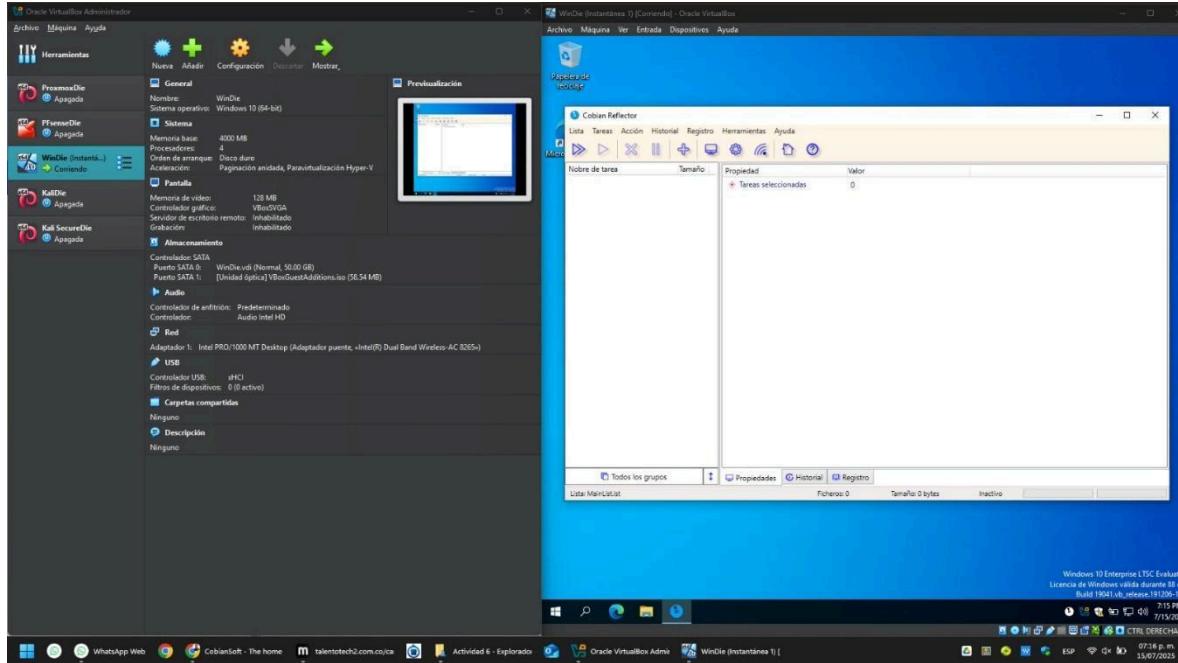
Elige español como idioma durante la instalación.



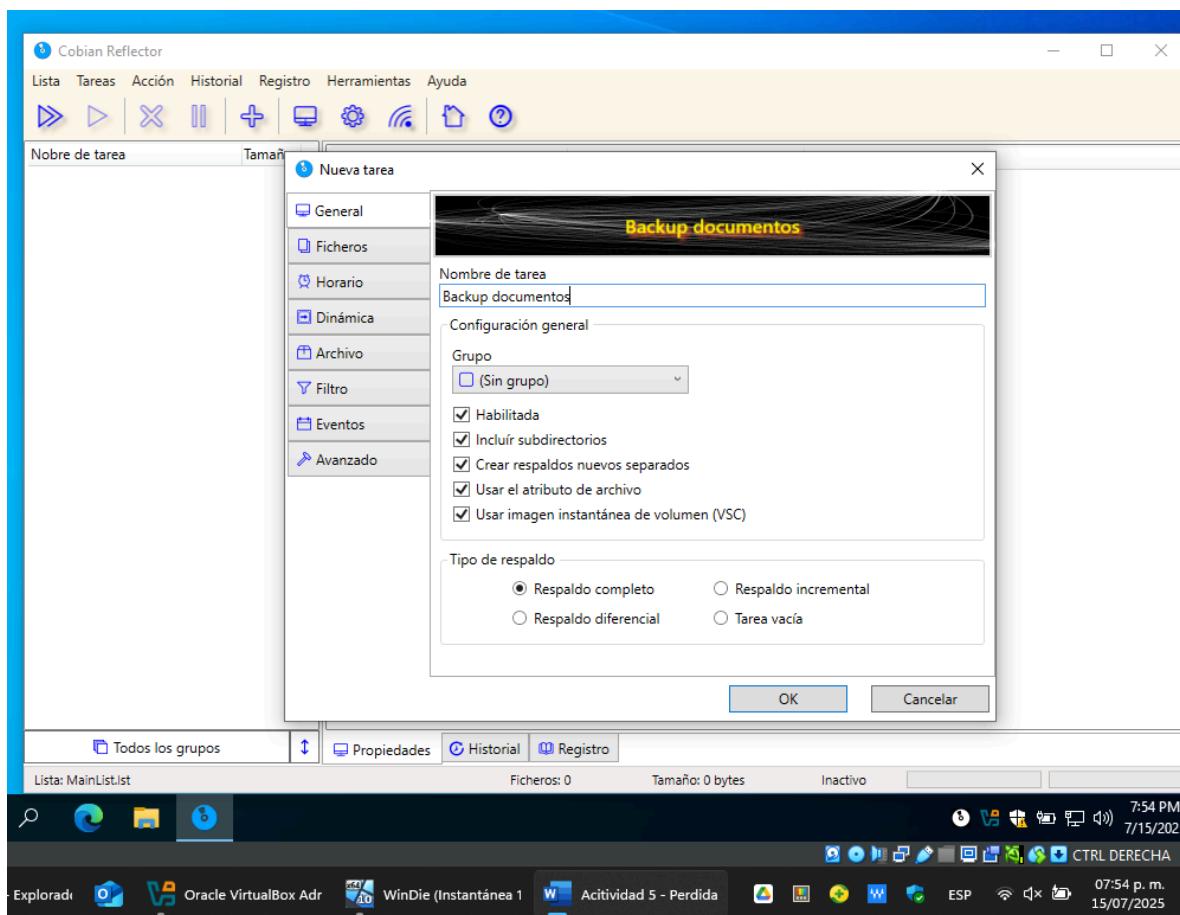
Selecciona la opción “Como un servicio” si deseas que el programa funcione incluso sin iniciar sesión.



Abre Cobian Reflector y haz clic en el botón “+” para crear una nueva tarea.

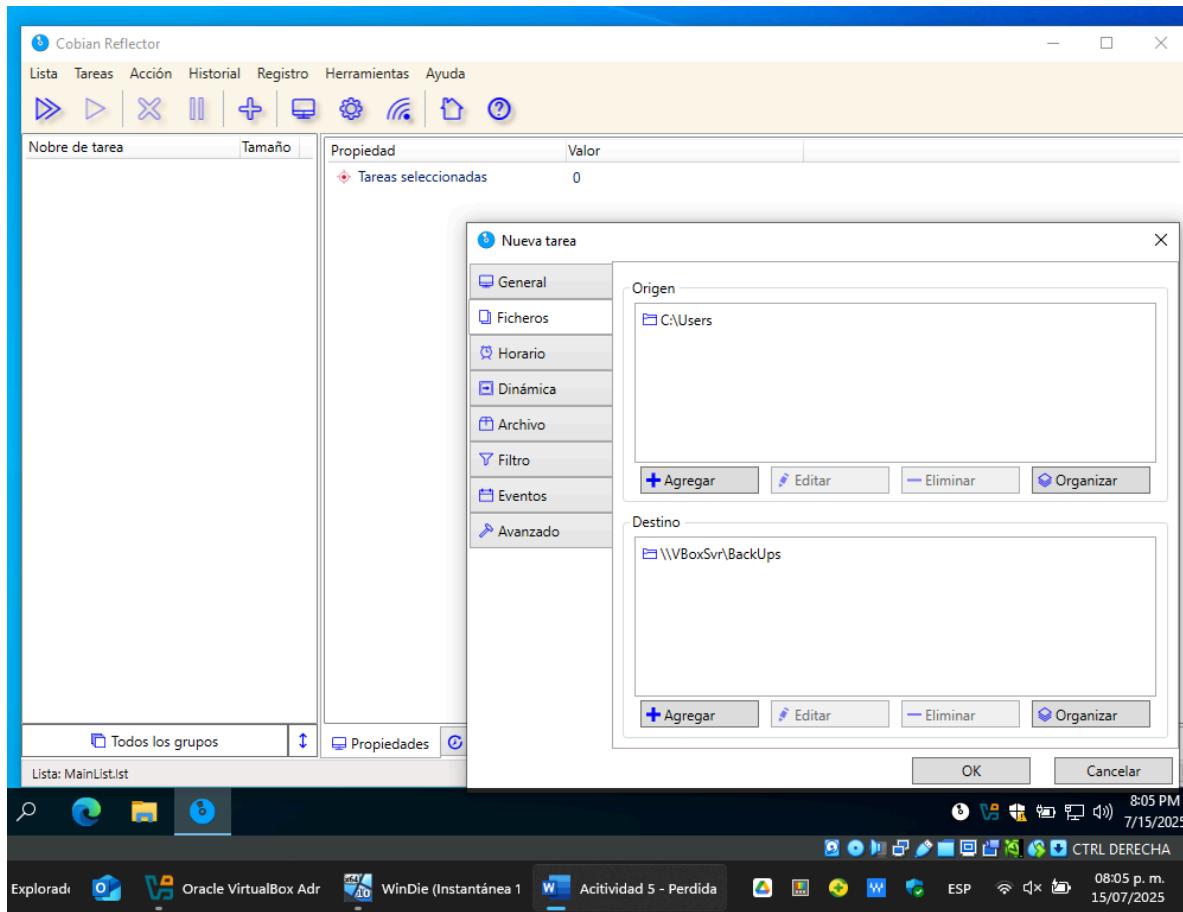


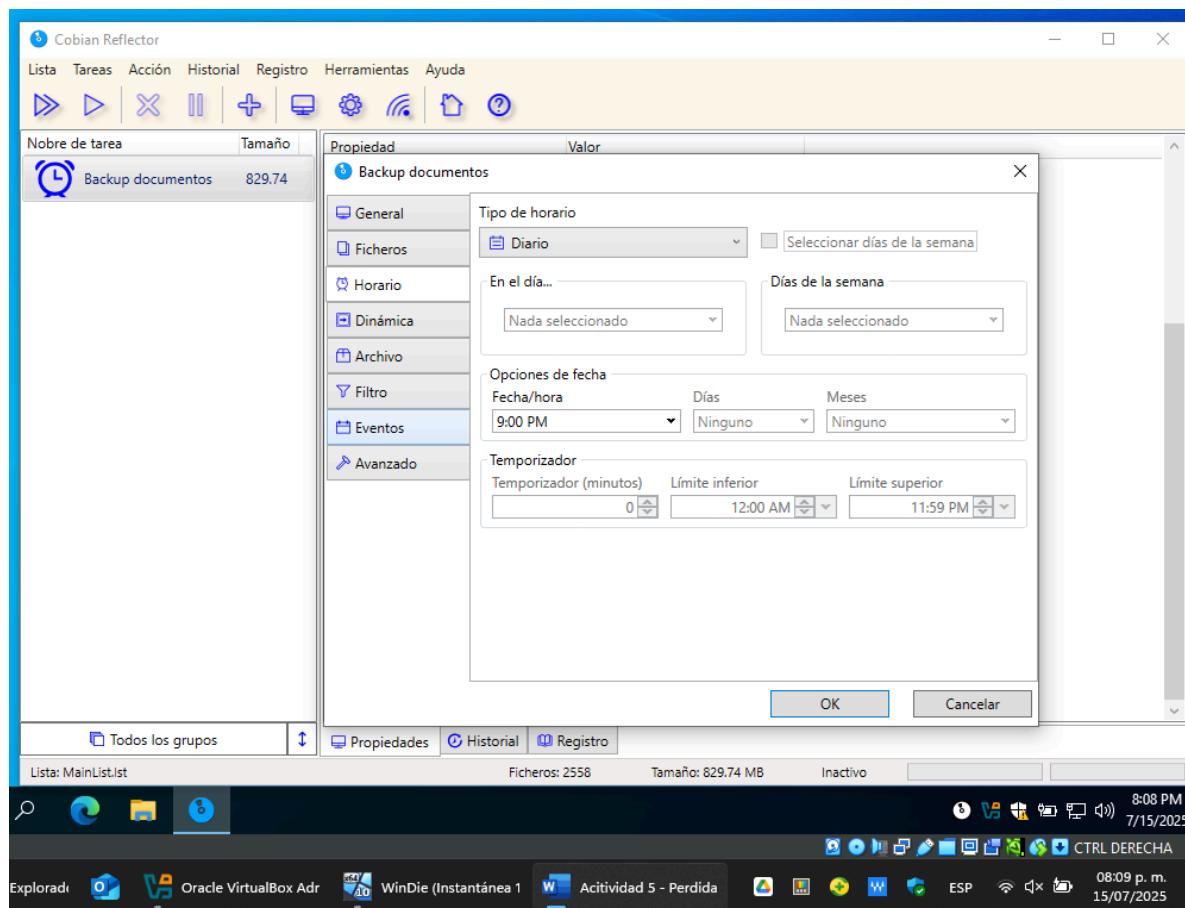
Asigna un nombre a la tarea (ejemplo: “Backup documentos”) y selecciona el tipo de respaldo ideal para tu necesidad:

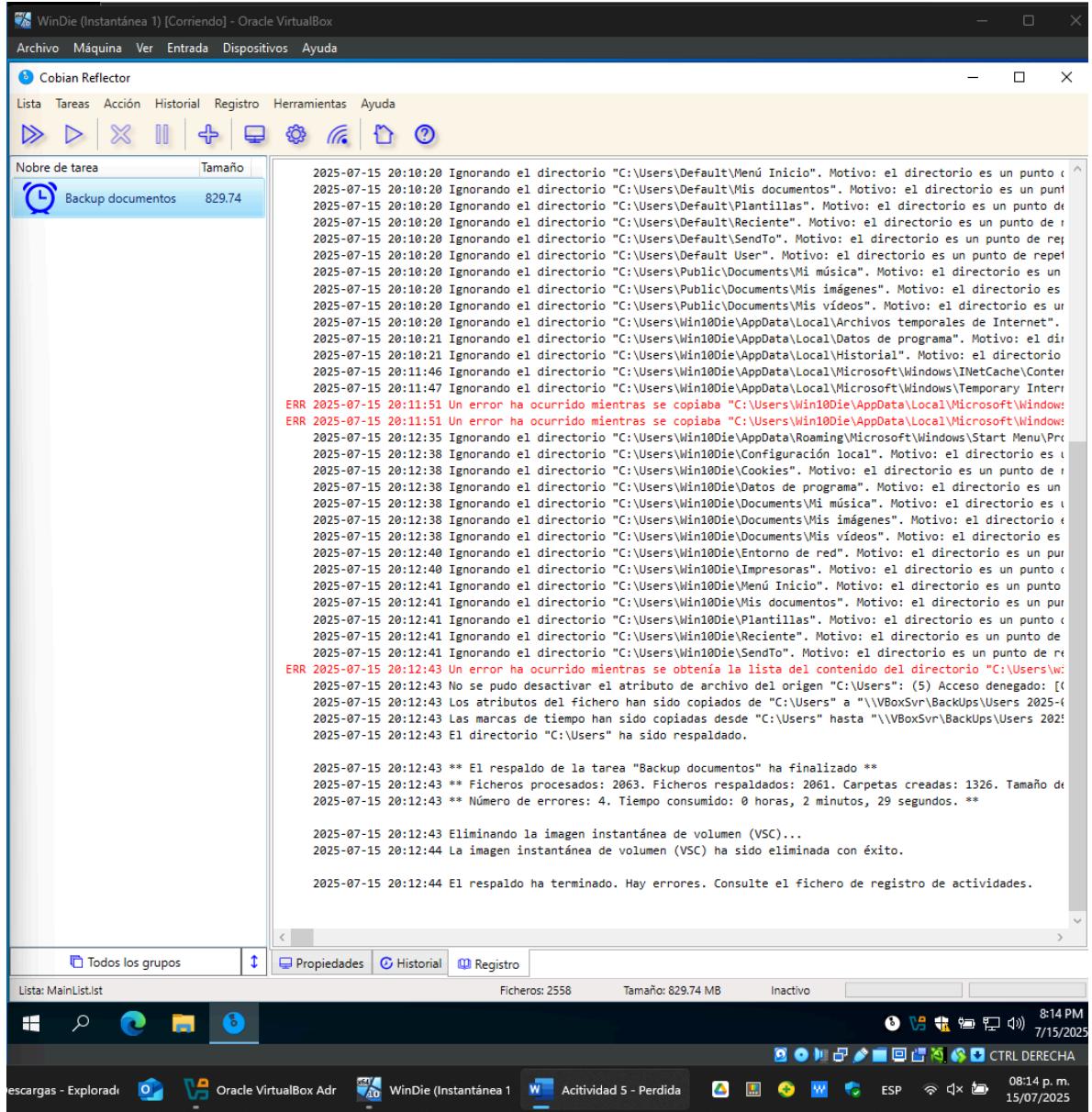


Copia completa

- Crea nueva tarea → Selecciona “Completa” → Agrega origen y destino → Define horario (opcional) → Ejecuta o programa.

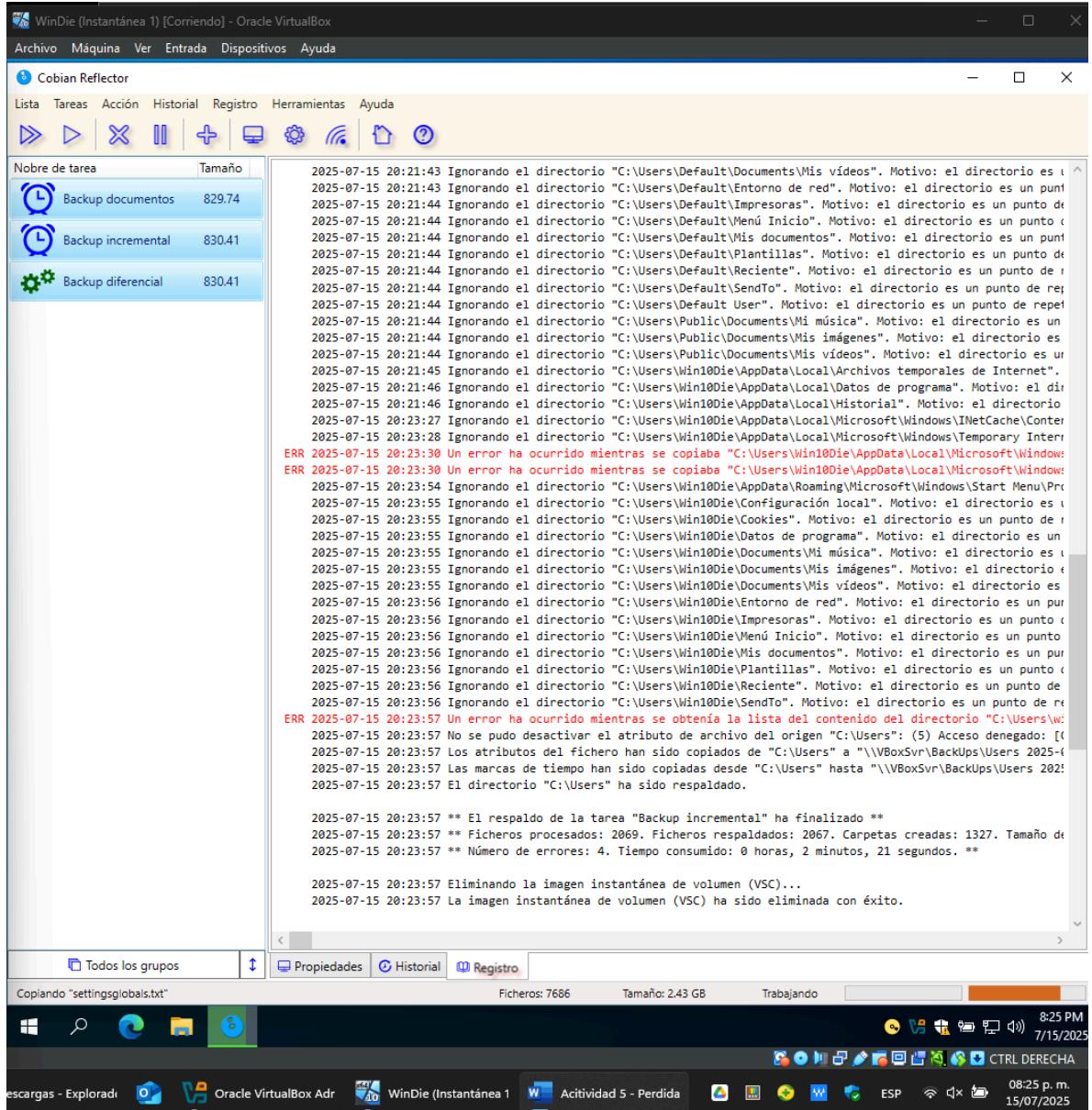






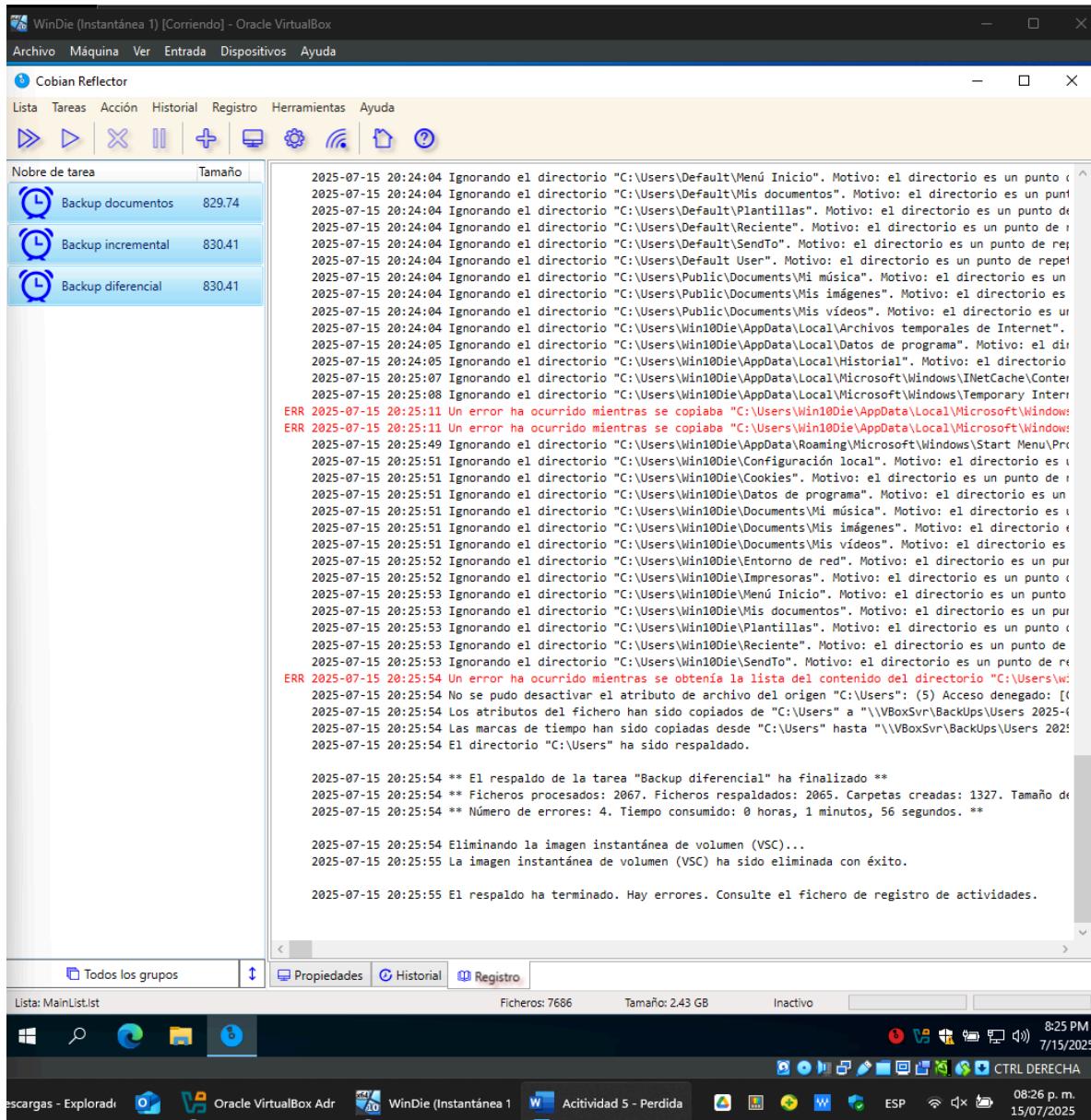
Copia incremental

- Se recomienda hacer primero una copia completa.
- Crea nueva tarea → Selecciona “Incremental” → Agrega origen y destino → Define el calendario → Ejecuta o programa.



Copia diferencial

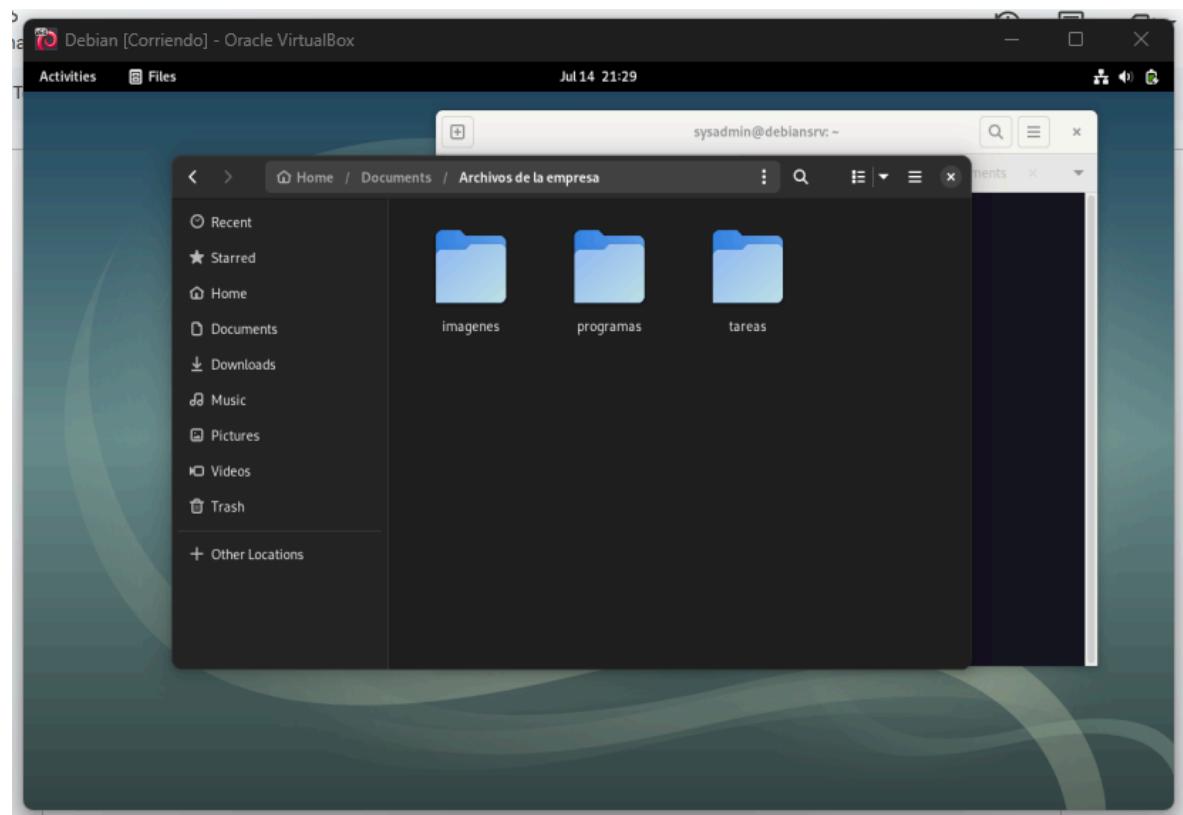
- Se debe haber realizado antes una copia completa.
 - Crea nueva tarea → Selecciona “Diferencial” → Agrega origen y destino → Programa según lo necesites → Ejecuta o programa.



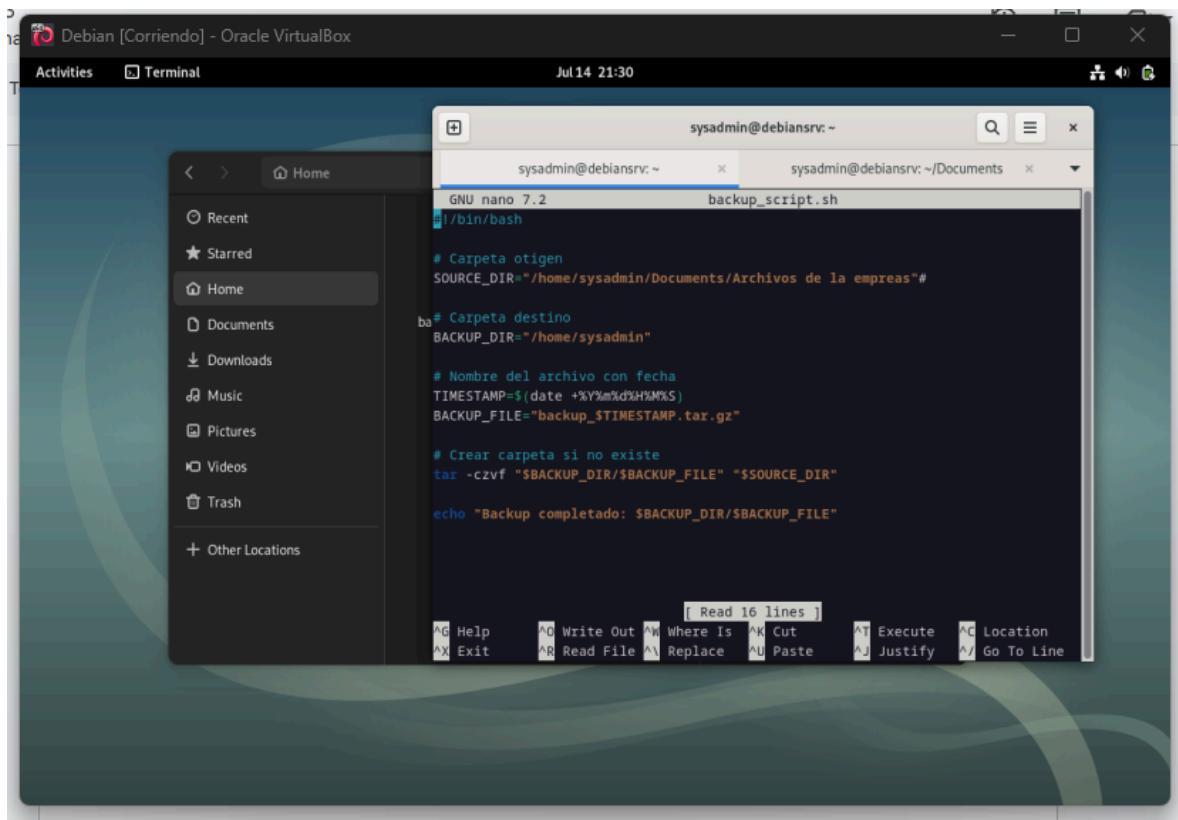
Puedes programar todas las tareas y ejecutarlas al mismo tiempo.

BACKUP COMPLETO EN LINUX (CRONTAB)

Vamos a realizar la configuración de un backup completo, iniciamos creando una carpeta con archivos en Documentos que es la carpeta a la cual le vamos a realizar el backup.



Tenemos que crear un script el cual realice una copia de la carpeta, la comprime y la guarda en otra ruta diferente.



Explicación del script:

`#!/bin/bash`: Indica que el script debe ser ejecutado con Bash.

`SOURCE_DIR`: La ruta del directorio que quieras respaldar. Hay que cambiar `"/home/tu_usuario/Documentos"` por la ruta correcta!

`BACKUP_DIR`: La ruta donde se guardarán los archivos de backup.

`TIMESTAMP=$(date +%Y%m%d%H%M%S)`: Genera la hora en el formato AñoMesDíaHoraMinutoSegundo.

`BACKUP_FILE`: Combina un prefijo con la marca de tiempo y la extensión `.tar.gz`.

`mkdir -p "$BACKUP_DIR"`: Crea el directorio de destino si no existe.

`tar -czvf "$BACKUP_DIR/$BACKUP_FILE" "$SOURCE_DIR"`: Este es el comando principal del backup:

c: Crea un nuevo archivo.

z: Comprime el archivo con gzip.

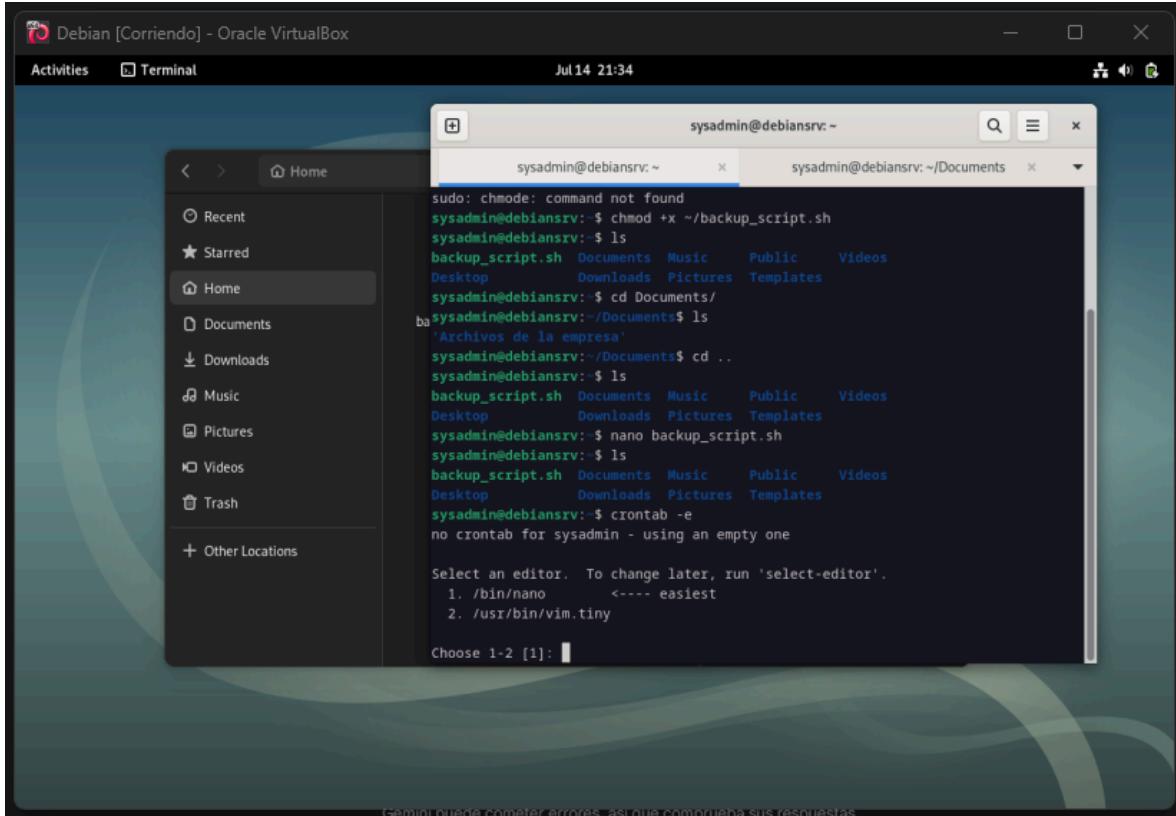
v: Muestra el progreso.

f: Especifica el nombre del archivo de salida.

find "\$BACKUP_DIR" -type f -name "*.tar.gz" -mtime +7 -delete: (Opcional) Este comando busca archivos .tar.gz en el directorio de backups que sean más antiguos de 7 días (+7) y los elimina. Esto es útil para gestionar el espacio en disco.

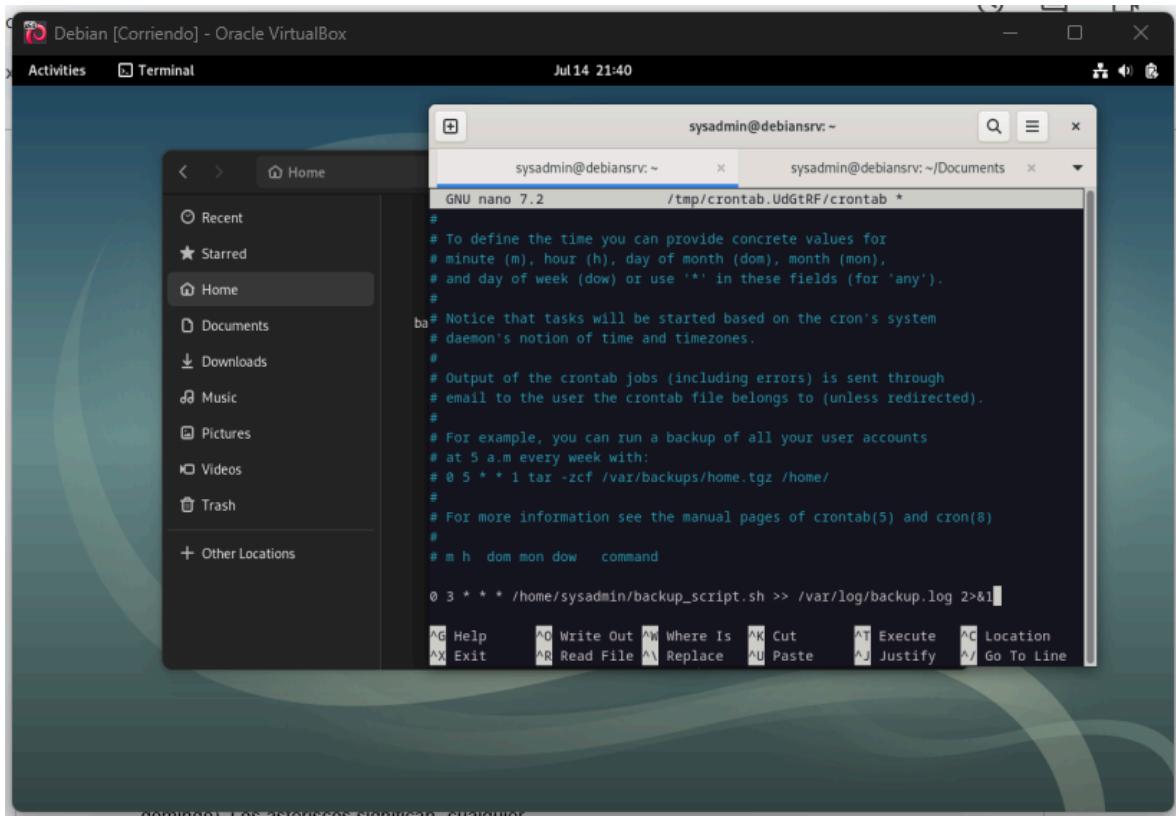
Se procede a configurar el crontab para que el programa se script automáticamente.

Ejecutamos el comando crontab -e y elegimos nano como editor de texto.



Agregamos la siguiente línea de comando:

```
0 3 * * * /home/tu_usuario/backup_script.sh >> /var/log/backup.log 2>&1
```



Explicación de la entrada de Crontab:

0 3 * * *: Esta es la "expresión cron" que define cuándo se ejecutará el comando.

El primer 0: Minuto (0 a 59) - En este caso, el minuto 0 de la hora.

El 3: Hora (0 a 23) - En este caso, las 3 AM.

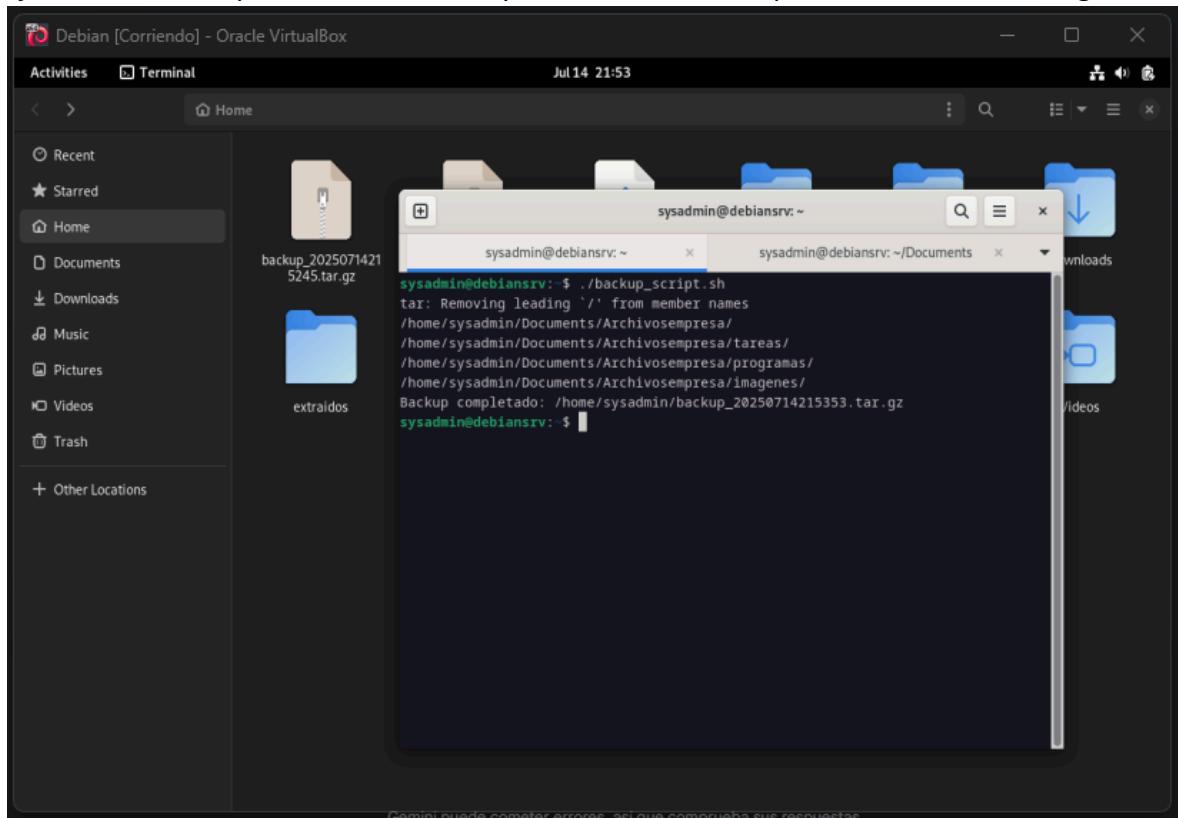
Los tres *: Día del mes (1 a 31), Mes (1 a 12), Día de la semana (0 a 7, donde 0 y 7 son domingo). Los asteriscos significan "cualquier".

Combinado, 0 3 * * * significa "cada día a las 3:00 AM".

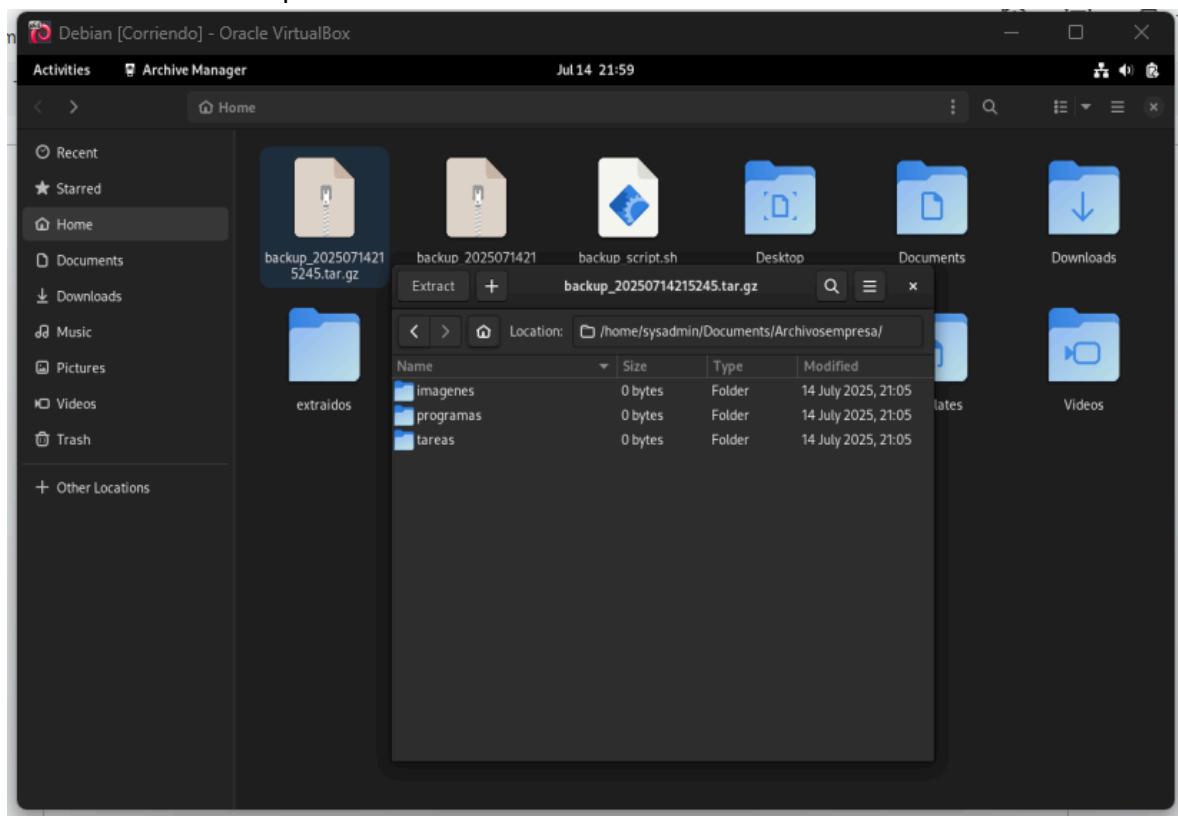
/home/tu_usuario/backup_script.sh: Es la ruta completa a tu script de backup.

>> /var/log/backup.log 2>&1: Esto redirige la salida estándar (stdout) y los errores estándar (stderr) del script a un archivo de registro llamado /var/log/backup.log. Es muy importante para depurar si algo sale mal. Puedes cambiar la ruta del archivo de log.

Ejecutamos el script de forma manual y crea el archivo comprimido en la ruta configurada.



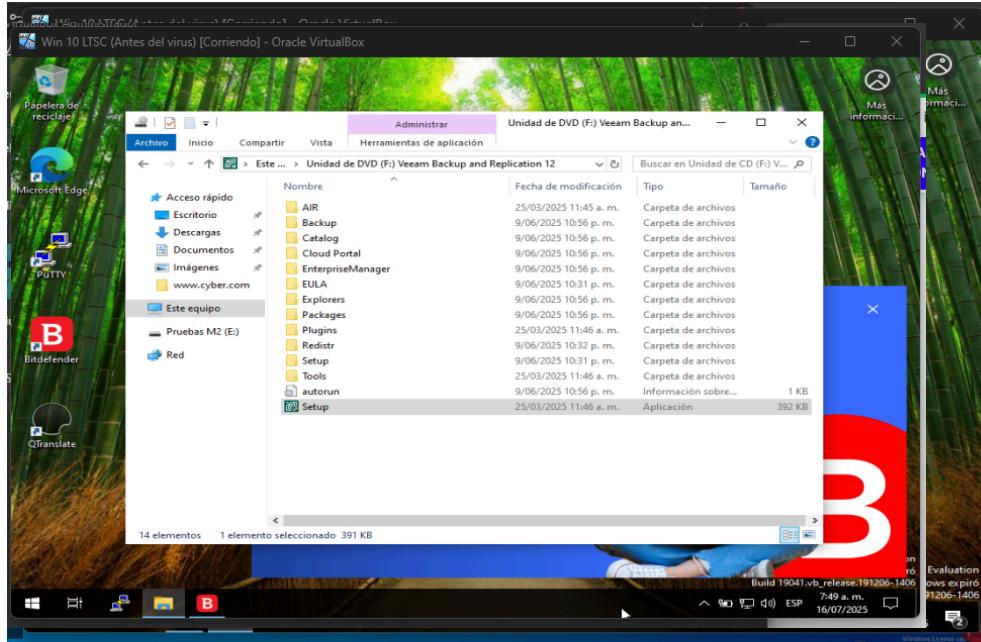
Se verifica la carpeta comprimida y efectivamente se encuentran las carpetas a las cuales se les realizó el backup.



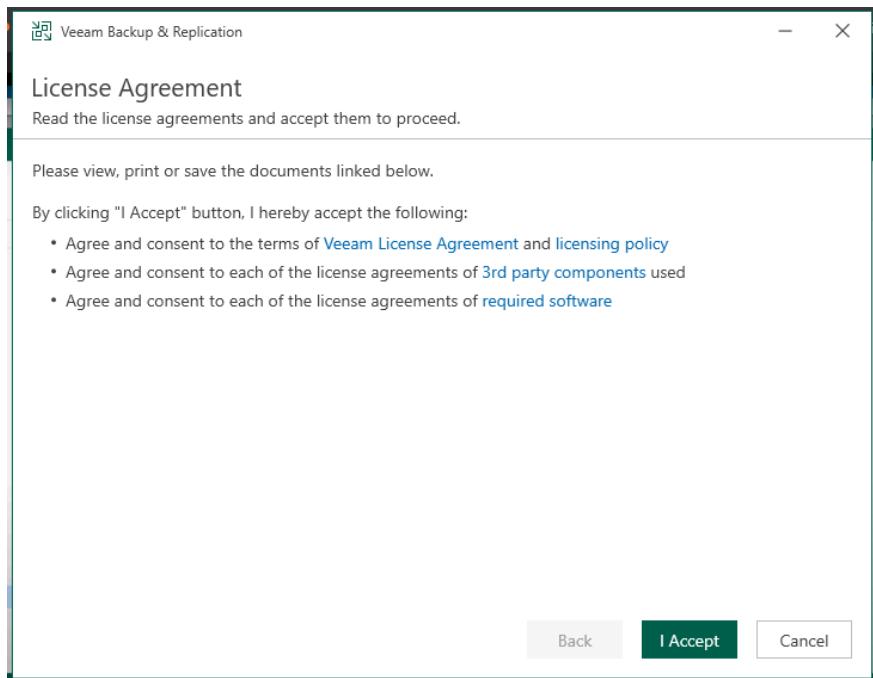
BACKUP CON VEEAM.

Como primer paso debemos registrarnos en la pagina de veeam para poder descargar el ISO y así poder instalarlo, en nuestro caso lo vamos a instalar en un windows 10.

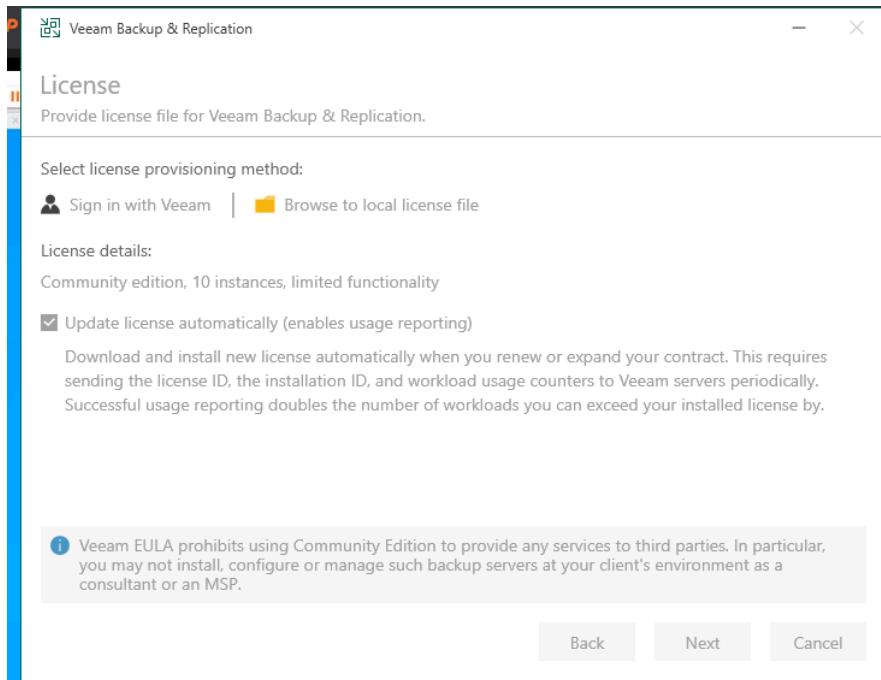
Iniciamos la instalación y seleccionamos backup & replication.



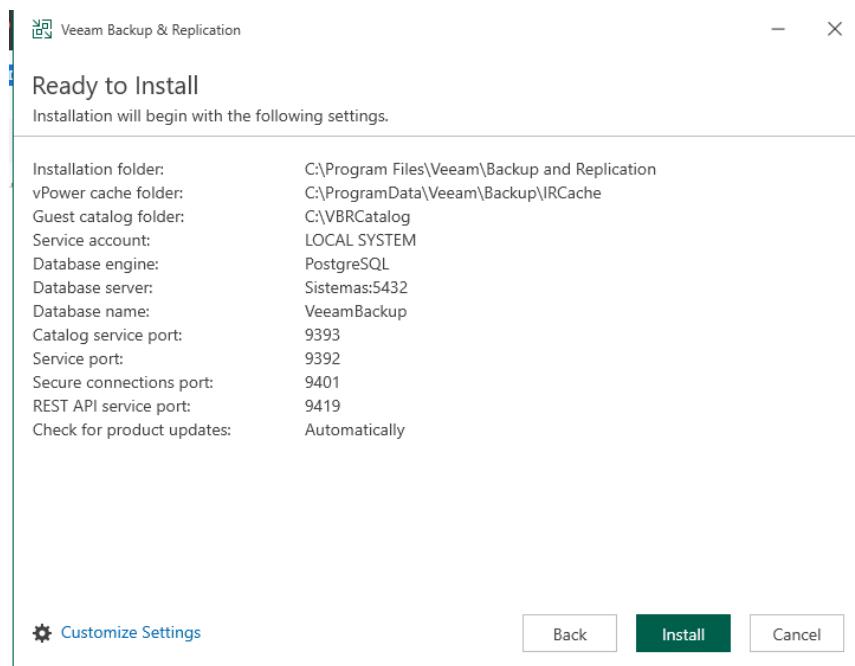
Aceptamos la licencia



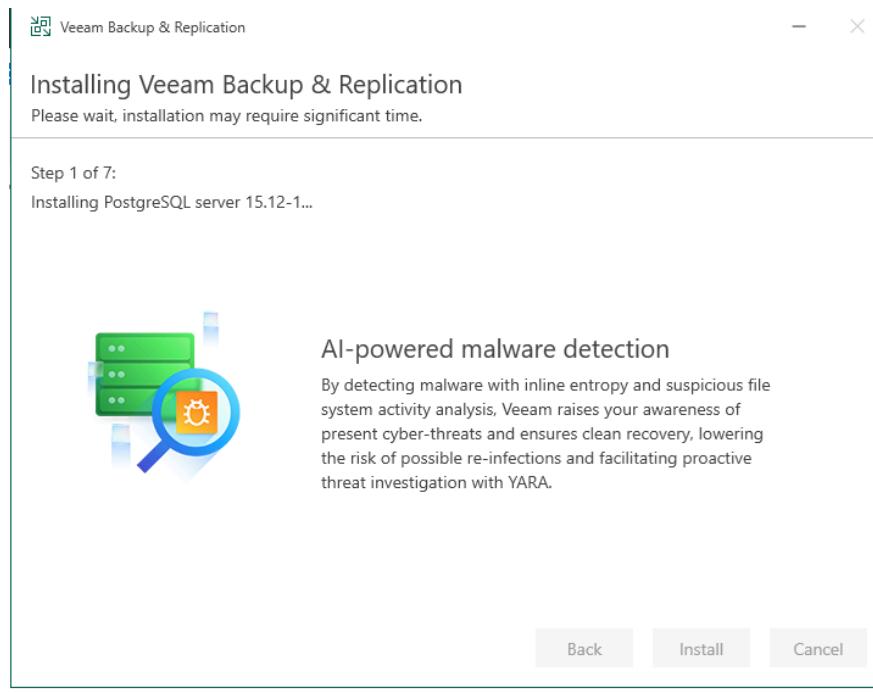
Nos pide licencia pero no agregamos ninguna ya que vamos a instalar el servicio gratuito, damos en next y continuar la instalación.



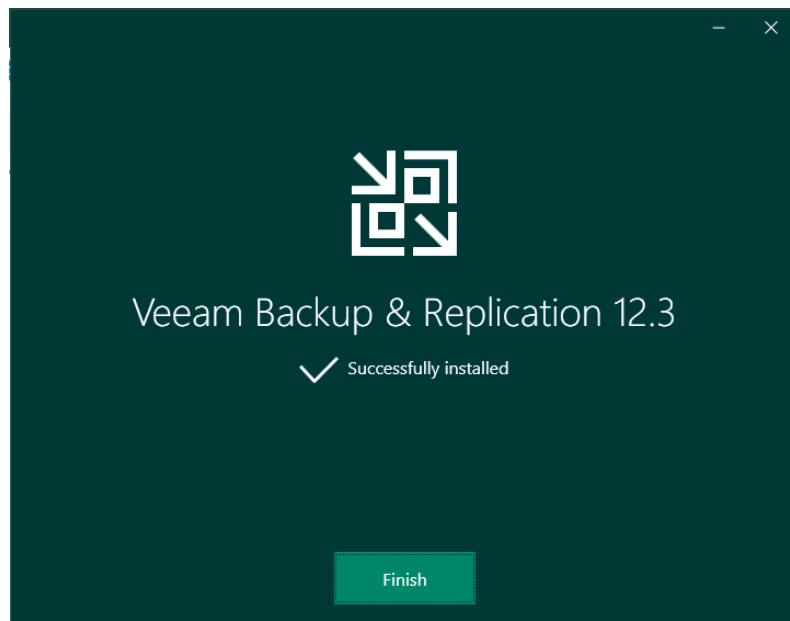
El programa analiza lo que va a instalar y nos muestra un resumen, si estamos seguros procedemos a instalar.



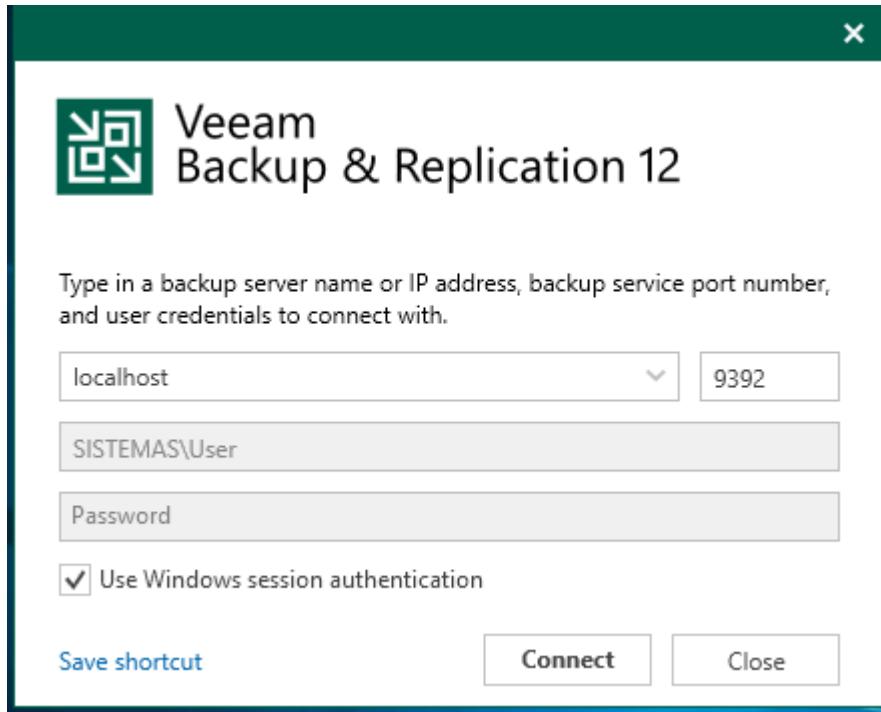
Al darle instalar inicia a mostrar los pasos y aplicaciones las cuales está instalando.



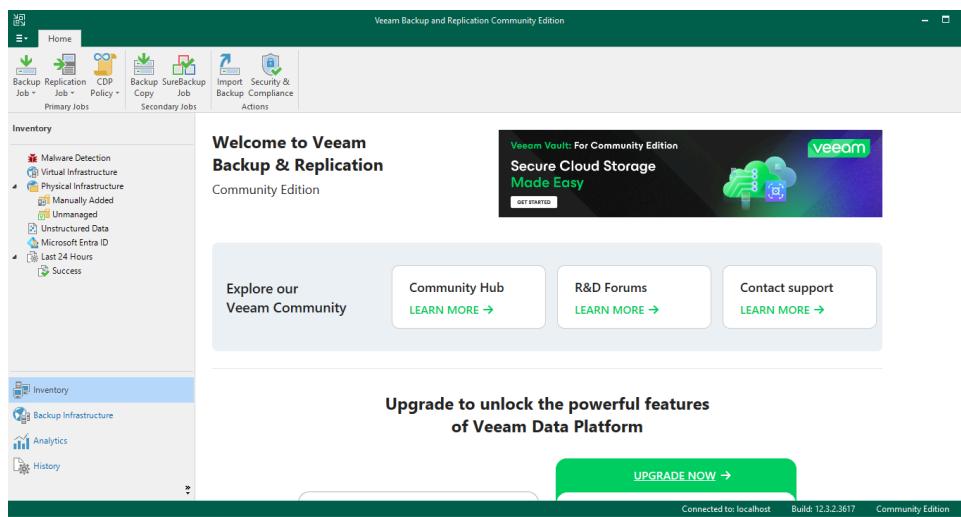
Al completar los 7 pasos nos arroja esta imagen informando que ya está finalizado.



Una vez finalizada la instalación abrimos el aplicativo y nos pedirá confirmar los datos para montar el servicio, los dejamos predeterminados.



Confirmados los datos se abre el panel administrativo donde vamos a configurar todo lo relacionado con nuestros backups.

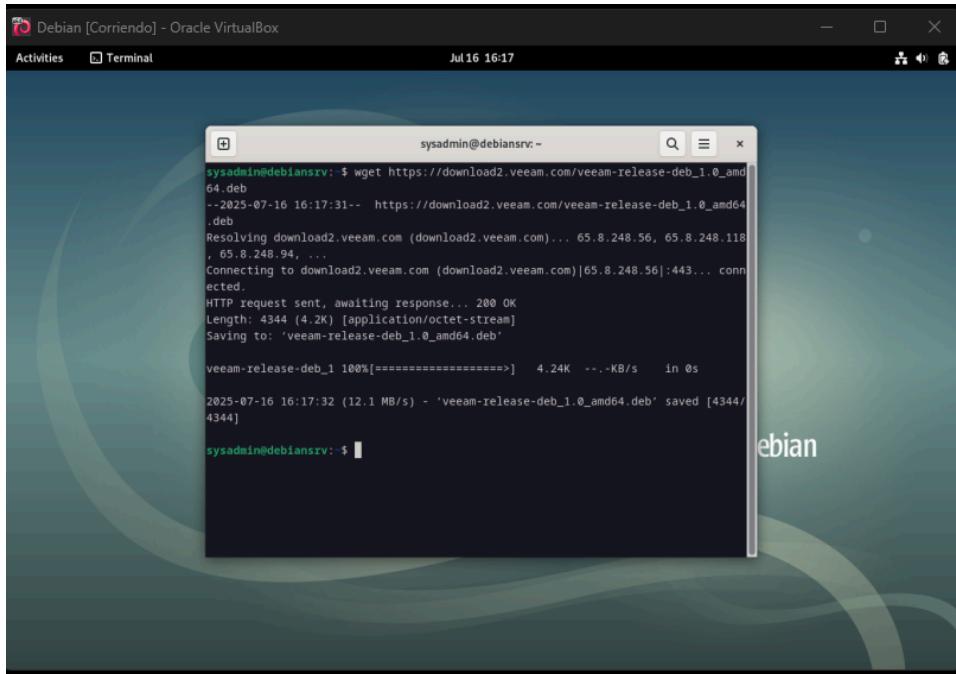


Instalación en Debian, descargamos el archivo desde el repositorio de veeam.

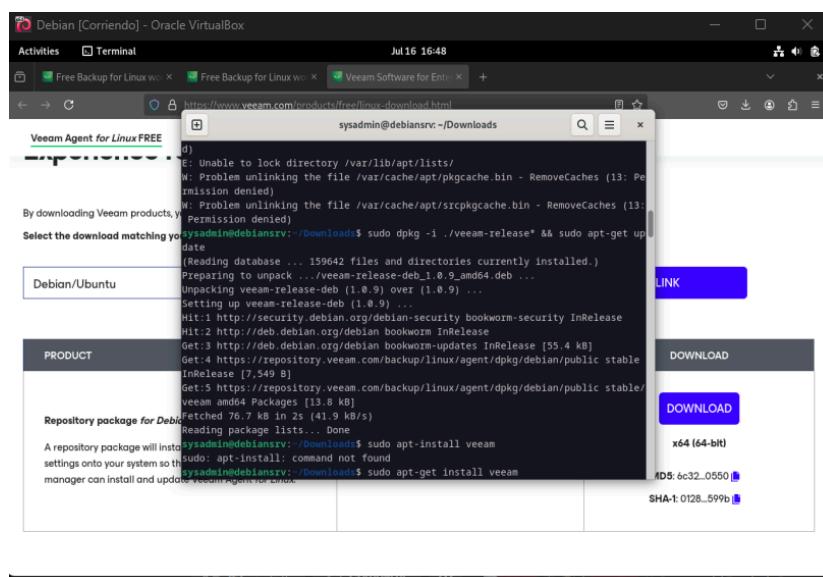
Descargamos el paquete para linux <https://www.veeam.com/products/free/linux.html>

o lo descargamos directo desde la consola:

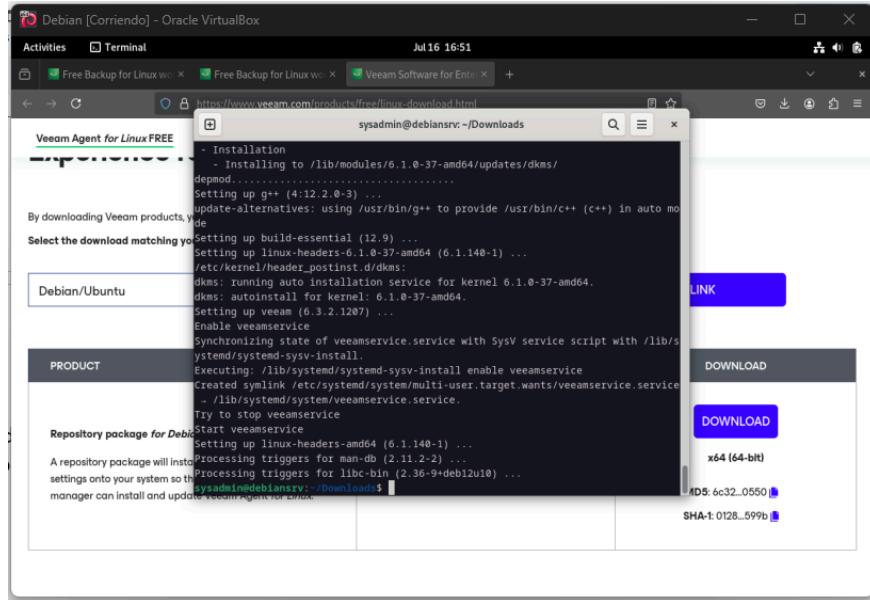
```
wget https://download2.veeam.com/veeam-release-deb_1.0:amd64.deb
```



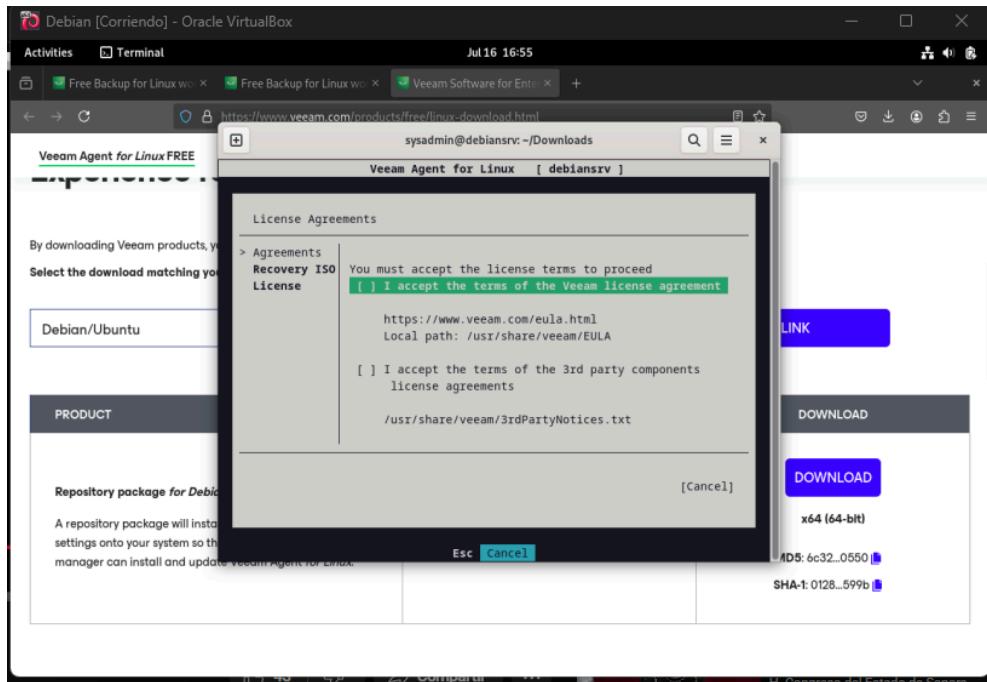
Instalamos el paquete descargado. `dpkg -i ./veeam-release && sudo apt-get update`



ejecutamos sudo apt-get install veeam y realiza toda la descarga de los archivos necesarios, esperamos a que termine.



Una vez finalizada la descarga ejecutamos sudo veeam para abrir el aplicativo.



Aceptamos términos y condiciones y siguiente.

Oprimimos c para configurar el backup.

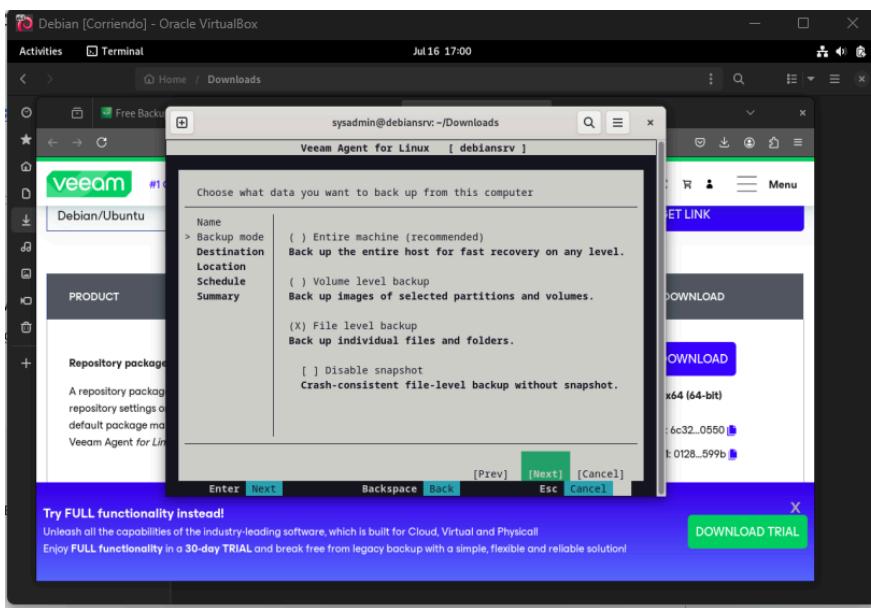
en nombre ponemos uno acorde a backup.

en tipo de backup tenemos:

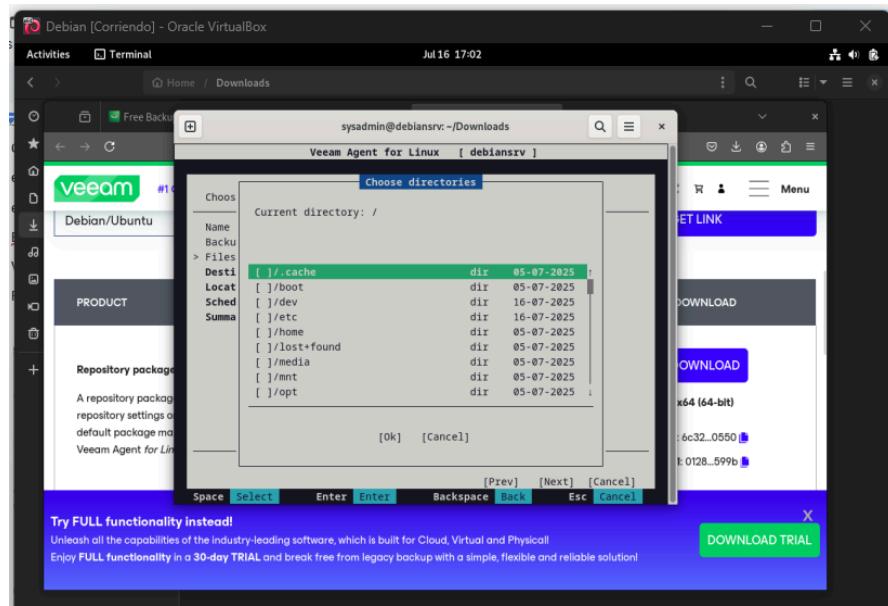
Enteri: Backup forma iso al SO.

Volumen: Se selecciona un volumen del disco.

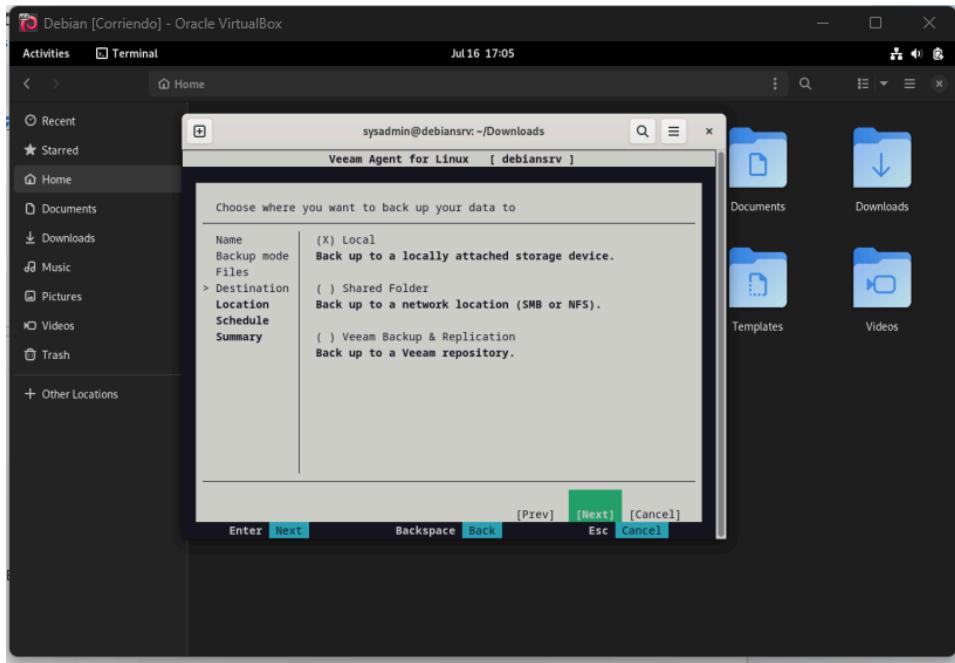
File: Se seleccionan carpetas a las cuales quiere hacer el backup.



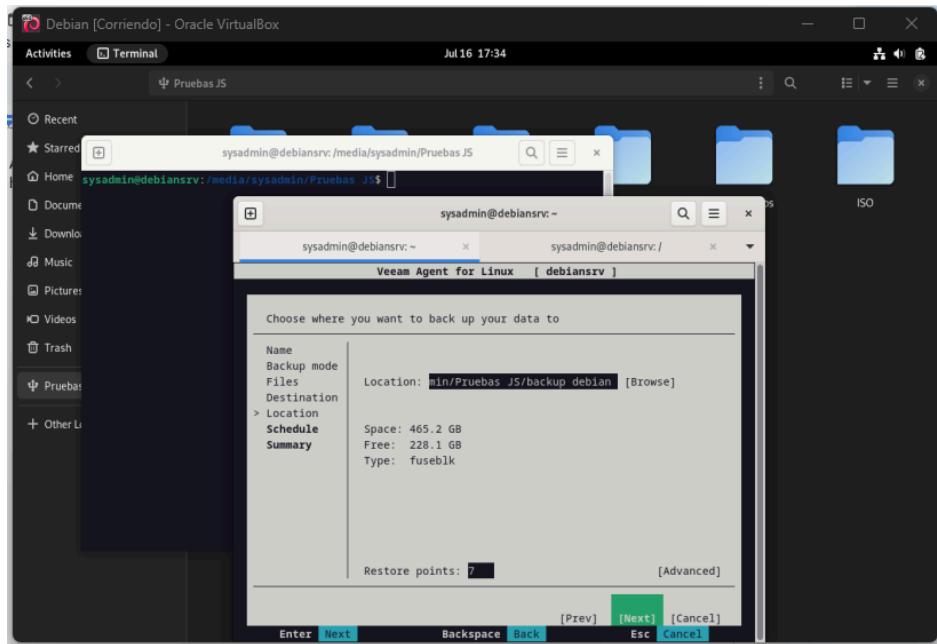
En mi caso seleccione files, y debemos seleccionar que carpetas vamos a respaldar.



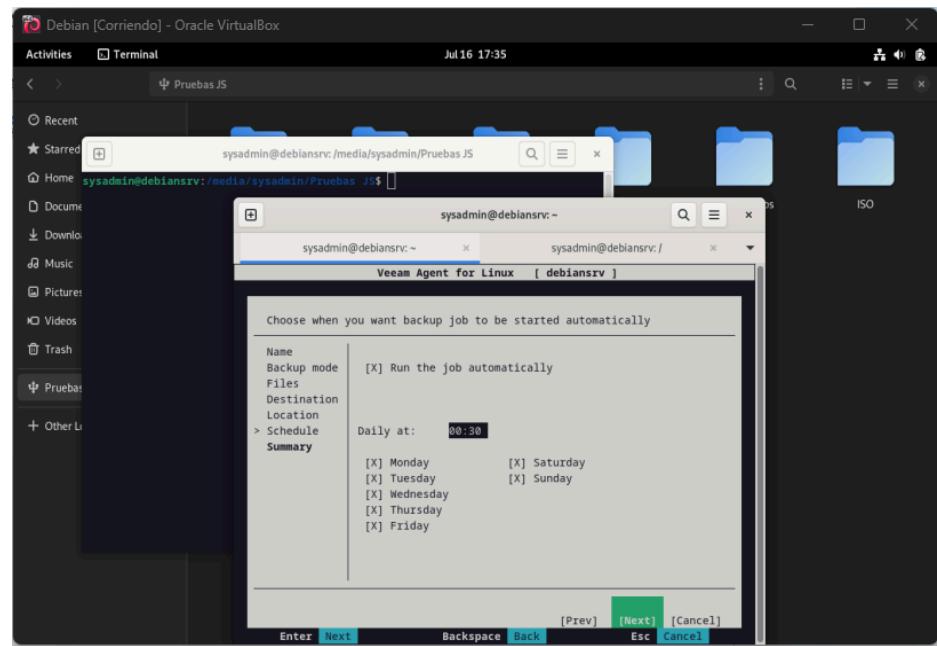
En mi caso selecciono respaldar el Home, y ahora seleccionamos donde guardar la copia.



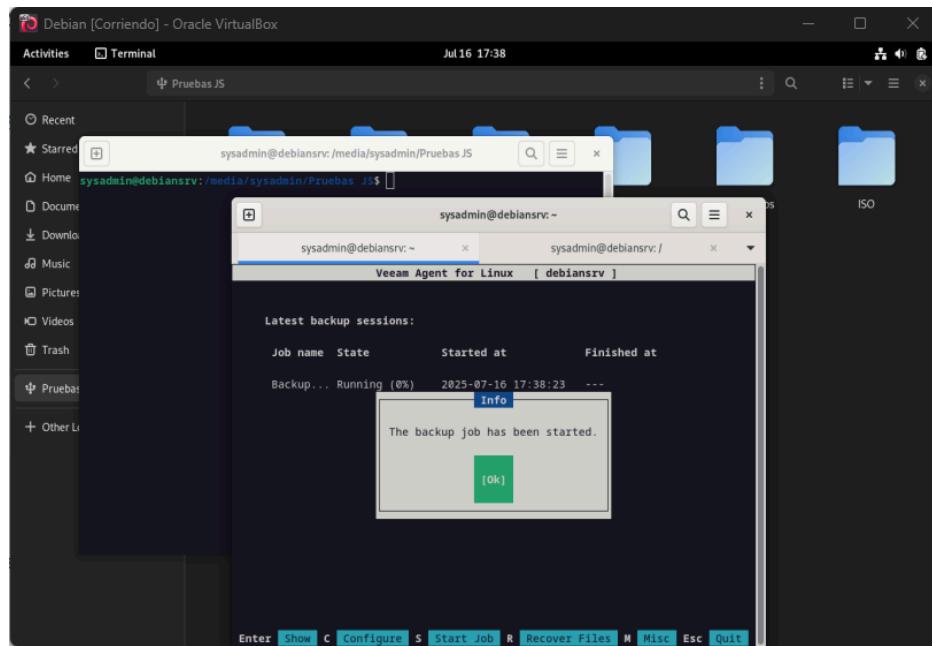
A manera de ejemplo vamos a crear una carpeta en un medio extraíble ya que no permite hacer backup en el mismo medio.



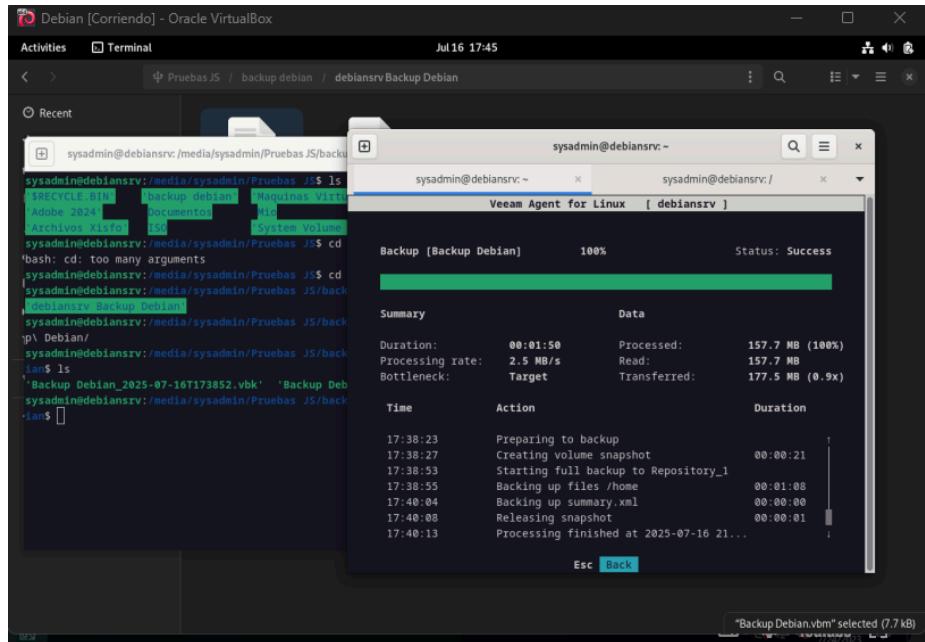
Configuramos los horarios a realizar el backup.



Inicia la primera copia.



Termina el backup y ya podemos verificar los archivos.



Backup Diferencial e Incremental, se basan siempre en una copia de seguridad completa inicial (Full Backup), que sirve como punto de referencia.

1. Backup Incremental:

- **¿Cómo funciona?** Un backup incremental copia *solo los datos que han cambiado desde la última copia de seguridad de cualquier tipo (ya sea completa o incremental anterior)*. Es decir, cada backup incremental se basa en el backup inmediatamente anterior.
 - **Ejemplo:**
 - **Domingo:** Full Backup (copia todos los datos).
 - **Lunes:** Backup Incremental (copia solo lo que cambió desde el Domingo).
 - **Martes:** Backup Incremental (copia solo lo que cambió desde el Lunes).
 - **Miércoles:** Backup Incremental (copia solo lo que cambió desde el Martes).
- **Ventajas:**
 - **Rapidez de la copia:** Son los backups más rápidos de realizar, ya que solo copian una pequeña cantidad de datos nuevos o modificados.

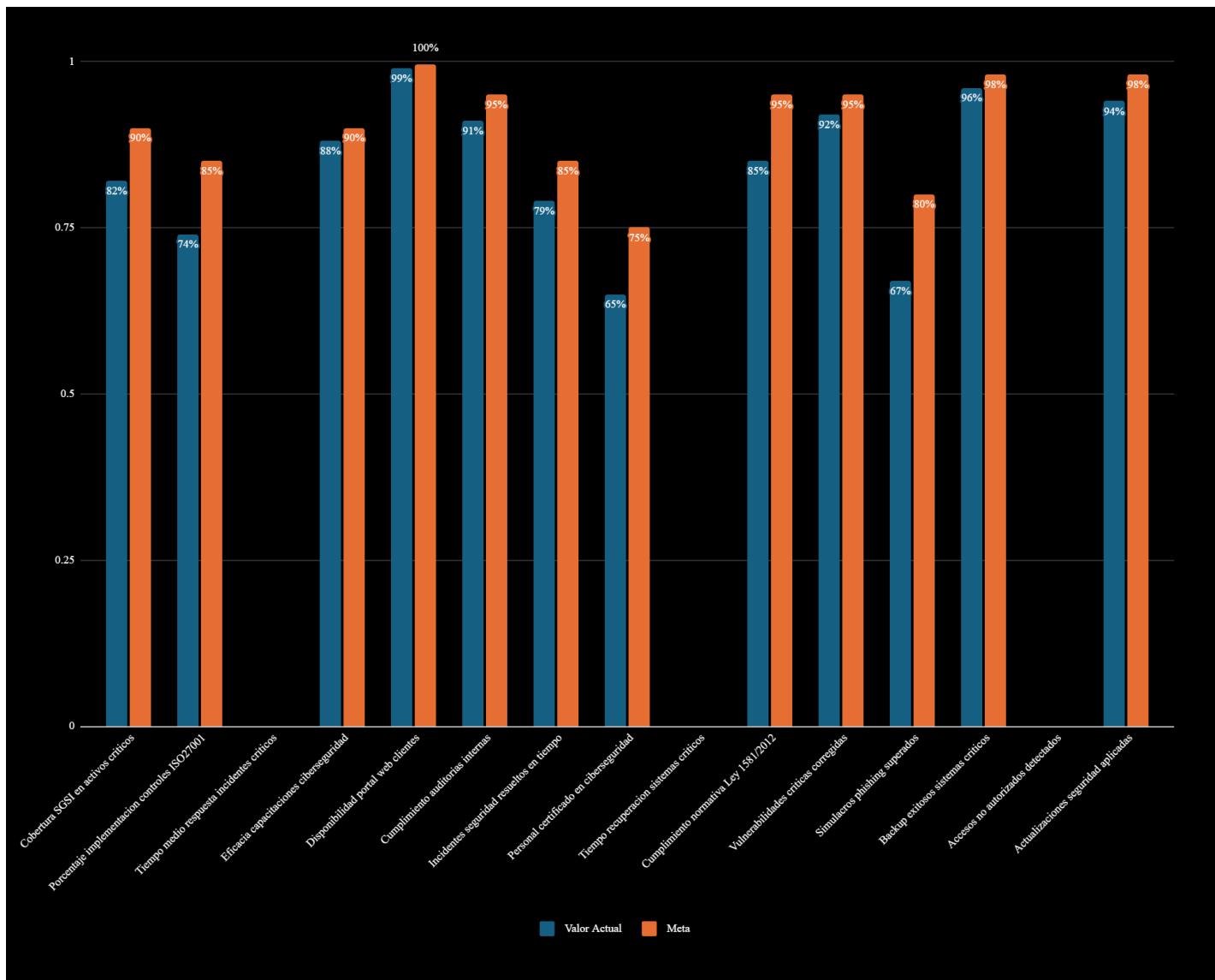
- **Menor espacio de almacenamiento:** Requieren la menor cantidad de espacio de almacenamiento, ya que cada copia es muy pequeña.
- **Mayor frecuencia:** Permiten realizar copias de seguridad con mayor frecuencia debido a su velocidad y bajo consumo de recursos.
- **Desventajas:**
 - **Restauración más compleja y lenta:** Para restaurar los datos a un punto específico, se necesita la copia completa inicial **más todas las copias incrementales sucesivas hasta la fecha deseada**. Si una de estas copias incrementales está dañada o falta, toda la cadena de restauración se rompe, haciendo imposible la recuperación de datos posteriores.
 - **Mayor dependencia:** Existe una alta dependencia entre las copias de seguridad.

2. Backup Diferencial:

- **¿Cómo funciona?** Un backup diferencial copia *todos los datos que han cambiado desde la última copia de seguridad completa*. A diferencia del incremental, no se basa en el backup anterior, sino siempre en el último backup completo.
 - **Ejemplo:**
 - **Domingo:** Full Backup (copia todos los datos).
 - **Lunes:** Backup Diferencial (copia lo que cambió desde el Domingo).
 - **Martes:** Backup Diferencial (copia lo que cambió desde el Domingo, incluyendo los cambios del Lunes y los del Martes).
 - **Miércoles:** Backup Diferencial (copia lo que cambió desde el Domingo, incluyendo los cambios del Lunes, Martes y Miércoles).
- **Ventajas:**
 - **Restauración más sencilla y rápida que el incremental:** Para restaurar los datos, solo se necesita la copia completa inicial **más la última copia diferencial**. Esto reduce la complejidad y el tiempo de restauración en comparación con el incremental.
 - **Menos archivos para la restauración:** Solo dos archivos son necesarios para la recuperación, lo que simplifica la gestión.
 - **Mayor tolerancia a fallos:** La corrupción de una copia diferencial no afecta a otras copias diferenciales anteriores o posteriores, ya que todas se basan en la misma copia completa.
- **Desventajas:**
 - **Mayor espacio de almacenamiento que el incremental:** Con el tiempo, el tamaño de cada backup diferencial puede crecer considerablemente, ya que acumula todos los cambios desde la última copia completa.
 - **Mayor tiempo de copia que el incremental:** A medida que pasa el tiempo desde la última copia completa, los backups diferenciales tardarán más en completarse porque tienen que copiar más datos.

ANEXO 6 Indicadores SGSI Heliópolis:

Cobertura SGSI en activos criticos	82%	90%	En progreso	Oficial SGSI
Porcentaje implementacion controles ISO27001	74%	85%	En progreso	Oficial SGSI
Tiempo medio respuesta incidentes criticos	6 horas	2 horas	No cumple	Jefe Sistemas
Eficacia capacitaciones ciberseguridad	88%	90%	En progreso	Jefe RRHH
Disponibilidad portal web clientes	98.90%	99.50%	En progreso	Admin Web
Cumplimiento auditorias internas	91%	95%	En progreso	Auditor Interno
Incidentes seguridad resueltos en tiempo	79%	85%	En progreso	Jefe Sistemas
Personal certificado en ciberseguridad	65%	75%	No cumple	Jefe RRHH
Tiempo recuperacion sistemas criticos	4.5 horas	2 horas	No cumple	Jefe Sistemas
Cumplimiento normativa Ley 1581/2012	85%	95%	En progreso	Oficial SGSI
Vulnerabilidades criticas corregidas	92%	95%	Cumple	Admin Redes
Simulacros phishing superados	67%	80%	No cumple	Jefe RRHH
Backup exitosos sistemas criticos	96%	98%	Cumple	Admin Backup
Accesos no autorizados detectados	15/mes	5/mes	No cumple	Admin Seguridad
Actualizaciones seguridad aplicadas	94%	98%	Cumple	Admin Sistemas



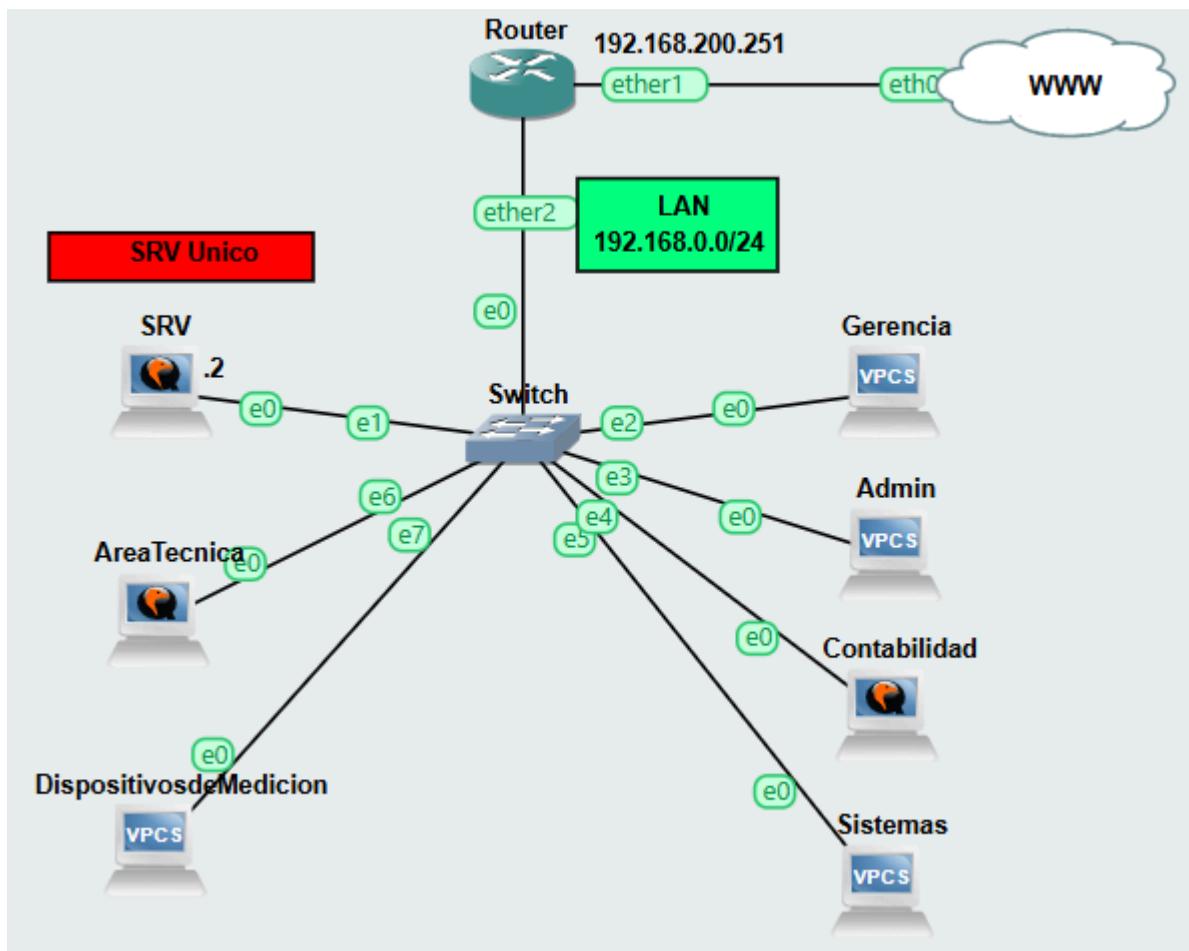
ANEXO 7 Matriz Riesgos Heliópolis:

HEL-R001	Perdida de acceso al portal web por clientes principales	HEL-001	Ataque DDoS	4	5	20	Critico
HEL-R002	Modificacion no autorizada de datos de consumo energetico	HEL-014	Intruso interno	3	5	15	Alto
HEL-R003	Ataque cibernetico a sistemas de monitoreo	HEL-003	Hacker externo	3	4	12	Alto
HEL-R004	Fuga de credenciales de acceso de clientes	HEL-015	Ingenieria social	4	4	16	Alto
HEL-R005	Interrupcion del suministro por sobrecarga del sistema	HEL-003	Fallo tecnico	2	5	10	Medio
HEL-R006	Acceso no autorizado a base de datos de clientes	HEL-002	Hacker externo	3	5	15	Alto
HEL-R007	Fallo del sistema de backup durante crisis	HEL-008	Fallo hardware	2	4	8	Medio
HEL-R008	Manipulacion de informacion en monitores	HEL-003	Intruso interno	3	4	12	Alto
HEL-R009	Perdida de conectividad con granjas solares	HEL-013	Fallo comunicacion	3	4	12	Alto
HEL-R010	Violacion de datos personales de clientes	HEL-002	Error humano	2	5	10	Medio
HEL-R011	Ataque de ransomware a servidores criticos	HEL-004	Malware	3	4	12	Alto
HEL-R012	Error humano en configuracion de sistemas	HEL-006	Error humano	4	3	12	Alto
HEL-R013	Fallo de firewall perimetral	HEL-009	Fallo tecnico	2	4	8	Medio
HEL-R014	Interceptacion de comunicaciones cliente-servidor	HEL-001	Interceptacion	2	3	6	Bajo
HEL-R015	Caida del servidor de aplicaciones principal	HEL-006	Fallo hardware	3	4	12	Alto

		RIESGO INHERENTE					
		MINIMA	MENOR	MODERADA	MAYOR	SUPERIOR	MAXIMA
PROBABILIDAD		1	2	4	8	16	24
CRITICO	5						
ALTO	4						
MEDIO	3						
BAJO	2						
MUY BAJO	1						

ANEXO 8 Análisis de vulnerabilidades y mitigación:

Para iniciar con el análisis de la empresa y revisando su topología actual nos damos cuenta que tiene muchos factores a mejorar ya que manejan una sola red y tienen todo en un solo servidor, se realizan las pruebas iniciales dentro de la LAN y observamos los siguientes resultados.



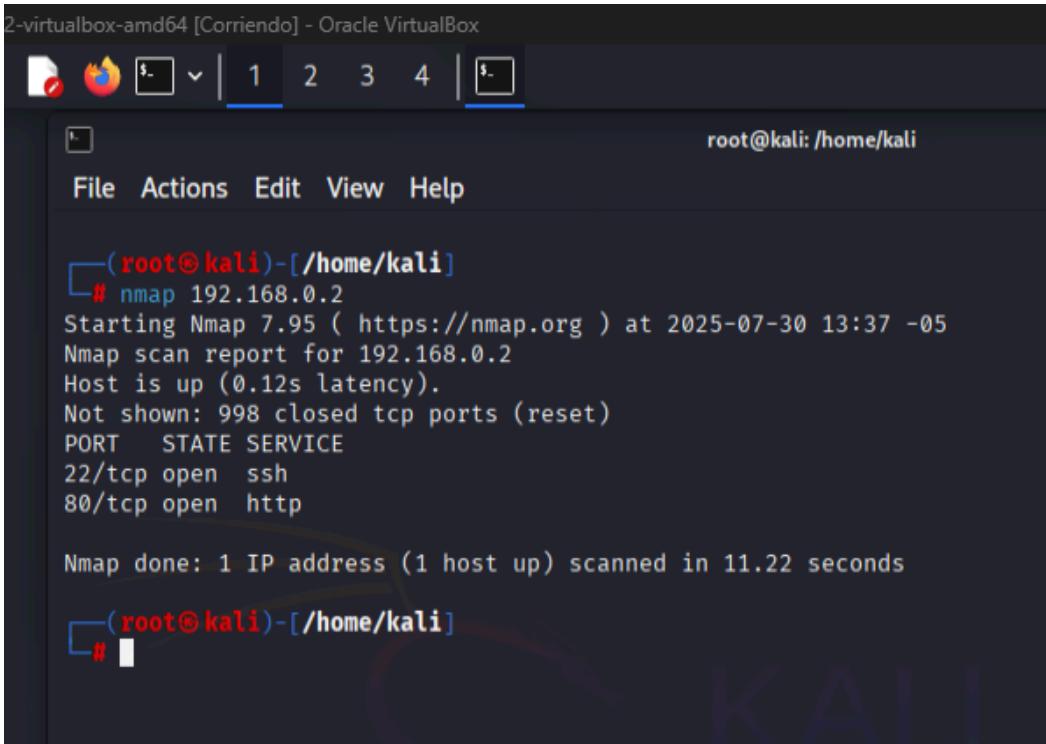
Escaneo con NMAP a Red Vulnerable:

Comando nmap 192.168.0.0/24 para escanear toda la red.

```
(root㉿kali)-[~/home/kali]
# nmap 192.168.0.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 13:44 -05
Nmap scan report for 192.168.0.1
Host is up (0.0064s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
2000/tcp  open  cisco-sccp
8291/tcp  open  unknown

Nmap scan report for 192.168.0.2
Host is up (0.010s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

comando nmap 192.168.0.2 srv



2-virtualbox-amd64 [Corriendo] - Oracle VirtualBox

File Actions Edit View Help

```
(root㉿kali)-[~/home/kali]
# nmap 192.168.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 13:37 -05
Nmap scan report for 192.168.0.2
Host is up (0.12s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 11.22 seconds
```

Sondeo de ping

nmap -sP 192.168.0.0/24

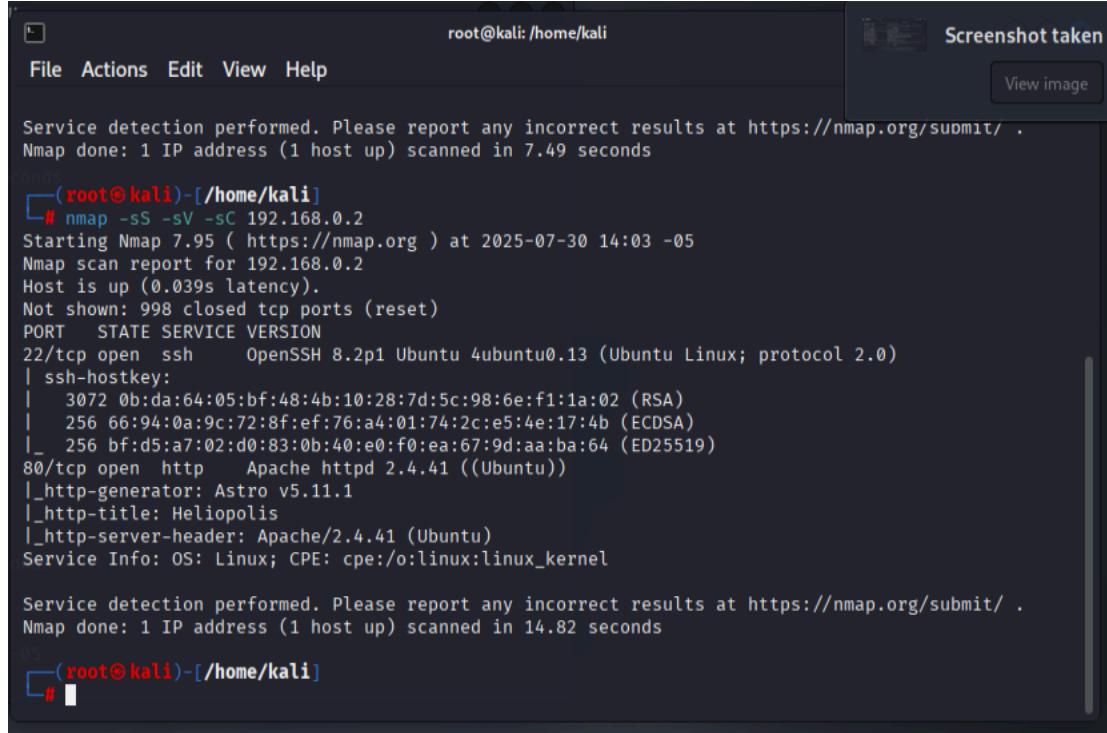
```
(root㉿kali)-[~/home/kali]
# nmap -sP 192.168.0.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 13:49 -05
Nmap scan report for 192.168.0.1
Host is up (0.0033s latency).
Nmap scan report for 192.168.0.2
Host is up (0.0065s latency).
Nmap scan report for 192.168.0.251
Host is up (0.0045s latency).
Nmap scan report for 192.168.0.252
Host is up (0.0045s latency).
Nmap scan report for 192.168.0.253
Host is up (0.0045s latency).
Nmap scan report for 192.168.0.254
Host is up (0.0043s latency).
Nmap done: 256 IP addresses (6 hosts up) scanned in 4.00 seconds
```

Se le realiza al servidor la verificación de servicio por puerto.

nmap -sV -sC 192.168.0.2

```
File Actions Edit View Help
root@kali:~/home/kali
(kali㉿kali)-[~] unknown
$ sudo su
[sudo] password for kali:
(root㉿kali)-[~/home/kali]
# nmap -sV -sC 192.168.0.2 6 hosts up) scanned in 10.21 seconds
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 13:59 -05
Nmap scan report for 192.168.0.2
Host is up (0.0068s latency).
Not shown: 998 closed tcp ports (reset) at 2025-07-30 13:49 -05
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   35  OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 1024 3072 0b:da:64:05:bf:48:4b:10:28:7d:5c:98:6e:f1:1a:02 (RSA)
|_ 256 66:94:0a:9c:72:8f:ef:76:a4:01:74:2c:e5:4e:17:4b (ECDSA)
|_ 256 bf:d5:a7:02:d0:83:0b:40:e0:f0:ea:67:9d:aa:ba:64 (ED25519)
80/tcp    open  http  Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Heliopolis
|_http-generator: Astro v5.11.1.53
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Host is up (0.0043s latency).
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.49 seconds
(root㉿kali)-[~/home/kali]
#
```

Para realizar el escaneo de manera Sigilosa usamos el mismo comando y agregamos -sS
 nmap -sS -sV -sC 192.168.0.0/24



```

root@kali: /home/kali
File Actions Edit View Help
Screenshot taken
View image

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.49 seconds

[root@kali ~]# nmap -sS -sV -sC 192.168.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 14:03 -05
Nmap scan report for 192.168.0.2
Host is up (0.039s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 0b:da:64:05:bf:48:4b:10:28:7d:5c:98:6e:f1:1a:02 (RSA)
|   256 66:94:0a:9c:72:8f:ef:76:a4:01:74:2c:e5:4e:17:4b (ECDSA)
|_  256 bf:d5:a7:02:d0:83:0b:40:e0:f0:ea:67:9d:aa:ba:64 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: Astro v5.11.1
|_http-title: Heliopolis
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.82 seconds

[root@kali ~]#

```

Para poder cambiar la mac virtualmente ingresamos spoof

nmap --spoof-mac 00:11:22:33:44 -sS -sV -sC 192.168.0.2



```

root@kali: /home/kali
File Actions Edit View Help
2 packets transmitted, 2 received, 0% packet loss, time 1019ms
rtt min/avg/max/mdev = 4.559/5.896/7.234/1.337 ms

[root@kali ~]# nmap --spoof-mac 00:11:22:33:44 -sS -sV -sC 192.168.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 09:29 -05
Spoofing MAC address 00:11:22:33:44:DB (Cimsys)
Nmap scan report for 192.168.0.2
Host is up (0.0061s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 0b:da:64:05:bf:48:4b:10:28:7d:5c:98:6e:f1:1a:02 (RSA)
|   256 66:94:0a:9c:72:8f:ef:76:a4:01:74:2c:e5:4e:17:4b (ECDSA)
|_  256 bf:d5:a7:02:d0:83:0b:40:e0:f0:ea:67:9d:aa:ba:64 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Heliopolis
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-generator: Astro v5.11.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.47 seconds

[root@kali ~]#

```

Conclusiones del escaneo nmap:

Vemos que todos los servicios están arriba en una sola máquina, esto es muy peligroso ya que un hacker con tan solo apoderarse de la máquina puede acceder a toda la información de los demás servicios.

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
80/tcp	open	http
2000/tcp	open	cisco-sccp
8291/tcp	open	unknown

Procedemos a hacer un análisis de Nessus a la red vulnerable:

Sev	CVSS	VPR	EPSS	Name	Family	Count	
LOW	2.1 *	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1	
INFO	HTTP (Multiple Issues)	Web Servers	3	
INFO	SSH (Multiple Issues)	General	2	
INFO	SSH (Multiple Issues)	Misc.	2	
INFO	SSH (Multiple Issues)	Service detection	2	
INFO				Nessus SYN scanner	Port scanners	2	
INFO				Service Detection	Service detection	2	
INFO				Apache HTTP Server Version	Web Servers	1	
INFO				Backported Security Patch Detection (WWW)	General	1	
INFO				Common Platform Enumeration (CPE)	General	1	
INFO				Device Type	General	1	
INFO				Nessus Scan Information	Settings	1	
INFO				OpenSSH Detection	Misc.	1	
INFO				OS Fingerprints Detected	General	1	

SRV Heliopolis Vulnerable / Plugin #10114

[← Back to Vulnerabilities](#)

Hosts 1 Vulnerabilities 19 History 1

LOW ICMP Timestamp Request Remote Date Disclosure

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Output

```
The difference between the local and remote clocks is -1 seconds.

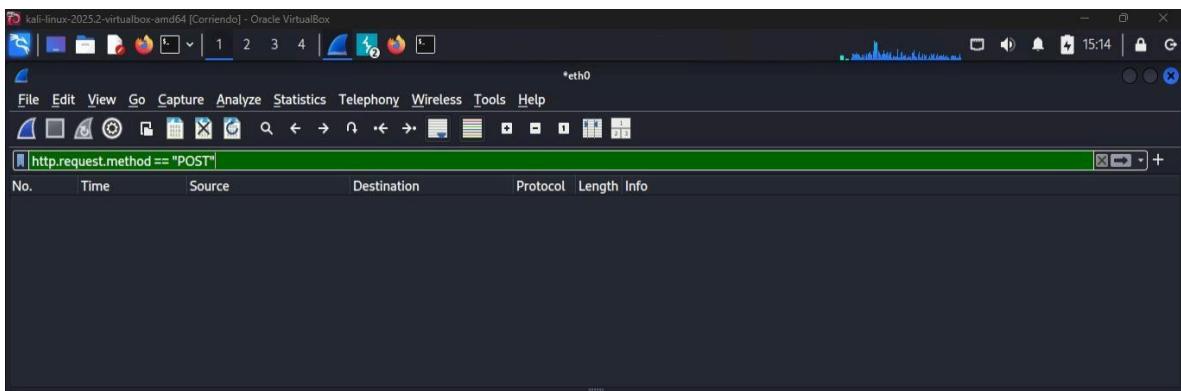
To see debug logs, please visit individual host
```

Port	Hosts
------	-------

En cuanto a la red se encontraron vulnerabilidades pequeñas pero que dan mucha información a un posible atacante, ya que entrega muchos datos de valor, como versiones, servicios que hay activos, también que los puertos en los que están los servicios son los comunes. Estos errores a

pesar de ser pequeños lo recomendable es corregirlos.

Wireshark:



En cuanto al Wireshark se analizó que había una vulnerabilidad crítica en el aplicativo, cuando el servidor hacia una petición post, concretamente en la parte de conexión del login con el backend, lo que pasaba era que con el wireshark al servidor no estar protegido con certificaciones HTTP de cifrado (**HTTPS**) y tampoco tener implementaciones de hash en las credenciales, el atacante podría obtener los datos de ingreso de la plataforma ya que los paquetes que viajan por la red no están cifrados. Este tipo de vulnerabilidad permite ataques del tipo **Man-in-the-Middle (MITM)**.

Ya verificando la red y yéndonos un poco más a fondo de los procedimientos que tienen dentro de la empresa podemos observar que no tienen un servidor de archivos unificado y que todos los equipos tienen sus archivos de forma local sin realizar backup de ellos.

También podemos observar que no tienen un servidor de dominio para darles permisos a los equipos y manejar políticas de dominio tanto a usuarios como a equipos.

Recomendaciones realizadas y procedimientos de mejora:

Como recomendación principal iniciamos con la segmentación de la red para que los diferentes procesos no tengan comunicación entre sí y así blindamos un poco a nivel de red. En cuanto al desarrollo de la página web, encontramos muchos huecos de seguridad los cuales se explicaran a continuación:

¿Por qué la implementación actual es insegura?

1. Contraseñas en texto plano

- Si un atacante accede a la base de datos (por ejemplo con **SQL injection** o credenciales robadas), obtendrá las contraseñas tal como el usuario las escribió.
- Además, muchas personas usan las mismas contraseñas en múltiples sitios.

Solución: Hash con **bcrypt + salting automático**. Esto evita ataques como: Esta solución será aplicada concretamente en el backend, en el archivo server.js.

- Ataques de diccionario
- Fuerza bruta
- Rainbow tables (precomputados)

2. Sin HTTPS (solo HTTP)

- Toda la información viaja en **texto plano** (correo, contraseña, token).
- Un atacante en la misma red (Wi-Fi pública, LAN interna) podría hacer un ataque de **MITM** (**Man In The Middle**) y leer los datos.

Solución: Certificado SSL (Let's Encrypt o Nginx Reverse Proxy con HTTPS).

3. No hay tokens o sesiones

- No puedes controlar qué usuarios están logueados.

- No puedes invalidar un login anterior.
- Un atacante puede hacer **replays** o **secuestro de sesión** fácilmente.

Solución: JWT (con expiración + verificación + firma secreta).

4. las rutas sensibles no están protegidas

- Cualquiera puede acceder a /Plataforma_gestion o cualquier otra ruta sin estar logueado.

Solución: Middleware que valide el token antes de acceder.

Después de este listado, procederemos a corregir aspectos de la página web para volverla segura:

CORRECCIONES:

1) Firmar tokens:

Poblemas sin JWT_SECRET (inseguro):

- El backend antes generaba tokens JWT sin firmarlos (o con una clave visible en el código), cualquier atacante podría:
 - Analizar un token válido desde el navegador (porque los JWT son fácilmente legibles, aunque estén codificados).
 - Modificar el contenido del token (por ejemplo, cambiar "rol": "usuario" a "rol": "admin").
 - Volver a enviarlo al servidor, que aceptaría el token sin saber que fue alterado.

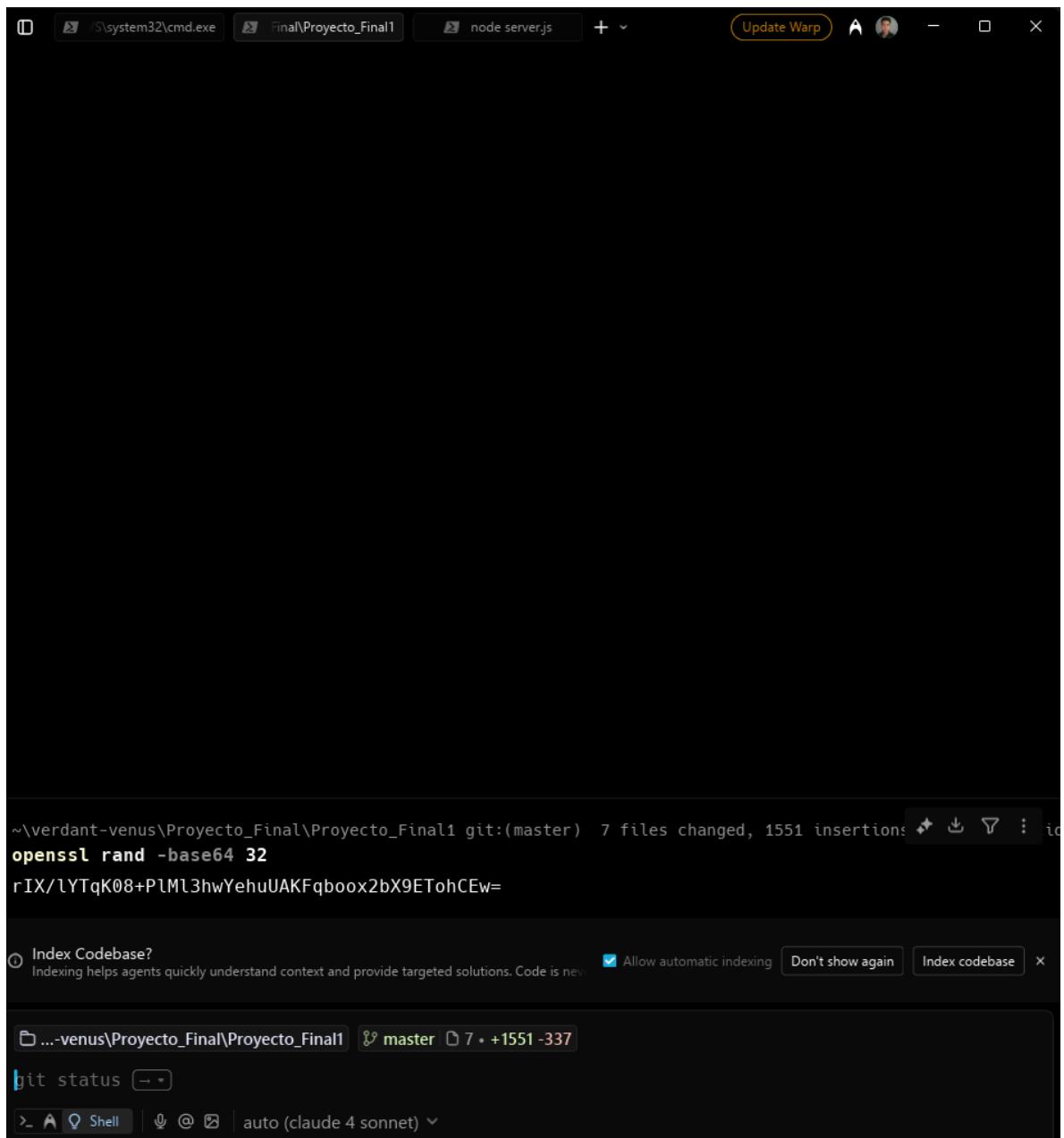
Resultado: El atacante podría acceder a datos privados, robar cuentas, incluso escalar privilegios.

Para corregir este problema se hizo lo siguiente:

1. Uso de dotenv (.env) para ocultar secretos:

Se movió la clave secreta JWT fuera del código y se almacenó en un archivo .env.

En ese archivo .env el cual está en la raíz, se creó una variable llamada **JWT_SECRET** y se genera una clave utilizando el siguiente comando en bash: **openssl rand -base64 32**. De esta forma se asegura de generar una firma segura para los tokens.

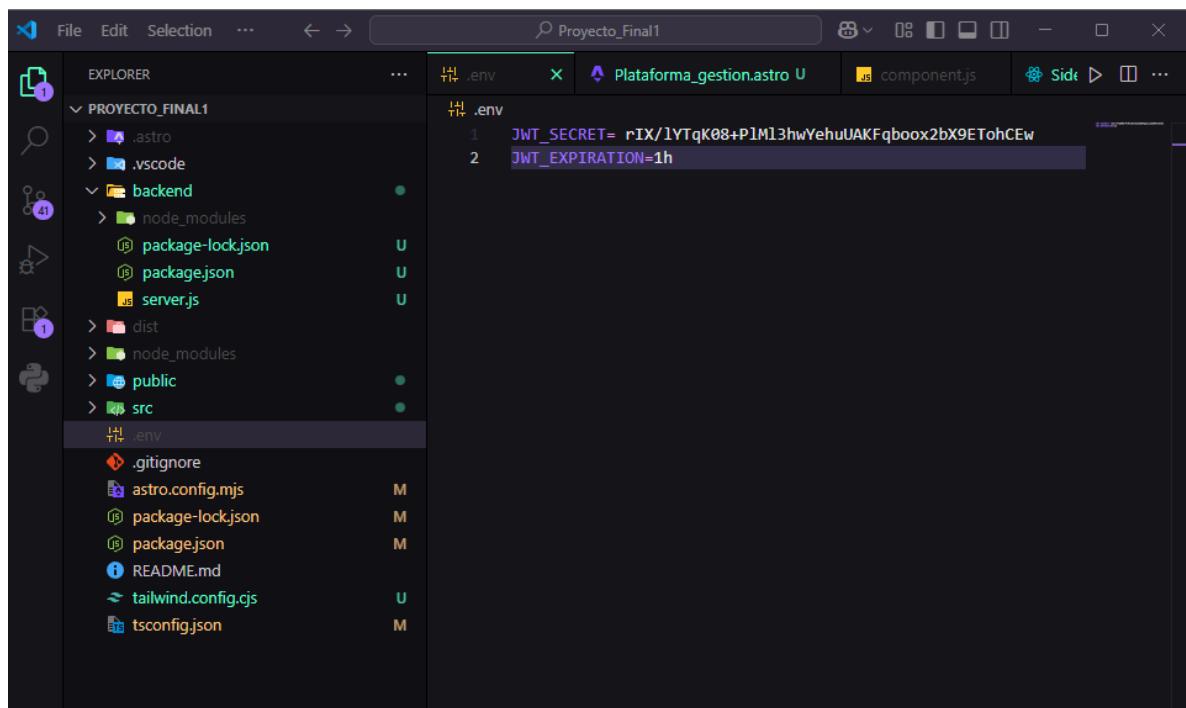


The screenshot shows a terminal window with several tabs at the top: 'system32\cmd.exe', 'Final\Proyecto_Final1', and 'node server.js'. The main area of the terminal displays the following command and its output:

```
~\verdant-venus\Proyecto_Final\Proyecto_Final1 git:(master) 7 files changed, 1551 insertions, 337 deletions (-)
openssl rand -base64 32
rIX/lYTqK08+PlMl3hwYehuUAKFqboox2bX9ETohCEw=
```

Below the terminal, a GitHub interface is visible, showing a tooltip for 'Index Codebase?' with the message: 'Indexing helps agents quickly understand context and provide targeted solutions. Code is new.' There are checkboxes for 'Allow automatic indexing' and 'Don't show again', and a button for 'Index codebase'.

También crearemos una variable que será el tiempo en que se expira:



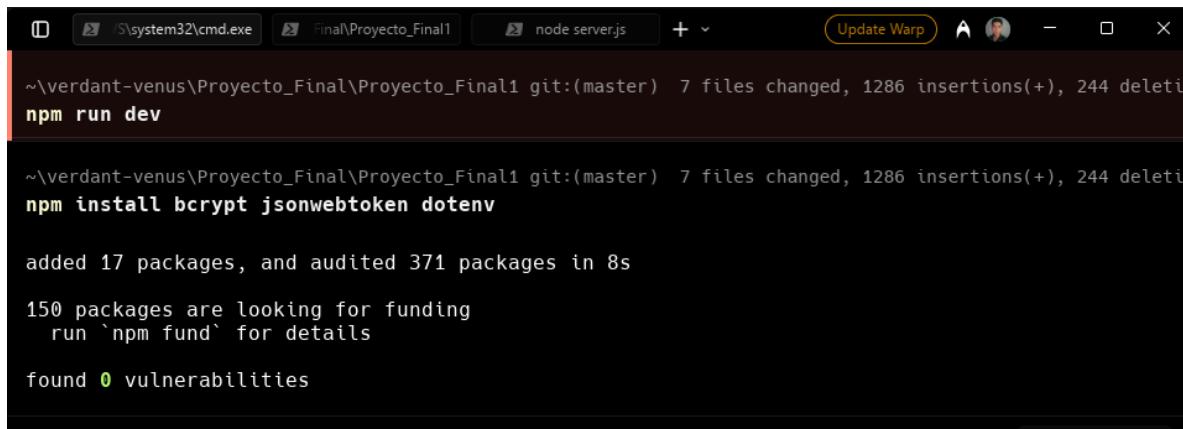
The screenshot shows the VS Code interface with the project structure on the left and the code editor on the right. The code editor displays the `.env` file with the following content:

```
JWT_SECRET= rIX/lYTqK08+P1M13hwYehuUAKFqboox2bX9ETohCEw
JWT_EXPIRATION=1h
```

2. Hash + salt + instalación de certificados SSL/TLS:

Para esta parte se harán varios pasos, es importante ya que una de las vulnerabilidades de la implementación actual es la forma en que se envían los datos para la verificación. Estos en el servidor vulnerable no tienen aplicados ningún tipo de hash y por lo tanto un atacante que esté en la red puede leer de manera fácil la información (texto plano) del paquete post que se envía a la hora del logueo. La primera medida que se hará es la implementación de la librería bcrypt en nuestro backend. De esta manera se puede encriptar de una manera segura y eficiente los datos de acceso.

El primer paso será instalar el bcrypt en nuestro proyecto, nos vamos a una terminal bash y colocamos el siguiente comando: **npm install bcrypt jsonwebtoken dotenv**



```
~\verdant-venus\Proyecto_Final\Proyecto_Final1 git:(master) 7 files changed, 1286 insertions(+), 244 deletions(-)
npm run dev

~\verdant-venus\Proyecto_Final\Proyecto_Final1 git:(master) 7 files changed, 1286 insertions(+), 244 deletions(-)
npm install bcrypt jsonwebtoken dotenv

added 17 packages, and audited 371 packages in 8s

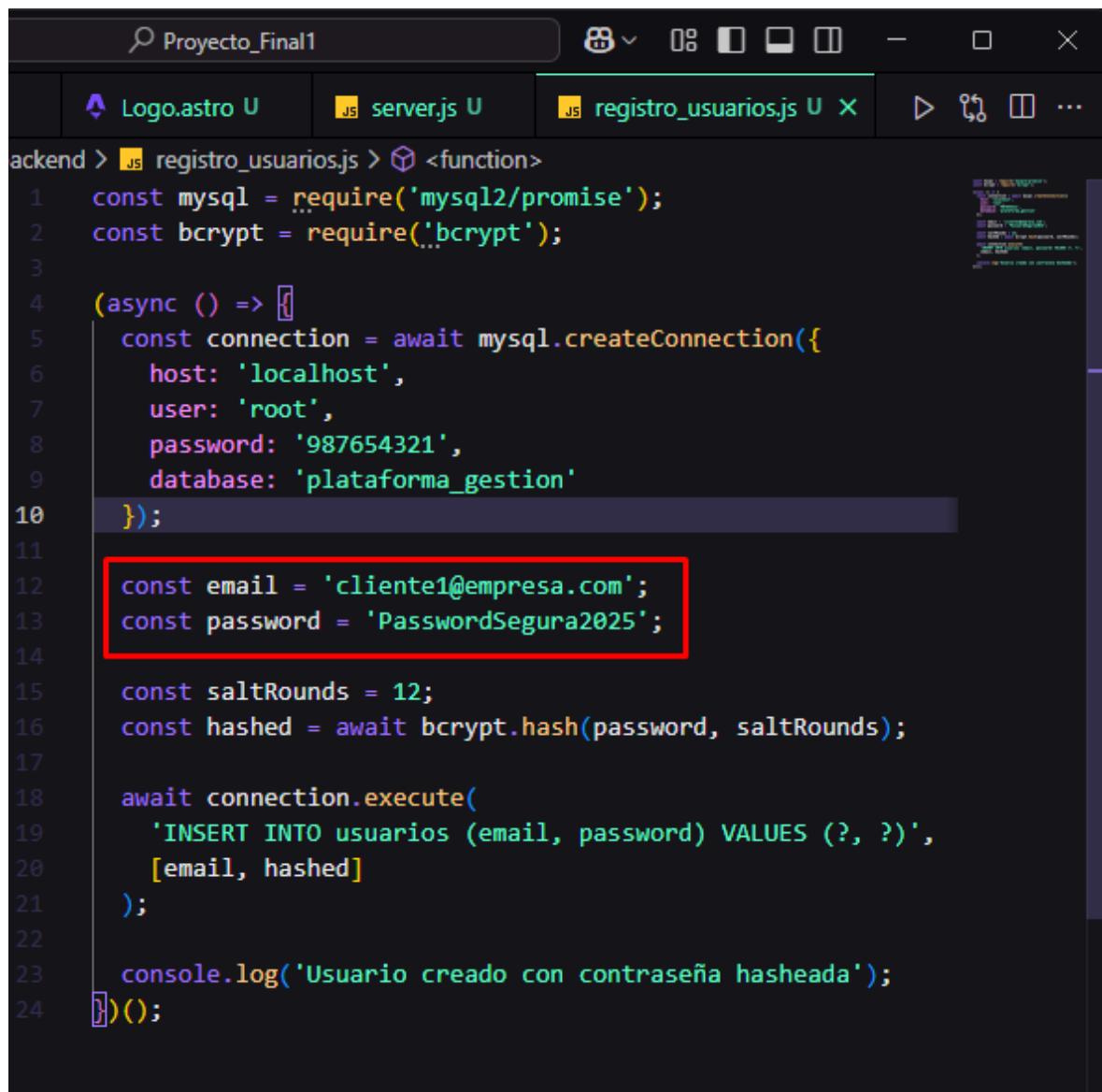
150 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities
```

Con esta instalación lo que se procede a hacer será modificar la estructura del manejo de registro de la empresa. Anteriormente la empresa al rentar la plataforma de gestión energética lo que hacía era crear la base de datos directamente en mysql, en dicha base de datos creaban los usuarios en texto plano, sin ninguna medida de protección a los datos.

El cambio que se hizo fue desarrollar un nueva forma de registro que implementa directamente una forma de encriptación a las contraseñas de los usuarios. Por lo tanto cuando una empresa contrate los servicios, el encargado de registrar a los usuarios lo hará de manera interna a través de

un script:



```

Proyecto_Final1
Logo.astro U server.js U registro_usuarios.js U X ...
backend > JS registro_usuarios.js > <function>
1 const mysql = require('mysql2/promise');
2 const bcrypt = require('bcrypt');
3
4 (async () => {
5   const connection = await mysql.createConnection({
6     host: 'localhost',
7     user: 'root',
8     password: '987654321',
9     database: 'plataforma_gestion'
10 });
11
12   const email = 'cliente1@empresa.com';
13   const password = 'PasswordSegura2025';
14
15   const saltRounds = 12;
16   const hashed = await bcrypt.hash(password, saltRounds);
17
18   await connection.execute(
19     'INSERT INTO usuarios (email, password) VALUES (?, ?)',
20     [email, hashed]
21   );
22
23   console.log('Usuario creado con contraseña hasheada');
24 })();

```

En la parte señalada en rojo el encargado del registro colocará las credenciales de los nuevos usuarios, esto lo que hará será agregarlos directamente a la base de datos, pero con una diferencia, con este nuevo método las contraseñas quedarán con un hash aplicado en la base de datos de MySQL.

```

mysql> SELECT * FROM usuarios;
+----+-----+-----+
| id | email           | password          |
+----+-----+-----+
| 1  | prueba@correo.com | 123456            |
| 2  | cliente1@empresa.com | $2b$12$d7Hc/6nSbn/0ncLFemFCzuVrtL1eOJmNGc7AXiQffpuDhYjiU2Xl2 |
+----+-----+-----+
2 rows in set (0.009 sec)

```

En la anterior imagen se puede observar un usuario registrado de manera directa a través de mysql y el otro registrado a través del script para registrar usuarios.

```
app.post('/login', (req, res) => {
  const { email, password } = req.body;
  db.query('SELECT * FROM usuarios WHERE email = ?', [email], async (err, results) => {
    if (err || results.length === 0) return res.status(401).json({ message: 'Credenciales inválidas' });
    const user = results[0];
    const match = await bcrypt.compare(password, user.password);
    if (!match) return res.status(401).json({ message: 'Credenciales inválidas' });
  });
});
```

Cuando el usuario intenta loguear lo que hará el proceso interno en el backend será hacer una comparación del email, luego de esto procederá a comparar las contraseñas. El usuario introduce una contraseña y bcrypt le hará el mismo procedimiento de hashing y comprueba si al convertirla da el mismo resultado que la contraseña hasheada que se guardada en la base de datos.

3. middleware para rutas protegidas:

Se protegió el acceso a la ruta /Plataforma_gestion del lado del cliente mediante una validación estricta del JWT. Esto se hizo debido a que se podía acceder a la plataforma de gestión sin antes loguearse.

Se añadió un script que:

- Oculta el contenido de la página hasta verificar el token con el backend.
- Redirige automáticamente al login (/) si el token no es válido o ha expirado.
- Muestra el contenido **únicamente si la validación es exitosa**.

Esto lo hace mediante la verificación del token como vimos anteriormente creamos un .env que contiene la “firma digital del token”, complementario a esto en el backend (Express), se creó una **ruta protegida** /api/protected que solo responde si el token es válido. Asegura que las peticiones sensibles sólo puedan realizarse si el usuario tiene un token legítimo. Por lo tanto si alguien intenta saltarse el logueo colocando la ruta exacta de la página, no podrá acceder ya que no habrá un token existente ni firmado, este se crea exclusivamente cuando el logueo se concreta.

Código modificado:

```
app.post('/login', (req, res) => {

  const { email, password } = req.body;

  db.query('SELECT * FROM usuarios WHERE email = ?', [email], async (err, results) => {

    if (err || results.length === 0) return res.status(401).json({ message: 'Credenciales inválidas' });

    const user = results[0];

    const match = await bcrypt.compare(password, user.password);

    if (!match) return res.status(401).json({ message: 'Credenciales inválidas' });

    const token = jwt.sign({ userId: user.id, email: user.email }, process.env.JWT_SECRET, {

      expiresIn: process.env.JWT_EXPIRATION

    });

    res.json({ success: true, token });

  });

});
```

Como podemos ver hace primero todo el proceso de verificación y por último le asigna un token al usuario, para después proceder a firmarlo con el contenido de nuestro archivo **.env**.

Código del Middleware:

```
const authMiddleware = (req, res, next) => {

  const auth = req.headers.authorization;

  if (!auth) return res.status(401).send({ message: 'No autorizado' });

  const token = auth.split(' ')[1];

  jwt.verify(token, process.env.JWT_SECRET, (err, decoded) => {

    if (err) return res.status(403).send({ message: 'Token inválido o expirado' });

    req.user = decoded;

    next();
  });
};
```

4. Limitación de Intentos de Inicio de Sesión con **express-rate-limit**:

Antes un usuario podía intentar loguearse infinitas veces, esto es muy peligroso ya que da entrada a que los atacantes logren vulnerar el sistema mediante fuerza bruta, es por esto que se colocó un límite de intentos.

Código agregado:

```
const limiter = rateLimit({
  windowMs: 15*60*1000,
  max: 10,
  message: 'Demasiados intentos, prueba más tarde.'
});
```

```
app.use('/login', limiter);
```

El rate limit es una función proporcionada por el paquete **express-rate-limit** que permite establecer límites en la cantidad de solicitudes que un cliente puede hacer a un endpoint específico dentro de un intervalo de tiempo determinado.

Parámetros utilizados:

- **windowMs: 15 * 60 * 1000**
Define una ventana de tiempo de 15 minutos (en milisegundos).
Durante ese intervalo, se contará cuántas veces un cliente intenta acceder a **/login**.
- **max: 10**
Permite un máximo de **10 solicitudes por IP** dentro de esa ventana de 15 minutos.
Si se excede este límite, el servidor **bloqueará temporalmente** los intentos posteriores.
- **message: 'Demasiados intentos, prueba más tarde.'**
Es el mensaje que se enviará al cliente cuando supere el límite de intentos.

La línea:

```
app.use('/login', limiter);
```

indica que el middleware se aplicará únicamente a las solicitudes dirigidas a **/login**, lo que protege específicamente el endpoint de inicio de sesión sin afectar otras rutas de la aplicación.

Estas fueron todas las medidas de seguridad aplicadas al código de la página web.

También se realiza la división de servicios en diferentes servidores para no tener un único punto de falla y en caso de ser vulnerada nuestra red no accedan a todos los servicios en un solo servidor.

Aclaración por el cual no se realiza uso de Router, no se usa el router ya que el Firewall usado en este caso permite configuración de enrutamientos capa 3 por ende nos evitamos un punto de falla adicional y lo dejamos solo para la administración general de la red.

La configuración de las VLAN en los equipos de core quedaron asignados así:

En el Firewall:

Interfaces		
WAN	10Gbase-T <full-duplex>	192.168.200.228
LAN	10Gbase-T <full-duplex>	192.168.50.1
VLAN100DMZ	10Gbase-T <full-duplex>	172.10.16.1
VLAN101GERENCIA	10Gbase-T <full-duplex>	192.168.15.1
VLAN102ADMIN	10Gbase-T <full-duplex>	192.168.16.1
VLAN103CONTABILIDAD	10Gbase-T <full-duplex>	192.168.17.1
VLAN104SISTEMAS	10Gbase-T <full-duplex>	192.168.18.1
VLAN105OPERACIONES	10Gbase-T <full-duplex>	192.168.19.1
VLAN106MONITOREO	10Gbase-T <full-duplex>	192.168.20.1
VLAN107INVITADOS	10Gbase-T <full-duplex>	192.168.21.1

En nuestro SW

SWL3#sh vlan			
	VLAN Name	Status	Ports
r	1 default	active	Gi3/1, Gi3/2
o	99 DMZ	active	Gi0/1, Gi0/2, Gi0/3, Gi1/0 Gi1/1
l	101 Gerencia	active	Gi1/2
a	102 Admin	active	Gi1/3
x	103 Contabilidad	active	Gi2/0
z	104 Sistemas	active	Gi2/1
s	105 Operaciones	active	Gi2/2
n	106 Monitoreo	active	Gi2/3
m	107 Invitados	active	Gi3/0
o	200 VLAN0200	active	
o	300 VLAN0300	active	
s	1002 fddi-default	act/unsup	
s	1003 trcrf-default	act/unsup	
s	1004 fddinet-default	act/unsup	
s	1005 trbrf-default	act/unsup	

Dentro de los servicios que tenía adicionalmente se implementa un servidor de dominio para poder crear políticas de dominio y tener centralizado los usuarios de la empresa, allí mismo configuraremos un file server para que toda la data de los usuarios esté centralizada y poder realizar un backup óptimo.

Configuramos un equipo que se encargará de centralizar los backups realizados al file server y así administrar de manera fácil nuestros backups y realizar revisiones periódicas.

Se instala un Firewall para poder generar ACL y tener un mayor control de permisos a nivel general de nuestra red.

NMAP RED SEGURA:

nmap 172.10.16.0/24

```

root@kali: /home/kali
# nmap 172.10.16.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 15:22 -05
Nmap scan report for 172-10-16-1.lightspeed.clmasc.sbcglobal.net (172.10.16.1)
Host is up (0.0037s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 172-10-16-2.lightspeed.clmasc.sbcglobal.net (172.10.16.2)
Host is up (0.0091s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap scan report for 172-10-16-3.lightspeed.clmasc.sbcglobal.net (172.10.16.3)
Host is up (0.0051s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
3306/tcp  open  mysql

Nmap scan report for 172-10-16-4.lightspeed.clmasc.sbcglobal.net (172.10.16.4)
Host is up (0.0074s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap scan report for 172-10-16-102.lightspeed.clmasc.sbcglobal.net (172.10.16.102)
Host is up (0.0061s latency).

```

Escaneo Sigiloso nmap -sS -sV -sC 172.10.16.0/24

```

Help   root@kali: /home/kali
Sniffer  Reporter  Collaborator  Sequencer  Decoder  Composer  Logger  Organizer  Extensions  Learn
File Actions Edit View Help
ver
Nmap scan report for 172-10-16-2.lightspeed.clmasc.sbcglobal.net (172.10.16.2)
Host is up (0.050s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 90:58:3c:2c:fe:ee:81:1b:75:df:e4:3d:28:73:1d:d9 (ECDSA)
|_ 256 26:43:a8:b5:4b:ca:94:e2:a8:21:89:1f:6c:94:42:06 (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-generator: Astro v5.11.1
|_http-title: Heliopolis
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172-10-16-3.lightspeed.clmasc.sbcglobal.net (172.10.16.3)
Host is up (0.011s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql   MariaDB 10.3.23 or earlier (unauthorized)

Nmap scan report for 172-10-16-4.lightspeed.clmasc.sbcglobal.net (172.10.16.4)
Host is up (0.054s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 7f:43:52:09:32:ae:0f:23:3e:3c:9c:a2:5c:eb:b8:ba (ECDSA)
|_ 256 3f:27:64:c6:57:8a:16:7a:2b:22:f0:a7:9c:78:49:0a (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

```

Nmap scan report for 172-10-16-102.lightspeed.clmasc.sbcglobal.net (172.10.16.102)
Host is up (0.0058s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   start_date: 2025-07-30T20:28:21
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_  Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 71.61 seconds

```

(root@kali)-[/home/kali]

Se puede analizar que ya todo está descentralizado, cada servidor se encarga de un servicio en específico, por este motivo se mitigan riesgos.

Análisis de Nessus a red DMZ:

Scan Details

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 3:43 PM
- End: Today at 4:03 PM
- Elapsed: 20 minutes

Vulnerabilities

Critical	High	Medium	Low	Info
0	0	0	0	19

172.10.16.2 SRV WEB

Host Details

- IP: 172.10.16.2
- DNS: 172.10.16.2.lightspc.dlmasc.sbcg.global.net
- OS: Cisco Catalyst 9200 Series Switches, Cisco Catalyst 9300 Series Switches, Cisco Catalyst 9300 Rugged Series, Nutanix
- Start: Today at 3:43 PM
- End: Today at 3:50 PM
- Elapsed: 7 minutes
- KB: Download
- Auth: Fail

Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
LOW	2.1	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	HTTP (Multiple Issues)	Web Servers	3
INFO	SSH (Multiple Issues)	General	2
INFO	SSH (Multiple Issues)	Misc.	2
INFO	SSH (Multiple Issues)	Service detection	2
INFO				Nessus SYN scanner	Port scanners	2
INFO				Service Detection	Service detection	2
INFO				Apache HTTP Server Version	Web Servers	1
INFO				Backported Security Patch Detection (WWW)	General	1

172.10.16.3 DB

Scan DMZ / 172.10.16.3

Severity	CVSS	VPR	EPSS	Name	Family	Count
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO				Nessus Scan Information	Settings	1
INFO				Nessus SYN scanner	Port scanners	1
INFO				OS Fingerprints Detected	General	1
INFO				OS Identification	General	1
INFO				Service Detection	Service detection	1
INFO				TCP/IP Timestamps Supported	General	1
INFO				Traceroute Information	General	1

Host Details

- IP: 172.10.16.3
- DNS: 172.10.16.3.lightspeed.clmasc.sbcgl.Obal.net
- OS: Cisco Catalyst 9200 Series Switches, Cisco Catalyst 9300 Series Switches, Cisco Catalyst IE9300 Rugged Series Nutanix
- Start: Today at 3:43 PM
- End: Today at 3:50 PM
- Elapsed: 7 minutes
- KB: Download
- Auth: Fail

Vulnerabilities

Critical: 1, High: 8

172.10.16.4 APLICACIONES

Scan DMZ / 172.10.16.4

Severity	CVSS	VPR	EPSS	Name	Family	Count
Critical	2.1	2.2	0.0337	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	SSH (Multiple Issues)	General	2
INFO	SSH (Multiple Issues)	Misc.	2
INFO	SSH (Multiple Issues)	Service detection	2
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO				Nessus Scan Information	Settings	1
INFO				Nessus SYN scanner	Port scanners	1
INFO				OpenSSH Detection	Misc.	1

Host Details

- IP: 172.10.16.4
- DNS: 172.10.16.4.lightspeed.clmasc.sbcgl.Obal.net
- OS: Cisco Catalyst 9200 Series Switches, Cisco Catalyst 9300 Series Switches, Cisco Catalyst IE9300 Rugged Series Nutanix
- Start: Today at 3:43 PM
- End: Today at 3:48 PM
- Elapsed: 5 minutes
- KB: Download
- Auth: Fail

Vulnerabilities

Critical: 1, High: 15

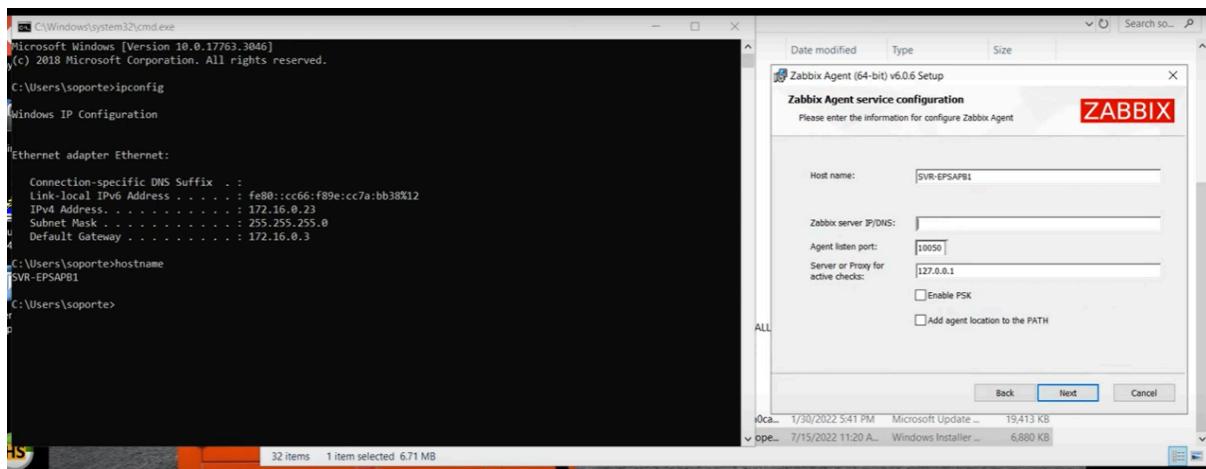
Podemos ver que en los servidores, la mayoría de vulnerabilidades son únicamente informativas, ocurre lo mismo que en la insegura, lo mejor sería proceder a hacer algunos cambios para que nuestros servidores no entreguen tanta información a los posibles atacantes y así prevenir.

ANEXO 9 Monitoreo y logs:

Para el sistema de control y monitoreo con logs se utilizó Zabbix, nos permite monitorear en todo momento distintas métricas, muy útil para entornos e implementaciones empresariales como es el caso de la empresa energética Heliópolis.

Instalación:

Ejecutamos el instalador y debemos saber la ip del equipo en el cual lo vamos a ejecutar, ya seguido es darle en siguiente y aceptar.



Una vez instalado y que se haya iniciado procedemos con agregar los host o equipos los cuales vamos a monitorear.

New host

Host IPMI Tags Macros Inventory Encryption Value mapping

* Host name

Visible name

Templates

* Groups

Interfaces No interfaces are defined.

[Add](#)

Description

Monitored by proxy

Enabled

Una vez agregados los equipos aparecen listados en la parte inferior del panel y ya se puede proceder a configurar todos los parámetros que se quieren monitorear, este paso ya es dependiendo las necesidades de cada empresa.

ZABBIX >> Create host

Monitoring Dashboard

Hosts Latest data

Maps Discovery

Services Inventory

Reports Configuration

Administration Support

Integrations Help

svr-zabbix

Host groups type here to search Select

IP Status

DNS Tags

Port Show hosts in maintenance

Show suppressed problems

Severity Not classified Warning High

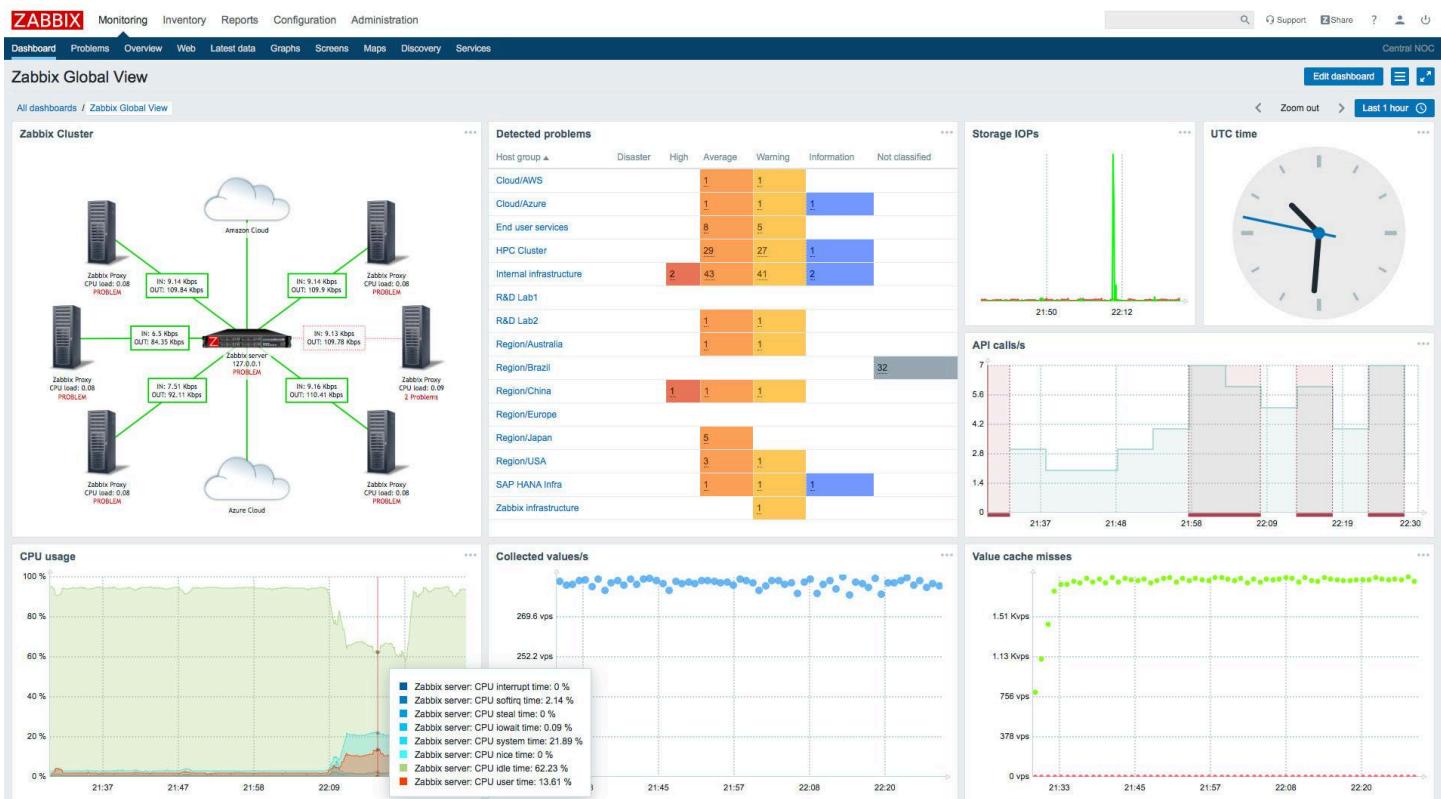
Information Average Disaster

Save as **Apply** **Reset**

Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
172.16.0.5:10050	ZBX	class: os target: windows	Enabled	Latest data 32	1	Graphs 5	Dashboards 2	Web
172.16.0.6:10050	ZBX	class: os target: windows	Enabled	Latest data 32	1	Graphs 5	Dashboards 2	Web
172.16.0.1:10050	ZBX	class: os target: windows	Enabled	Latest data 134	1	Graphs 16	Dashboards 2	Web
172.16.0.14:10050	ZBX	class: os target: windows	Enabled	Latest data 32	1	Graphs 5	Dashboards 2	Web
127.0.0.1:10050	ZBX	class: os class: software target: linux ***	Enabled	Latest data 129	1	Graphs 25	Dashboards 4	Web

Displaying 5 of 5 found

Ya configurados algunos parámetros en el panel se puede observar unas gráficas de mediciones las cuales se pueden ajustar a medida.



ANEXO 10 Simulación incidente:

1. Contexto de la Organización.

Nombre de la empresa: Heliópolis

Sector: Energía renovable

Infraestructura:

- Granjas solares con sensores IoT.
- Plataforma web para clientes (frontend en Astro).
- Backend API en Node.js/Express.
- Base de datos MySQL.
- Servidores centralizados para base de datos, backend y frontend.
- Ausencia de certificados SSL/TLS.

La empresa permite a sus clientes autenticarse desde la web para acceder a su consumo energético, estado de facturación y controlar sistemas de gestión energética inteligente.

2. Descripción del Incidente Simulado.

Tipo de incidente: Intercepción de tráfico - Ataque Man-In-The-Middle (MITM).

Fecha del incidente simulado: [25/07/2025].

Descripción técnica:

Un atacante con acceso a la misma red local que los usuarios (por ejemplo, en una red WiFi compartida o comprometida) explota la falta de cifrado HTTPS en la comunicación entre el cliente (navegador) y el backend de autenticación.

Al interceptar una petición **POST** de inicio de sesión usando una herramienta como **Wireshark**, el atacante logra visualizar en texto plano las credenciales (**email** y **password**) de los usuarios legítimos.

Herramientas utilizadas en el ataque simulado:

- Wireshark (para análisis de tráfico de red).
- Proxy mitmproxy / Burp Suite (opcional para demostrar manipulación activa).
- Navegador configurado sin verificación de certificados.
- Red sin cifrado (red WiFi simulada).

3. Detalles Técnicos de la Vulnerabilidad:

- **Causa raíz:** Ausencia de certificados SSL/TLS en el servidor. (**http://** en lugar de **https://**).
- **Vector de ataque:** Red local compartida o comprometida.
- **Datos comprometidos:** Credenciales de acceso de usuario (**email**, **password**) transmitidos en texto plano.
- **Impacto:** Acceso no autorizado a cuentas, manipulación de datos de consumo energético, posible sabotaje de gestión energética remota.

4. Resultado de la simulación:

- El atacante puede autenticarse como el cliente capturado y tener acceso completo a su cuenta, visualizar su historial de consumo, modificar parámetros de energía, e incluso activar o desactivar remotamente servicios conectados (en caso de funciones IoT).

5. Conclusión:

Este incidente demuestra cómo la ausencia de medidas básicas como HTTPS puede ser crítica en una infraestructura que gestiona recursos energéticos inteligentes. En un entorno real, este tipo de vulnerabilidad podría derivar en ataques de mayor escala como **secuestro de cuentas, sabotaje energético remoto, o robo de identidad**.

La simulación permite justificar la inversión en ciberseguridad, no solo como una protección técnica, sino como un **pilar estratégico para la continuidad operativa de la empresa**.

13. Bibliografía y Referencias:

- International Organization for Standardization. (2022). *ISO/IEC 27001:2022*: [ISO/IEC 27001:2022](#)
- International Organization for Standardization. (2022). *ISO/IEC 27002:2022*: [ISO/IEC 27002:2022](#)
- Congreso de la República de Colombia. (2012). *Ley 1581 de 2012*: [Ley 1581 de 2012](#).
- Consejo Nacional de Operación. (2025). *Acuerdo CNO 1960 del SIN*: [Acuerdo CNO 1960 del SIN](#).
- North American Electric Reliability Corporation (NERC), *NERC-CIP Standards*: [NERC-CIP Standards](#).

- MAGERIT v3.0, Metodología oficial:
[MAGERIT v3.0.](#)
- Archivos técnicos y manuales:
 - ❖ [Virtualbox.](#)
 - ❖ [Kali Linux.](#)
 - ❖ [Pfsense Installation.](#)
 - ❖ [Mikrotik.](#)
 - ❖ [Nessus.](#)