UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Infraestructura de virtualización para la gestión de datos de una estación de referencia de operación continua

TESINA

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Juan Manuel Peralta Rodríguez

DIRECTOR DE TESINA

Ing. José Abraham Bonilla Pastor

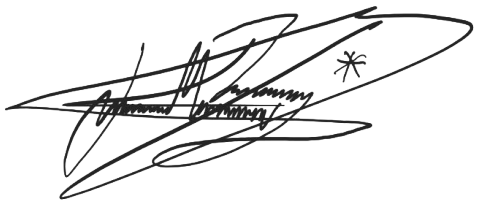
Ciudad Universitaria, Cd. Mx., 2026

PROTESTA UNIVERSITARIA DE INTEGRIDAD Y HONESTIDAD ACADÉMICA Y PROFESIONAL
(Titulación con trabajo escrito)

De conformidad con lo dispuesto en los artículos 87, fracción V, del Estatuto General, 68, primer párrafo, del Reglamento General de Estudios Universitarios y 26, fracción I, y 35 del Reglamento General de Exámenes, me comprometo en todo tiempo a honrar a la institución y a cumplir con los principios establecidos en el Código de Ética de la Universidad Nacional Autónoma de México, especialmente con los de integridad y honestidad académica.

De acuerdo con lo anterior, manifiesto que el trabajo escrito titulado INFRAESTRUCTURA DE VIRTUALIZACION PARA LA GESTION DE DATOS DE UNA ESTACION DE REFERENCIA DE OPERACION CONTINUA que presenté para obtener el titulo de INGENIERO EN COMPUTACIÓN es original, de mi autoría y lo realicé con el rigor metodológico exigido por mi Entidad Académica, citando las fuentes de ideas, textos, imágenes, gráficos u otro tipo de obras empleadas para su desarrollo.

En consecuencia, acepto que la falta de cumplimiento de las disposiciones reglamentarias y normativas de la Universidad, en particular las ya referidas en el Código de Ética, llevará a la nulidad de los actos de carácter académico administrativo del proceso de titulación.



JUAN MANUEL PERALTA RODRIGUEZ
Número de cuenta: 317355723

Agradecimientos

La culminación de este proyecto representa no solo un esfuerzo personal, sino el fruto del acompañamiento y la guía de quienes estuvieron a mi lado durante toda mi formación en la Facultad de Ingeniería.

A mis padres Erendira Rodriguez Tapia y Edgar Joel Peralta Cheu, por ser un apoyo inquebrantable en el recorrido de toda mi vida escolar. Todo este camino fue posible gracias a su esfuerzo, y poder dedicarles la finalización de este ciclo es, sin duda, cerrar con broche de oro esta gran etapa.

A mi hermana Luz Erendira Peralta Rodríguez, quien me inspiró más de una vez a no rendirme y a seguir avanzando frente a cada obstáculo.

A toda mi familia, por estar siempre presente, creyendo en mí y dándome los ánimos incondicionales para continuar y llegar hasta aquí.

A mis compañeros de clase, que a lo largo de este trayecto se convirtieron en amigos verdaderos y en una segunda familia: Daniel, Karla, Luis, Uriel, Manuel, Cesar, Days, Frank, Erandi, Charly y Fernanda. Gracias por aceptar que hiciéramos equipo, por apoyarnos mutuamente para sobrellevar la presión y por darnos el impulso necesario para pasar cada una de las materias.

A mis profesores, por compartir sus conocimientos y enseñarme todo lo que hoy sé, pero, sobre todo, por ayudarme a forjar el carácter y la disciplina necesarios para afrontar las distintas situaciones que se presenten de ahora en adelante.

Este documento es con especial dedicatoria a las memorias de:

Teodoro Rodríguez García e Ildefonso Peralta Galvez

Con este importante paso, por fin cumplo una promesa que hice mientras se encontraban en vida. Su ausencia física no impidió que su recuerdo fuera un motor para llegar hasta aquí.

ÍNDICE

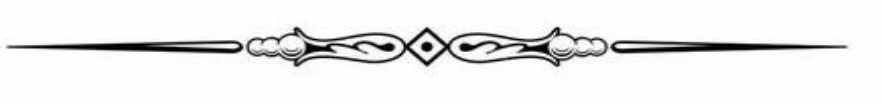
TABLAS, IMÁGENES Y ESQUEMAS

Resumen

El presente documento detalla el proceso de implementación de una infraestructura de virtualización que tiene como objetivo realizar una conexión entre la Facultad de Ingeniería de la Universidad Nacional Autónoma de México y el Instituto Nacional de Estadística y Geografía (INEGI) al integrar la Estación de Referencia de Operación Continua (CORS) administrada por el Departamento de Geodesia y Cartografía de la División de Ingeniería Civil y Geomática (DICYG) de la Facultad de Ingeniería, a la Red Geodésica Nacional Activa (RGNA) del INEGI, con la finalidad de facilitar el acceso público, eficiente y seguro a los datos que dicha estación genera mediante soluciones que aplican principios de Ingeniería en Computación garantizando la correcta diseminación y disponibilidad de la información geoespacial de esta estación.

Abstract

This document details the implementation process of a virtualization infrastructure aimed at establishing a connection between the Faculty of Engineering of the National Autonomous University of Mexico and the National Institute of Statistics and Geography (INEGI) by integrating the Continuously Operating Reference Station (CORS)—managed by the Department of Geodesy and Cartography of the Division of Civil and Geomatic Engineering (DICYG) of the Faculty of Engineering—into INEGI's Active National Geodetic Network (RGNA). The purpose is to facilitate public, efficient, and secure access to the data generated by this station through the application of Computer Engineering principles, creating a virtualization-based infrastructure to guarantee the proper dissemination and availability of its geospatial information.



INTRODUCCIÓN

Introducción

El dinamismo de la era digital y la creciente demanda de consulta de información inmediata y veraz son factores que fomentan la transición hacia infraestructuras basadas en software. En este panorama, el aislamiento técnico de los sistemas de información constituye un desafío crítico que limita la eficiencia operativa y la toma de decisiones en tiempo real donde resulta imperativo implementar mecanismos de interoperabilidad que permitan el procesamiento fluido de datos.

Partiendo de esta premisa, el presente proyecto surge como un ejercicio de integración en el cual se presenta la implementación de una infraestructura de virtualización diseñada para establecer un ‘puente digital’ por el cual se realizará la transferencia de las observaciones satelitales GNSS generadas por la estación en forma de datos entre la Facultad de Ingeniería de la UNAM y el Instituto Nacional de Estadística y Geografía (INEGI) al integrar la Estación de Referencia de Operación Continua (CORS, por sus siglas en inglés) administrada por el Departamento de Geodesia y Cartografía perteneciente a la División de Ingenierías Civil y Geomática (DICyG) de la Facultad de Ingeniería a la Red Geodésica Nacional Activa (RGNA) del INEGI desde un enfoque que prioriza la eficiencia y la seguridad informática en la gestión de los datos suministrados por esta estación de referencia.

Desde que la Facultad de Ingeniería recibió la donación de la estación de referencia a lo largo del semestre 2025-1 hasta el inicio del desarrollo de este proyecto esta estación de referencia operó de manera totalmente aisalda, es decir, la información se encontraba limitada y no existía un flujo de los datos en tiempo real hacia el exterior o interior de la facultad, restringiendo su potencial como nodo de información geodésica y confinando el procesamiento de sus activos a una red local.

Frente a este escenario de aislamiento, se propuso el diseño e implementación de un ecosistema controlado mediante una infraestructura de virtualización, la cual actúa como el eje motor para la creación de entornos de

ejecución aislados donde pueden coexistir de manera armónica procesos críticos como la administración de datos de alta precisión e instancias de experimentación y gestión administrativa, optimizando los recursos físicos (hardware) disponibles y garantizando que los datos generados por la estación de referencia se mantengan congruentes y seguros.

La estructura de este documento se organizó de manera sistemática en la cual se toman en cuenta 4 etapas para el desarrollo y culminación del despliegue de esta infraestructura, dividiendo dicha implementación de la siguiente manera:

- **Capítulo 1. Antecedentes y Justificación:** Se establece el origen del proyecto, contextualizando el entorno tecnológico con el que se contaba dentro del Departamento de Geodesia y Cartografía de la DICyG, así como la problemática que motivó la búsqueda de esta solución, definiendo en este capítulo la importancia estratégica de crear un sistema de comunicación que sea resiliente ante las posibles amenazas externas e internas que pudieran afectar la congruencia de los datos que se manejan.
- **Capítulo 2. Marco Teórico:** Se analizan los pilares técnicos que sustentan la solución, analizando definiciones importantes como servidores, virtualización, hipervisor, firewall, red virtual privada (VPN), entre otras. Esto proporciona la base teórica necesaria para comprender la elección de las herramientas seleccionadas para desarrollar este proyecto.
- **Capítulo 3. Implementación de la Solución:** Este capítulo articula la fase práctica y el núcleo del proyecto detallando en primera instancia la configuración de un servidor de máquinas virtuales como base operativa principal, posteriormente, se describe la creación de una máquina virtual que se encargará de la administración de los datos que la estación de referencia genera, almacenando y proveyendo la información mediante la puesta en marcha de dos servidores, un servidor FTP y un servidor web, asimismo, se desglosa la integración de un firewall junto con la definición de reglas para el filtrado del tráfico entrante para finalmente detallar la configuración de un

servidor VPN que proveerá un acceso remoto cifrado para salvaguardar la integridad de la administración de la estación de referencia.

- **Capítulo 4. Verificaciones finales y entrega:** Se valida el desempeño integral de la arquitectura, confirmando la operatividad final de la infraestructura implementada mediante una verificación del flujo de datos entre la estación de referencia y el usuario final, verificando el rendimiento del servidor de virtualización junto con el funcionamiento de la máquina virtual utilizada para desarrollar este proyecto y el correcto despliegue de los servidores FTP y web dentro de esta, también se corrobora que el redireccionamiento de puertos establecido dentro del firewall que protege a la estación de referencia esté correctamente declarado para finalmente mencionar la entrega formal del proyecto.

La meta es garantizar que la información generada dentro de la estación de referencia, desde su obtención (dentro de la Facultad de Ingeniería) hasta su disposición como un bien público a través del portal del INEGI, mantenga altos estándares de integridad, disponibilidad y accesibilidad como los establecidos en el ISO/IEC 27002, logrando convertir dicha estación en un nodo de información seguro y constante de la Red Geodésica Nacional Activa del INEGI (organismo rector de la información geográfica en el país).

CAPÍTULO 1

ANTECEDENTES Y JUSTIFICACIÓN

Capítulo 1. Antecedentes y justificación

La donación de una estación de referencia de operación continua (CORS) GNSS (**Imagen 1**) a la Facultad de Ingeniería de la UNAM (la cual es administrada actualmente por el Departamento de Geodesia y Cartografía de la DICyG) presentó una oportunidad estratégica. Bajo esta premisa es que el Dr. Juan Daniel Castillo Rosas, jefe del departamento durante el desarrollo de este proyecto, impulsó la iniciativa y realizó la solicitud formal para integrar dicha estación a la Red Geodésica Nacional Activa (RGNA) del Instituto Nacional de Estadística y Geografía (INEGI).

Imagen 1. Estación de Referencia de Operación Continua de la Facultad de Ingeniería de la UNAM.

Dicha solicitud que realizo el Dr. Juan Daniel Castillo Rosas se centró en cómo lograr establecer dicha conexión y poder compartir de manera segura las observaciones satelitales GNSS generadas por la estación de referencia, ya que estas se encontraban aisladas y subutilizadas, lo que impedía el aprovechamiento por parte de la comunidad geodésica, académica y profesional de estas posiciones geodésicas que pueden aportar valiosos conocimientos y puntos de referencia en el desarrollo de investigaciones y prácticas.

Para entrar en contexto, el **INEGI** es un organismo público autónomo de México que funge como ente rector encargado de normar y coordinar el Sistema Nacional de Información Estadística y Geográfica de México, teniendo como objetivo central captar y difundir información de alta calidad y exactitud sobre el territorio, los recursos y la población de la república.

Para este proyecto, se destaca una de las infraestructuras con las que el INEGI cuenta, la **Red Geodésica Nacional Activa (RGNA)**, esta es un conjunto de estaciones de monitoreo continuo operadas tanto por el INEGI como por otros terceros y constituye el marco de referencia oficial para el posicionamiento geodésico de alta precisión en el país, esta red es una de las bases para la cartografía, grandes obras de ingeniería y el estudio de la dinámica terrestre, donde las estaciones que la conforman están distribuidas en todo el territorio nacional y operan de forma permanente con el propósito de proporcionar servicios de posicionamiento geodésico de alta precisión.

Sin embargo, tras una primera reunión para aclarar objetivos, alcances y fases de desarrollo para lograr que la estación de referencia de la facultad se incorpore dentro de la RGNA se concluyó que desarrollar esta conexión implicaría la implementación de una infraestructura computacional y el reforzamiento de la seguridad perimetral de red de la estación de referencia.

En primer lugar, la estación de referencia (ubicada en el edificio B del conjunto Norte de la Facultad de Ingeniería) estaba conectada directamente a la red externa, es decir, el acceso a la configuración de la estación no se encontraba tan restringido, lo que significaba una vulnerabilidad critica ante posibles ataques informáticos e implicaba un riesgo de pérdida de las observaciones satelitales GNSS generadas por la estación de referencia, en segundo lugar, desarrollar la conexión implicaba la habilitación de un servidor FTP y un servidor web (ubicados en el edificio R del conjunto Sur de la Facultad de Ingeniería) para el almacenamiento y publicación de los datos generados por la estación de referencia con los interesados en ellos a través del INEGI.

Por lo tanto, la solución técnica se centró en definir como implementar dicha conexión y simultáneamente salvaguardar la información de manera eficiente aprovechando el equipo de cómputo existente en el departamento, llegando a la siguiente propuesta de desarrollo.

Solución propuesta

El desarrollo de este proyecto buscó introducir la estación de referencia de la Facultad de Ingeniería a la RGNA para así crear una conexión entre la facultad con el INEGI y posteriormente con el público en general mediante la publicación de los datos generados por la estación mediante el uso de los recursos de cómputo disponibles en del departamento.

Por ende, se hizo disposición de un equipo de cómputo (**Imagen 2**) con las características suficientes para crear un servidor de alto rendimiento, permitiendo proponer el diseño de una arquitectura de tecnología de la información (TI) basada en la virtualización.

Imagen 2. Equipo de cómputo utilizado para el desarrollo del proyecto.

La primer parte de la propuesta planteó la neutralización del punto crítico de vulnerabilidad de la estación de referencia, concretamente se buscó evitar que la estación estuviera conectada directamente a la red externa mediante la implementación de un firewall encargado de aislar la estación creando un perímetro

de seguridad que controlara y filtrara minuciosamente todo el tráfico entrante y saliente, la función del firewall es actuar como guardia de control de la estación, permitiendo únicamente el paso de los datos autorizados y bloqueando cualquier intento de acceso potencialmente malicioso.

Por otra parte, para gestionar los datos generados por la estación se propuso implementar una infraestructura de virtualización al convertir el equipo de cómputo visualizado en la Imagen 2 en un servidor de máquinas virtuales, un servidor que permitirá crear máquinas y servidores virtuales dentro de un solo equipo de cómputo que funcionen de manera aislada entre ellos permitiendo crear la infraestructura necesaria para establecer la conexión entre la Facultad de Ingeniería y el INEGI con el objetivo de dejar recursos disponibles para el desarrollo de futuros proyectos sin afectar el funcionamiento final de este proyecto.

Una vez creado el servidor de máquinas virtuales, se procedería a crear dentro de este una máquina virtual capaz de gestionar los datos proporcionados por la estación de referencia, y al mismo tiempo, hospedar tanto el servidor FTP como el servidor web necesarios para la publicación de los datos, buscando la compatibilidad con las aplicaciones proporcionadas por el fabricante de la estación para administrar el servidor NTRIP interno de la estación el cual permite compartir datos de corrección en tiempo real, esto con el fin de usar los datos generados por la estación para el beneficio de 3 áreas de interés:

- **Académica y formativa**. Donde la integración de la estación en una red nacional convierte a la Facultad de ingeniería en un nodo activo del marco geodésico de México, ofreciendo a estudiantes y docentes una plataforma de vanguardia para la enseñanza práctica, el desarrollo de proyectos y la investigación aplicada.
- **Investigación.** Al añadir un nuevo punto de monitoreo continuo de alta precisión a la RGNA, este proyecto enriquece la densidad de la red, ya que proporcionar los datos generados por la estación significa más información de apoyo para investigadores de toda la nación que estudian desde

fenómenos como la dinámica de la corteza terrestre, la subsidencia del terreno y la sismología, hasta atmosféricos como el impacto de la radiación solar en la ionosfera.

- **Social y profesional.** Al hacer los datos públicos y accesibles a través del INEGI se democratiza el acceso a información geoespacial de alta calidad, beneficiando directamente a profesionales de la topografía, la ingeniería civil y la planeación urbana, además de potenciar aplicaciones en gestión de riesgos y desarrollo de infraestructura.

Aprobación y fases de desarrollo

Después de presentar la propuesta de solución descrita anteriormente, esta fue sometida a revisión y aprobada en una segunda reunión con el Dr. Juan Daniel Castillo Rosas; fue en ese momento que se puso formalmente en marcha el desarrollo del proyecto, el cual se dividió en las siguientes 4 fases técnicas:

Fase 1: Despliegue de una infraestructura de virtualización. Donde se implementó un servidor de virtualización (Hipervisor) en el edificio R del Conjunto Sur de la Facultad de Ingeniería de la UNAM; sobre este servidor se desplegó una máquina virtual (VM) dedicada y configurada para operación continua, con el rol específico de gestionar la ingesta, procesamiento y almacenamiento de los datos provenientes de la estación de referencia.

Fase 2: Implementación de seguridad perimetral. Se configuró e implementó un dispositivo como Firewall dedicado (con pfSense como sistema operativo), con el objetivo de crear un segmento de red seguro (**DMZ** o **zona desmilitarizada**[1]) para la estación de referencia, ubicada en la cúpula del edificio B del Conjunto Norte de la Facultad de Ingeniería, protegiéndola de amenazas externas.

[1] **Zona desmilitarizada.** segmento de red perimetral que crea una capa adicional de seguridad entre una red interna y una red no confiable

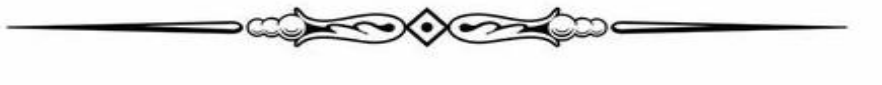
Fase 3: Configuración de servicios y herramientas administrativas. Dentro de la máquina virtual principal, se instalaron y configuraron los servicios de publicación de datos: un servidor FTP para la transferencia de archivos entre la estación de referencia y la máquina virtual, un servidor web para la consulta de los datos; paralelamente, se instaló el software propietario del fabricante para la administración y monitoreo del servidor NTRIP interno de la estación.

Fase 4: Verificaciones finales y entrega. Se ejecutó una fase de pruebas integrales para validar el flujo completo de los datos, desde la estación de referencia hasta los servidores de publicación; esta etapa incluyó la revisión de la configuración de red y servicios implementados, culminando con la entrega formal del proyecto para integrar la estación de referencia a la RGNA.

Sin embargo, el desarrollo de un proyecto de esta naturaleza no comenzó con la configuración de un servidor, sino con el establecimiento de un lenguaje común que permitió el entendimiento de la implementación de esta infraestructura, ya que para esto se toman en cuenta la Ingeniería de Redes, la Ciberseguridad y la Administración de Sistemas. Debido a esto, antes de detallar la ejecución técnica del proyecto se establecieron los cimientos teóricos de este, donde se definen los principios, tecnologías y estándares que sustentan la solución.

CAPÍTULO 2

MARCO TEÓRICO



Capítulo 2. Marco teórico

Servidor

En el mundo de la computación, el término “servidor” representa un elemento clave en la arquitectura de las redes de datos; de acuerdo con Tanenbaum y Wetherall [1] y Tanenbaum y Van Steen [2], formalmente, un servidor es un sistema computacional estructurado por hardware especializado, software del sistema o aplicaciones específicas con la finalidad de almacenar, procesar, gestionar y distribuir datos, recursos o servicios, para que otros equipos, llamados clientes, puedan acceder a dicha información o funcionalidad de forma remota, segura y eficiente.

Este tipo de interacción se conoce como el modelo cliente-servidor (**Imagen 3**) el cual es una de las bases sobre la cual se desarrollan la mayoría de los servidores modernos, desde esta perspectiva, el servidor se concibe como un proceso en ejecución que permanece en espera para atender solicitudes de uno o varios clientes, ofreciendo servicios específicos a través de una red que puede ser tan simple como una conexión local o tan amplia como internet, y operando bajo protocolos de red estandarizados como TCP/IP.

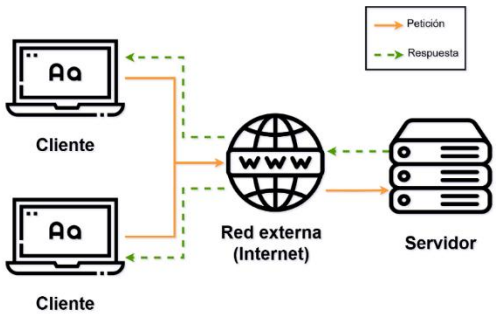


Imagen 3. Ejemplificación del modelo cliente servidor.

Como indican Tanenbaum y Van Steen [2], Los servidores tienen la capacidad de atender simultáneamente cientos o miles de clientes, facilitando la interacción constante y eficiente dependiendo el tipo de servicio que proveen, pueden clasificarse como servidores FTP, servidores web, servidores de correo electrónico, servidores de bases de datos, entre otros.

Dentro de la amplia variedad de servidores existentes, es fundamental profundizar en dos tipos representativos debido a su uso predominante en el desarrollo de este proyecto, el servidor web y el servidor FTP.

Servidor web

Un servidor web hace uso del protocolo *HTTP (Hypertext Transfer Protocol)*, el cual es un protocolo de la **capa de aplicación**[2] y es utilizado para la comunicación en la web, funciona sobre **TCP/IP**[3] y permite la transferencia de documentos de hipertexto (como páginas web) desde el servidor hacia el navegador cliente, es un protocolo orientado a la conexión basado en peticiones y respuestas para obtener recursos de forma eficiente, este protocolo define la manera en la que el servidor procesa las solicitudes del cliente, responde con los recursos necesarios (como paginas HTML, imágenes, archivos, etc.) manteniendo la comunicación para ofrecer contenido en respuesta a peticiones HTTP, entonces, siguiendo a Tanenbaum y Wetherall [1], se puede definir un servidor web como una aplicación o proceso que, ejecutándose sobre un equipo de cómputo, gestiona y atiende solicitudes a clientes a través del protocolo HTTP del modelo TCP/IP.

Servidor FTP

Tal como señalan Tanenbaum y Wetherall [1], Un servidor FTP *(File Transfer Protocol)* hace uso del protocolo con el mismo nombre el cual pertenece a la capa de aplicación, al igual que el protocolo HTTP, este protocolo permite la transferencia unidireccional o bidireccional de archivos entre clientes y el servidor, donde cada cliente se conecta al servidor mediante una autenticación única para ejecutar comandos como listar, cambiar directorios, descargar archivos, entre otros, de tal manera que la información viaje de manera correcta y segura.

[2] **Capa de aplicación.** Capa del modelo OSI o protocolo TCP/IP, cuya función principal es proveer servicios de red directamente a las aplicaciones de los usuarios (navegadores web, clientes de correo, clientes FTP).
[3] **TCP/IP.** Protocolo que define las reglas para la transferencia de datos desde el origen hasta el destino.

Virtualización

De acuerdo con Portnoy [3], La virtualización es la tecnología que permite crear una representación digital de un sistema (hardware, sistema operativo y aplicaciones), es decir, abstraer el componente físico en un objeto digital con la finalidad de maximizar la utilización del recurso que dicho objeto proporciona, en el ámbito de la computación se puede decir que la virtualización es la administración de recursos de hardware mediante un *hipervisor* para poder representar un sistema mediante software.

Gracias a la virtualización es posible ejecutar múltiples sistemas aislados en una única máquina física por medio de un hipervisor, es decir, los sistemas no pueden interactuar directamente con los demás facilitando la consolidación de servidores, es un proceso que optimiza la infraestructura de un centro de datos al permitir llevar a cabo varias cargas de trabajo en un número menor de equipos computacionales físicos, optimizando la utilización de recursos y reduciendo los gastos de hardware, energía y refrigeración.

Como detalla Portnoy [3], Existen 3 tipos de virtualización:

- **Virtualización completa.** El hipervisor se encarga de **emular**[4] el hardware subyacente para de esta forma interceptar y traducir todas las instrucciones que el sistema operativo virtualizado ejecuta.
- **Virtualización asistida por hardware.** Usa características específicas del hardware para mejorar la eficiencia y rendimiento de la virtualización, permitiendo que el sistema operativo virtualizado tenga acceso a estas características mejorando el desempeño de las máquinas virtuales.
- **Para-virtualización.** Modifica el sistema operativo virtualizado para una mejor comunicación con el hipervisor, de esta forma se eleva el rendimiento eliminando capas de emulación.

[4] **Emular.** Imitar acciones y/o funciones, procurando igualarlas e incluso excederlas.

Hipervisor

En palabras de Portnoy [3], el hipervisor es un software que funciona como capa de abstracción que gestiona la asignación y el control de los recursos físicos (CPU, memoria, almacenamiento, red) entre las distintas máquinas virtuales (VM) que se ejecutan en un servidor.

Como se ilustra en la **Imagen 4**, existen dos tipos de hipervisores:

- **Hipervisor tipo 1 (bare-metal):** Se instala directamente sobre el hardware del servidor. Esto permite obtener un alto rendimiento, ya que tiene acceso directo a los recursos físicos, logrando que cada máquina virtual esté totalmente aislada de las demás.
- **Hipervisor tipo 2 (hosted):** Se ejecuta como una aplicación sobre un sistema operativo anfitrión (*host*). Esto hace que tanto el rendimiento como el nivel de aislamiento de cada máquina virtual sean inferiores en comparación con un hipervisor *bare-metal*, debido a la capa de abstracción adicional y al uso común del kernel del sistema operativo *host*.

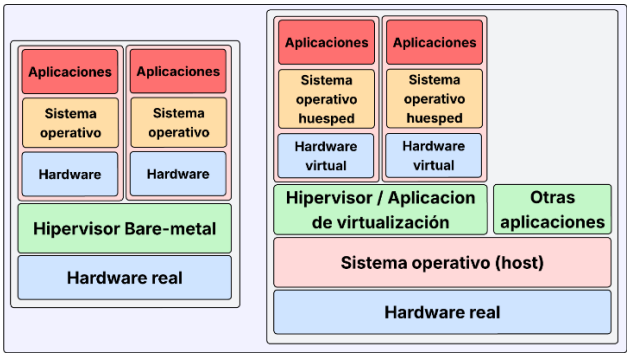


Imagen 4. Tipos de hipervisores.

Máquina virtual (VM)

Según Portnoy [3], la máquina virtual es un entorno virtual que representa un equipo de cómputo mediante software, teniendo su propio sistema operativo y hardware virtualizado permitiendo ejecutar sus aplicaciones de manera aislada e independiente de otras máquinas virtuales o sistemas operativos hosts, asumiendo el caso en que haya más de una máquina virtual existente.

Servidor virtual

Un servidor virtual es una máquina virtual configurada para desempeñar las funciones de un servidor, la diferencia entre un servidor físico y uno virtual radica en que un servidor físico es un equipo de cómputo real con sus propios componentes (CPU, RAM, disco duro, etc.) que ejecuta un único sistema operativo y sus aplicaciones, por otra parte, un servidor virtual es parte de un equipo de cómputo físico que funciona dentro de un hipervisor, permitiendo que dicho sistema de cómputo físico aloje múltiples servidores virtuales, cada uno con su propio sistema operativo y recursos aislados ofreciendo una alta flexibilidad, escalabilidad y alta eficiencia para la administración de las tareas en ejecución.

Seguridad informática

Para Tanenbaum y Wetherall [1], la seguridad informática busca garantizar la protección de la información frente a accesos no autorizados, ataques y fallos en la comunicación mediante el uso de protocolos para la administración segura de claves y autenticación de usuarios mediante dispositivos como Firewalls y un conjunto de tecnologías como redes privadas virtuales (VPN), sistemas de prevención y detección de intrusos (IDS/IPS), redirección/reenvío de puertos, entre otros.

Firewall

Como explican Tanenbaum y Wetherall [1], un firewall (o cortafuegos) actúa como una barrera de seguridad que monitorea, filtra y controla el tráfico de datos entrante y saliente entre una red interna confiable y redes externas consideradas no seguras (como internet). Su propósito es gestionar el acceso a los recursos y evitar la propagación de amenazas informáticas, basándose en un conjunto de reglas de seguridad predefinidas.

Como se ejemplifica en la **Imagen 5**, el funcionamiento del firewall consiste en examinar cada paquete de datos que intenta entrar o salir de la red. Este proceso compara el tráfico con las políticas establecidas en el sistema (tales como filtrado

por dirección IP, asignación de puertos, protocolos o contenido del paquete) para decidir si se permite o se bloquea el paso de la conexión.

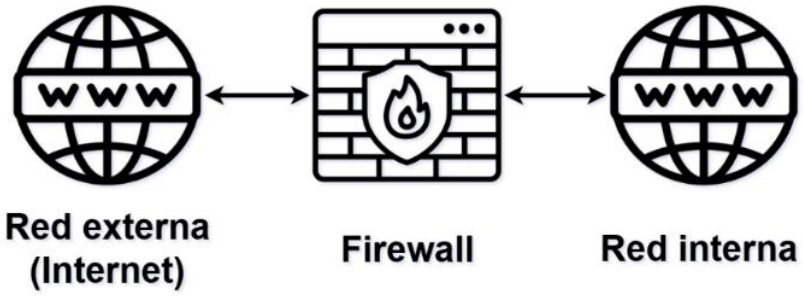


Imagen 5. Funcionamiento de un firewall.

Red Privada Virtual (VPN)

De acuerdo con Tanenbaum y Wetherall [1], la red privada virtual (VPN) crea una red privada dentro de un túnel cifrado que se comunica a través de infraestructuras públicas (como internet) que permite a los usuarios acceder a recursos de una red privada remota mediante este túnel y la autenticación de la conexión que permite proteger los datos transmitidas de manera segura y privada a través de dichas redes públicas.

Redirección/reenvío de puertos

Según la documentación de Red Hat Enterprise Linux [4], el reenvío de puertos es una técnica de red que redirige estáticamente las solicitudes de comunicación desde una combinación especifica de dirección IP y número de puerto público hacia otra privada y viceversa a través de un NAT de manera segura, este proceso ocurre mientras los paquetes de datos atraviesan un dispositivo de red como un Firewall y tiene el propósito de permitir que clientes externos (ubicados fuera de una red local) puedan conectarse a una computadora o un servicio específico que opera dentro de una red local privada (servidores web, de correo o FTP) de manera segura, ya que funge como un filtro que permite controlar que tipo de tráfico puede acceder a los dispositivos internos, dando paso solo a las conexiones dirigidas a puertos específicos que lleguen a un servicio designado bloqueando el resto del tráfico no deseado.

En síntesis, estos son considerados los conceptos clave para el entendimiento de las terminologías utilizadas a lo largo del desarrollo de este proyecto dejando base sólida teórica y referencial establecida. A partir de este punto, se da paso a la fase de implementación de la solución, donde dichos fundamentos se aplicarán de manera práctica para materializar la propuesta, dar respuesta a la problemática planteada y alcanzar los objetivos definidos.

CAPÍTULO 3

IMPLEMENTACIÓN DE LA SOLUCIÓN

Capítulo 3. Implementación de la solución

Para la implementación de la solución, se planificó un desarrollo de lógica secuencial y lineal que garantizara tanto la integridad de los datos, así como la operatividad de la infraestructura planteada, alineando el diseño con los del departamento de Cartografía y Geodesia, priorizando el aprovechamiento de los recursos de hardware existentes, la estrategia de distribución de la información dentro de la UNAM y la eficiencia en la entrega de los datos, dejando estos listos para ser consultados por los interesados.

Fase 1: Despliegue de una infraestructura de virtualización.

La etapa inicial consistió en diseñar una arquitectura que facilitara la gestión de los datos provenientes de la estación de referencia, permitiendo que el administrador gestionara la información de manera intuitiva y optimizando el hardware disponible para asegurar la compatibilidad con iniciativas futuras dentro del departamento.

Para ello, se seleccionó un **modelo de virtualización**, ya que permite cumplir con los requerimientos de este proyecto y ofrece una estructura flexible basada en tres objetivos críticos que garantizan la seguridad y la escalabilidad (Portnoy, 2003):

1. **Aislamiento de recursos.** Separar el entorno operativo del servicio de datos GNSS respecto a otras aplicaciones, garantizando así su integridad, seguridad y estabilidad dentro de la infraestructura de virtualización.
2. **Escalabilidad de la infraestructura.** Permitir la expansión del servicio para la adición de entornos de prueba, el desarrollo de futuros proyectos y el aprovechamiento de la flexibilidad que ofrece este tipo de infraestructura.
3. **Optimización de recursos.** Adaptar el hardware disponible para cumplir con el desarrollo de este proyecto, tomando en cuenta la demanda de procesamiento que se puede tolerar y centralizando la administración de los datos, simplificando los procesos de respaldo y recuperación de manera que no haya perdida de información al desarrollar nuevos proyectos.

Por lo tanto, para cumplir cabalmente con estos objetivos y con el desarrollo del proyecto es que se evaluó de manera minuciosa las características técnicas del equipo de cómputo proporcionado por el departamento (detalladas en la tabla 1) para el desarrollo de la infraestructura propuesta.

Componente	Especificaciones
Procesador (CPU)	Intel® Core™ i9-14900KF
Memoria RAM	64 GB
Almacenamiento	1.8 TB
Tarjeta de Red	Adaptador de red Ethernet Intel® I226-T1
GPU	NVIDIA RTX A5000

Tabla 1. Características técnicas del servidor anfitrión (host).

Dado que las especificaciones de hardware fueron suficientes para su configuración como un servidor, es que se procedió a instalar en el equipo un hipervisor bare-metal (hipervisor tipo 1), lo que convirtió finalmente el equipo de cómputo en un servidor de máquinas virtuales, la base de la infraestructura de virtualización.

Desde una perspectiva técnica, la decisión de transformar el equipo en un servidor de máquinas virtuales se fundamentó, en primer lugar, en las capacidades del procesador Core i9-14900KF, ya que su elevado número de núcleos y soporte nativo para tecnologías de virtualización asistida por hardware (Intel VT-x) posibilitan la ejecución concurrente y de alto rendimiento de múltiples instancias de propósito general o específico, dependiendo de lo que se busque implementar o desarrollar.

Por otra parte, los 64 GB de RAM disponibles ofrecen un margen operativo robusto para gestionar los recursos de las máquinas virtuales creadas o por crear (incluyendo la involucrada en el desarrollo de este proyecto) y del hipervisor implementado, permitiendo gestionar y planear de manera más certera el desarrollo de nuevos proyectos, tomando en cuenta que los 1.8 TB de almacenamiento garantizan un espacio suficiente para para la creación de nuevas máquinas virtuales.

Finalmente, el adaptador de red Intel® I226-T1 al ser un componente apto para cargas de trabajo intensivas, asegura la baja latencia y alta fiabilidad de los paquetes de datos enviados y recibidos, siendo todas características indispensables para la transmisión continua de los datos requerida en el desarrollo de este proyecto.

Selección de un hipervisor

Al no existir un solo sistema operativo que permita convertir el equipo de cómputo en un hipervisor bare-metal, para tomar la elección final fue necesario también tomar en cuenta el costo-beneficio del desarrollo de este proyecto, la complejidad de implementación que este conlleva y la fácil administración por parte del receptor final del mismo.

En primer lugar, **VMware ESXI** es un software muy usado en la industria corporativa, es extremadamente robusto y estable, ya que posee un ecosistema de herramientas de gestión avanzado (vCenter), por otra parte, **Microsoft Hyper-V** viene integrado en Windows y tiene una correcta integración con Azure y herramientas de Windows, el cual es administrable mediante PowerShell o una interfaz gráfica de Windows, sin embargo estas opciones se descartan, ya que al momento del desarrollo del proyecto no se contaba con una licencia activa de Windows server o de VMware ESXI, ni con el tiempo requerido para solicitarla.

Por lo que se decidió cambiar el enfoque y se optó por usar alguna herramienta de software libre como **Kernel-based Virtual Machine - QEMU (KVM QEMU)**, un módulo del kernel de Linux que convierte al host en un hipervisor bare-metal, o **Proxmox Virtual Environment (Proxmox VE)**, un sistema operativo de código abierto basado en Debian GNU/Linux que junto con KVM - QEMU permite la virtualización completa, funcionando como el hipervisor que permitirá la gestión centralizada de recursos de hardware mediante una interfaz de usuario gráfica web.

Estando en esta problemática es que se decidió realizar un recurso de apoyo que facilitara evaluar las ventajas y desventajas de las opciones mencionadas

anteriormente, dando como resultado la tabla 2, donde se consideraron algunos factores para la selección final.

Característica	VMware ESXi (vSphere)	Proxmox VE	Microsoft Hyper-V Server	KVM / QEMU
Licencia	Propietaria	Open Source (AGPL v3)	Propietaria	Open Source (GPL v2)
Base	VMkernel	Debian Linux (KVM + LXC)	Windows Core	Linux Kernel
Costo	Alto	Gratuito	Costo de licencia Windows Server	Gratuito
Curva de Aprendizaje	Media/Alta (Certificaciones)	Baja/Media (Interfaz web intuitiva)	Baja (Conocimiento de Windows)	Alta (Línea de comandos / Archivos de configuración)
Uso Ideal	Grandes Empresas / Estándar Industrial	PyMEs, Universidades, Homelabs	Entornos 100% Microsoft	Proveedores de nube, administradores de sistema avanzados, emulación

Tabla 2. Comparativa entre hipervisores.

Con base en la comparativa técnica realizada, se determinó que Proxmox VE es la solución óptima para la implementación del servidor de virtualización, su principal ventaja en comparación con las otras opciones radica en el hecho de ser gratuito, cuenta con documentación en constante actualización y tiene **interfaz gráfica de usuario web** intuitiva y fácil de usar, destacando que esta última permite a los futuros administradores realizar tareas críticas de creación, eliminación y mantenimiento de máquinas virtuales mediante conocimientos fundamentales de administración de sistemas, eliminando la barrera de un alto dominio en programación o líneas de comando complejas.

Se considero que esta elección asegura el cumplimiento de los objetivos del proyecto, optimizando el aprovechamiento del hardware actual y garantizando la escalabilidad a futuro sin comprometer la estabilidad del servicio principal: la gestión eficiente de los datos provenientes de la estación de referencia.

Por lo tanto, una vez teniendo claro que hipervisor ocupar, es que se procedió a iniciar la implementación de la infraestructura de virtualización.

Preparativos para la instalación del hipervisor

El primer paso para iniciar el despliegue de Proxmox VE fue preparar un medio de instalación de arranque a partir de la **imagen ISO**[5] del sistema operativo del hipervisor, la cual fue posible obtener accediendo a la sección de descargas de su sitio oficial https://www.proxmox.com/en/downloads (tal como se visualiza en la Imagen 6), tomando en cuenta que la imagen ISO tiene un tamaño aproximado de 1.3 GB.

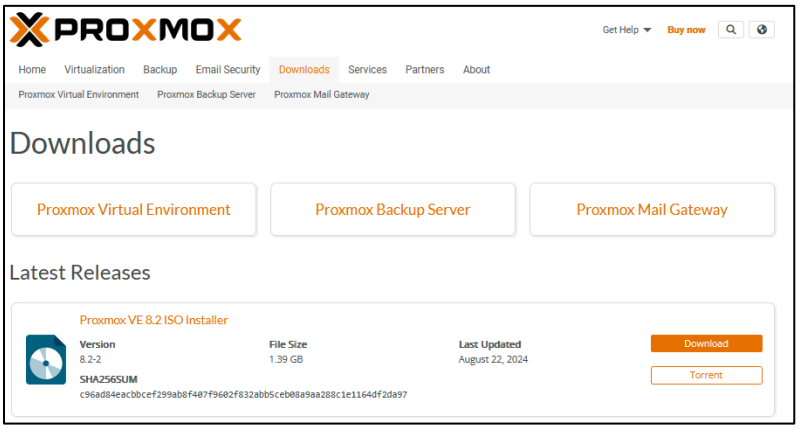


Imagen 6. Sitio web de descarga de Proxmox VE.

Debido a que el desarrollo de este proyecto es para asegurar el envío y recepción continuo de los datos proporcionados por la estación, la estabilidad es un factor clave, por lo que se seleccionó la versión estable más reciente disponible en vez de una en desarrollo, esto aseguró una alta compatibilidad y fiabilidad con diferentes sistemas y componentes, destacando que al momento del desarrollo de este proyecto, la versión estable disponible fue Proxmox VE 8.2, y dependiendo de la fecha de consulta de la sección de descargas de la página oficial, es posible que haya una nueva versión disponible para instalar, ya que Proxmox VE es un sistema operativo que está en constante desarrollo, implementando correcciones y mejoras al sistema para un mejor rendimiento.

[5] **Imagen ISO.** Archivo único que contiene una copia exacta del sistema de ficheros de instalación.

A demás, para la instalación de un sistema operativo no basta con solo tener la imagen ISO de este, es necesario crear un medio de instalación, pudiendo ser un CD/DVD, memoria USB o medios de red.

Considerando una memoria USB como la mejor opción es que se procedió a grabar la imagen ISO en una, creando así un medio de instalación mediante el uso de una herramienta de software llamada Rufus, una herramienta de software de código abierto reconocida por su fiabilidad y eficiencia para crear USB de arranque (medio de instalación) a partir de imágenes de disco (imágenes ISO), la elección de Rufus se fundamenta en su capacidad para ofrecer un control granular sobre la configuración del dispositivo, lo cual es crítico para asegurar la compatibilidad con el hardware del equipo de cómputo.

Rufus permite configurar el medio de instalación de diferentes maneras, pero para el caso de este proyecto, el medio de instalación fue configurado con un esquema de partición GUID (GPT), el cual es un estándar indispensable para sistemas que operan bajo la interfaz de firmware UEFI (Unified Extensible Firmware Interface), a diferencia de MBR, GPT ofrece soporte para volúmenes de almacenamiento superiores a 2 TB y un mayor número de particiones primarias (si se requieren) dentro del almacenamiento del equipo en el cual se instalara el hipervisor.

Aunado a esto, para asegurar la máxima compatibilidad y una correcta detección del medio de instalación por parte del firmware UEFI del equipo anfitrión, se decidió que el sistema de archivos que tendría el medio de instalación fuera FAT32, procurando una ejecución exitosa del entorno de instalación de Proxmox VE (**Imagen 7**).

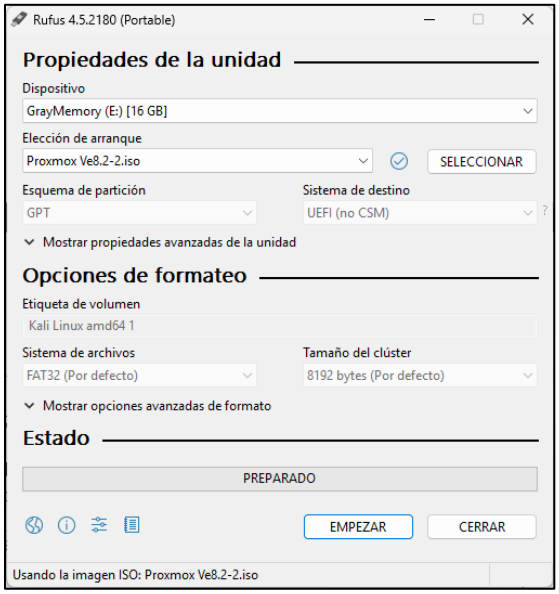


Imagen 7. Configuración de Rufus para crear un medio de instalación.

Instalación y configuración del hipervisor

Una vez que el medio de instalación quedó listo para usarse se procedió a configurar el hardware anfitrión para que este iniciara desde la unidad USB, para lo cual fue necesario interrumpir la secuencia de arranque estándar del equipo ingresando al menú de arranque de la BIOS o cambiando el orden de arranque desde la configuración de esta, ya que la configuración de fábrica de la BIOS normalmente prioriza el arranque del sistema desde los discos duros internos conectados directamente a ella, en este caso, mediante un cable SATA.

Para efectuar dicha interrupción durante la fase inicial de encendido o POST (Power-On-Self-Test) del equipo, se accedió al menú de arranque de la placa base mediante la pulsación de una tecla de función específica, siendo **F9** la tecla de función utilizada para entrar al menú de arranque del equipo de cómputo proporcionado por el departamento.

Desde esta interfaz, se modificó temporalmente la jerarquía de inicio para seleccionar la unidad USB como dispositivo primario, permitiendo el arranque externo sin alterar la configuración permanente en el **firmware**[6] de la placa base.

Al hacer esto, el firmware del sistema cedió el control al cargador de arranque contenido en la memoria USB (medio de instalación), dando como resultado, en lugar de cargar el sistema operativo (si existe), el asistente de instalación de Proxmox VE, cargando en la memoria RAM los archivos necesarios para comenzar el proceso de configuración y particionado del disco principal (**Imagen 8**).

Imagen 8. Interfaz del asistente de instalación de Proxmox VE.

Mediante el uso de este asistente de instalación grafica provisto por el medio de instalación, es como se instaló el sistema operativo Proxmox VE, tomando en cuenta que la elección de este método de instalación fue debido a su naturaleza guiada, la cual simplifica la configuración de parámetros críticos del sistema a través de menús interactivos, y al mismo tiempo, minimiza la probabilidad de errores durante el despliegue inicial.

[6] **Firmware.** Software que proporciona instrucciones de máquina al hardware de un dispositivo.

Para la instalación de Proxmox VE fue necesario configurar los siguientes parámetros, buscando que al finalizar la instalación el sistema operara de manera correcta:

- **Configuración de almacenamiento.** Se seleccionó el disco duro principal del equipo de cómputo como el destino para la instalación del sistema base de Proxmox VE, en esta etapa, el instalador permite definir tanto el dispositivo físico de destino como el esquema de particionado para el sistema de archivos raíz (**root**), para este proyecto, se optó por el sistema de archivos **ext4**, debido a su eficiencia y bajo consumo de recursos de hardware y suficiente para un servidor no clúster, garantizando latencias mínimas en el flujo constante de datos de la estación de referencia, reduciendo la sobrecarga operativa y optimizando el rendimiento general del servidor en entornos de escritura continua.
- **Ajustes de localización.** Se estableció la región, la zona horaria y la distribución del teclado, estos parámetros son fundamentales para asegurar que los registros del sistema (logs), las tareas programadas (cron jobs) y la interacción por consola se ajusten a los estándares locales correctos.
- **Credenciales de administración.** Se definió la contraseña para el usuario *root* (superusuario) al igual que una dirección de correo electrónico para el administrador, donde la contraseña es crucial para el acceso a la interfaz web y la consola, mientras que el correo electrónico es utilizado para registrar y vincular la propiedad a este.
- **Configuración de Red.** Se estableció una configuración de red estática, un requisito indispensable para un entorno de servidor, destacando:
    - **Hostname.** Se asignó un nombre de host dentro del dominio local para identificar unívocamente al servidor dentro de la red.
    - **Dirección IP.** Se asignó una IP estática para garantizar un punto de acceso a la gestión que no cambie con el tiempo.

- **Gateway (puerta de enlace).** Se le asignó la dirección IP del enrutador para permitir la comunicación del servidor con redes externas, incluido el acceso a internet.

- **Servidor DNS.** Se le asignó la dirección del servidor encargado de la resolución de nombres de dominio, esencial para que el servidor pueda localizar otros equipos y servicios en la red, siendo los DNS de la UNAM los utilizados para este proyecto.

Una vez finalizado el proceso de configuración, el sistema se reinicia automáticamente, completando así la instalación del hipervisor en el equipo de cómputo y dando como resultado un servidor de máquinas virtuales, con Proxmox VE totalmente operativo y listo para la fase de gestión y administración de máquinas virtuales y/o contenedores.

Dicha administración se realiza mediante el uso de un navegador web desde cualquier equipo que se encuentre dentro de la misma red local que el servidor, navegando a la dirección IP estática asignada durante la instalación, especificando el puerto asignado y el protocolo https.

Así mismo, el acceso a esta interfaz requiere las credenciales establecidas durante la instalación, es decir el nombre de usuario (root) y la contraseña definida en el paso correspondiente de la instalación (**Imagen 9**).

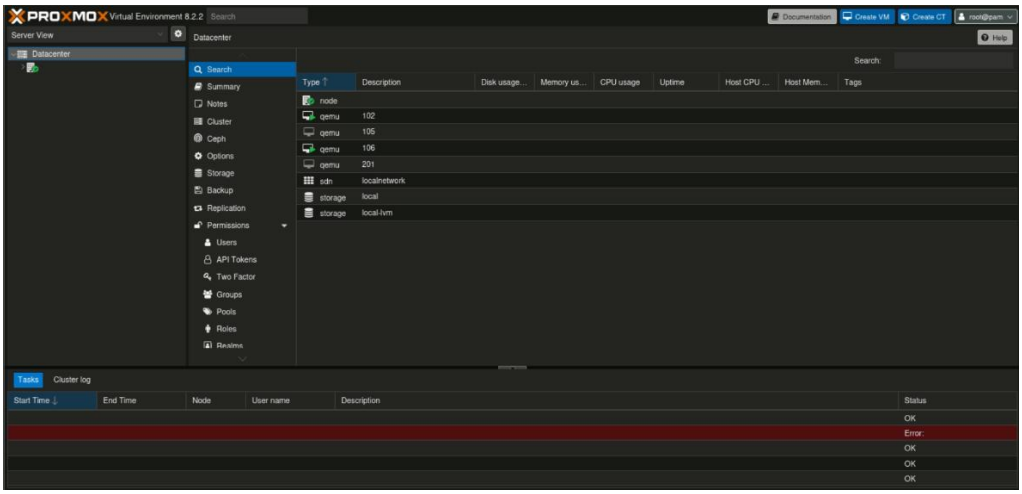


Imagen 9. Interfaz web de Proxmox VE.

Creación de una máquina virtual

La arquitectura del proyecto requiere un nodo (máquina virtual) de control centralizado responsable de la gestión y procesamiento de la información proveniente de la estación de referencia, dentro del cual se deberán de ejecutar un par de aplicaciones administrativas de la estación de referencia (proporcionadas por el fabricante de la estación de referencia), tomando en cuenta que dichas aplicaciones solo pueden ser ejecutadas con Windows.

Para materializar este componente, se determinó que la creación de la máquina virtual dedicada tendría como sistema operativo Windows 8.1 Pro, ya que al momento de la implementación se disponía de una licencia valida proporcionada por el departamento.

La preparación del entorno implico la gestión de dos imágenes ISO fundamentales, las cuales fueron cargadas al repositorio de almacenamiento local de Proxmox para agilizar el proceso de instalación.

1. **ISO de instalación de Windows 8.1.** Contiene los paquetes de instalación del sistema operativo base que servirá como plataforma para las aplicaciones y servicios del proyecto.
2. **ISO de controladores VIrtIO para Windows.** Esta imagen es de vital importancia en entornos de virtualización KVM como Proxmox, proporciona un conjunto de controladores para-virtualizados que permiten al sistema operativo invitado (en este caso Windows 8.1) comunicarse de manera más eficiente con el hipervisor.

La creación de la máquina virtual fue realizada a través del asistente de creación de máquinas virtuales de Proxmox (Imagen 10), ya que este provee un proceso de creación personalizable y avanzado, permitiendo una definición precisa de los recursos de hardware virtual que el hipervisor asignara a la máquina virtual.

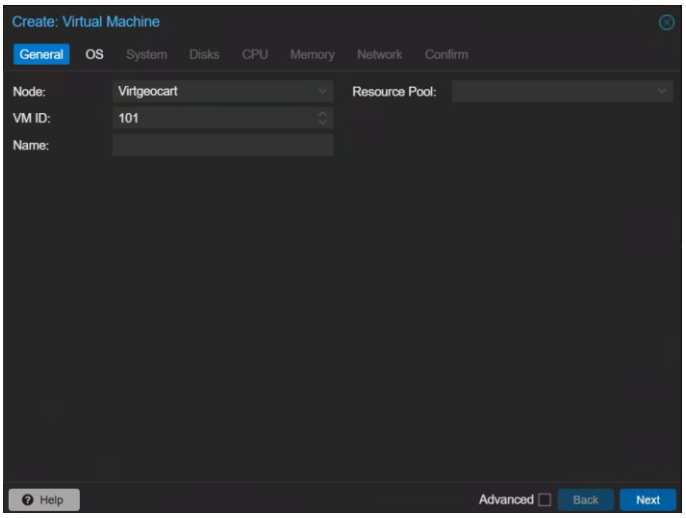


Imagen 10. Asistente para la creación de una máquina virtual en Proxmox.

La correcta asignación de estos recursos (**Imagen 11**) fue un paso crítico, ya que un dimensionamiento inadecuado podría resultar en cuellos de botella de rendimiento o en un consumo ineficiente de los recursos físicos del servidor, el objetivo fue dotar la máquina virtual de la capacidad necesaria para operar de forma óptima, sin sobre aprovisionar y comprometer el desempeño de otras posibles cargas de trabajo en el futuro, donde la configuración de hardware virtual asignada para este nodo de control fue la siguiente:

- **CPU (vCPU).** Se asignaron 4 núcleos virtuales (vCPUs), distribuidos en una topología de 2 sockets con 2 núcleos cada uno, esta configuración multinúcleo facilita el procesamiento en paralelo y mejora la respuesta en cargas de trabajo multihilo, así mismo, se seleccionó el tipo de **CPU x86-64-V2-AES** para asegurar que un conjunto de instrucciones modernas, incluyendo **AES-NI**[7], estén disponible para el sistema operativo alojado en la VM, optimizando la seguridad y rendimiento.
- **Memoria RAM.** Se destinaron 8 GB de memoria RAM, el hipervisor Proxmox gestiona esta memoria de forma dinámica mediante la tecnología de

[7] **AES-NI.** Conjunto de instrucciones para procesadores que acelera el cifrado y descifrado de datos utilizando el algoritmo AES.

ballooning[8] (a través de los drivers VIrtIO), permitiendo que la VM devuelva la memoria no utilizada al host, logrando así un uso más eficiente de los recursos globales del sistema, permitiendo que otras máquinas virtuales (si existen) accedan a estos en caso de ser necesario.

- **Almacenamiento (Disco duro virtual).** Se configuró un disco virtual de 300 GB particionado de la siguiente manera para una gestión de datos estructurada.

- **Partición C: (126 GB).** Reservada exclusivamente para el sistema operativo Windows 8.1 y la instalación de aplicaciones y servicios necesarios para la administración de la estación de referencia y la gestión de los datos recibidos de esta.

- **Partición D: (174 GB).** Esta unidad se configuró como el repositorio principal de datos para centralizar la información proveniente de la estación de referencia, donde la asignación de este volumen responde a un requerimiento técnico del INEGI, garantizar un respaldo histórico de al menos 10 años.

  El cálculo del espacio total se determinó mediante el análisis del flujo de datos promedio, el cual se estableció en 40 MB diarios tras un periodo de observación de 40 días posteriores a la implementación de la fase 3, con esta capacidad de 174 GB, se asegura una ventana de almacenamiento de entre 10 y 12 años, proporcionando un margen de seguridad ante posibles fluctuaciones en el tamaño de los archivos diarios y optimizando la integridad del acervo cartográfico, siendo esta separación de sistema y datos es una práctica recomendada para simplificar las tareas de respaldo y mantenimiento.

- **Red.** Se configuro la interfaz de red virtual en modo Puente (Bridge), ya que esta configuración conecta la VM directamente a la red física, permitiendo

[8] **Ballononing.** Técnica de gestión de memoria que permite al hipervisor recuperar memoria RAM no utilizada de las máquinas virtuales.

que obtenga su propia dirección IP del servidor DHCP o que se le asigne una IP estática, de esta manera, la VM opera como un dispositivo independiente y plenamente accesible en la red local, facilitando la comunicación directa con la estación de referencia y otros dispositivos.

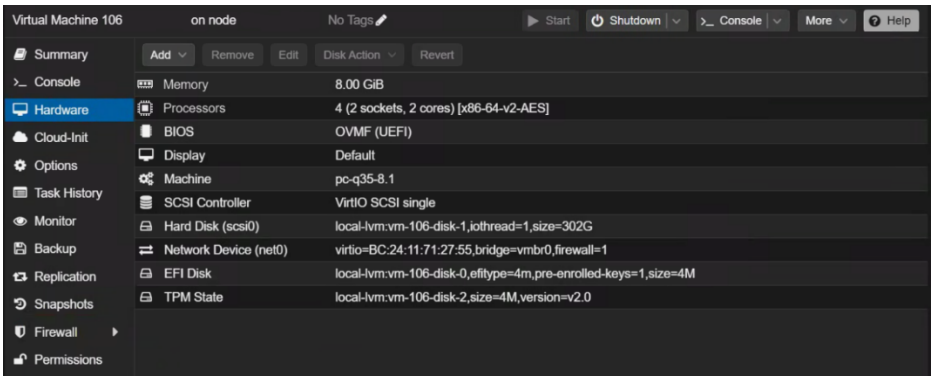


Imagen 11. Recursos asignados a la máquina virtual vistos desde la interfaz web.

Fase 2: Implementación de seguridad perimetral “pfSesnse”.

Dentro del desarrollo de la infraestructura correspondiente al edificio donde se localiza la estación de referencia, existía una vulnerabilidad critica, la cual consistía en que el acceso a los servicios de administración de la estación (tanto la interfaz web como el servidor FTP integrado) se realizaban a través de una dirección IP pública sin mecanismos de autenticación robustos ni cifrado en la conexión. Esto expuso la estación a la red externa, permitiendo que cualquier actor con conocimiento de dicha dirección pudiera acceder, monitorear e incluso manipular las configuraciones y los datos generados, representando un riesgo para la integridad y confidencialidad del proyecto.

Para mitigar esta brecha de seguridad se optó por implementar un firewall perimetral mediante el uso de **pfSense** como una capa de seguridad activa entre la red externa y la estación de referencia.

Configuración de pfSense

pfSense es un sistema operativo de código abierto basado en **FreeBSD**[9], reconocido en el ámbito de la seguridad de redes debido a su flexibilidad, escalabilidad y su amplio conjunto de características de nivel empresarial, para este proyecto, pfSense se despliega en un equipo de cómputo dedicado, el cual se interpuso físicamente entre la conexión a internet (interfaz WAN) y el segmento de red que alberga la estación de referencia (interfaz LAN), lo cual permitió una segmentación efectiva de la red y un control sobre el tráfico que fluye hacia y desde la estación de referencia.

Característica	Descripción
CPU	Intel® Core™2 CPU 6300 @ 1.86 GHz, 2 CPUs x 2 core(s)
Memoria RAM	4 GB
Almacenamiento	512 GB
Interfaz de red para WAN	Broadcom Inc. NetXtreme BCM5754 Gigabit
Interfaz de red para LAN	Accton Technology Corporation, SMC2-1211TX
Sistema operativo	pfSense 2.6.1

Tabla 3. Características del equipo dedicado con pfSense.

Para poder administrar la configuración del firewall pfSense, es necesario tener un equipo cliente de este, es decir, que pertenezca a la LAN del firewall, para así poder acceder a la interfaz web (**Imagen 12**) de pfSense y poder administrar las políticas de seguridad necesarias para el correcto funcionamiento del proyecto.

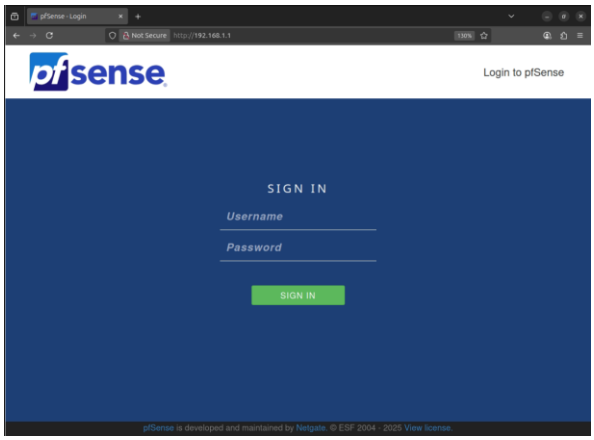


Imagen 12. Interfaz web para administrar pfSense.

[9] **FreeBSD.** Sistema operativo libre, de código abierto tipo Unix

La configuración aplicada se centró en la aplicación del principio de mínimo privilegio, es decir, se denegó el tráfico por defecto, permitiendo únicamente las comunicaciones explícitamente autorizadas, destacando la configuración de:

- **Reglas de firewall para administración remota.** Se crearon las reglas de entrada en la interfaz WAN para permitir el tráfico mediante los protocolos HTTP/HTTPS, restringiendo el acceso solo a la interfaz web de administración de la estación de referencia, esto garantiza que solo el personal de administración pueda acceder a dicha interfaz utilizando las credenciales de usuario requeridas por la propia estación.
- **Redirección de puertos (Port forwarding).** Se configuró una regla NAT para redirigir las solicitudes web (HTTP/HTTPS) que lleguen a la dirección IP publica hacia la dirección IP privada de la estación de referencia en su puerto de administración correspondiente, aplicando la función del firewall como intermediario seguro, evitando que otro tipo de paquetes utilicen el mismo canal de comunicación.
- **Asignación de direcciones IP estáticas.** Se configuró una reserva DHCP dentro de pfSense para asignar de manera persistente la misma dirección IP a la interfaz de red de los equipos clientes de la red interna, es decir, la estación de referencia y el equipo de administración local, asegurando una comunicación predecible y facilitando la creación de reglas de firewall precisas para cada IP.
- **Implementación de acceso mediante VPN.** Se configuró el servicio **OpenVPN** para establecer un túnel seguro y cifrado entre un cliente remoto y la red LAN del firewall a través de una red externa, esto para permitir la administración remota del firewall y la estación CORS de manera segura.

Fase 3: Implementación y configuración de servicios y herramientas administrativas.

Una vez configurada e inicializada, la máquina virtual se convirtió en el núcleo operativo donde se controlaría el flujo de datos del proyecto, ya que su función principal es centralizar la administración de la información generada por la estación de referencia, para esto, se configuraron dos servidores de red críticos, un servidor FTP y un servidor web, buscando que el flujo de los datos funcione como se visualiza en la **Imagen 13**:

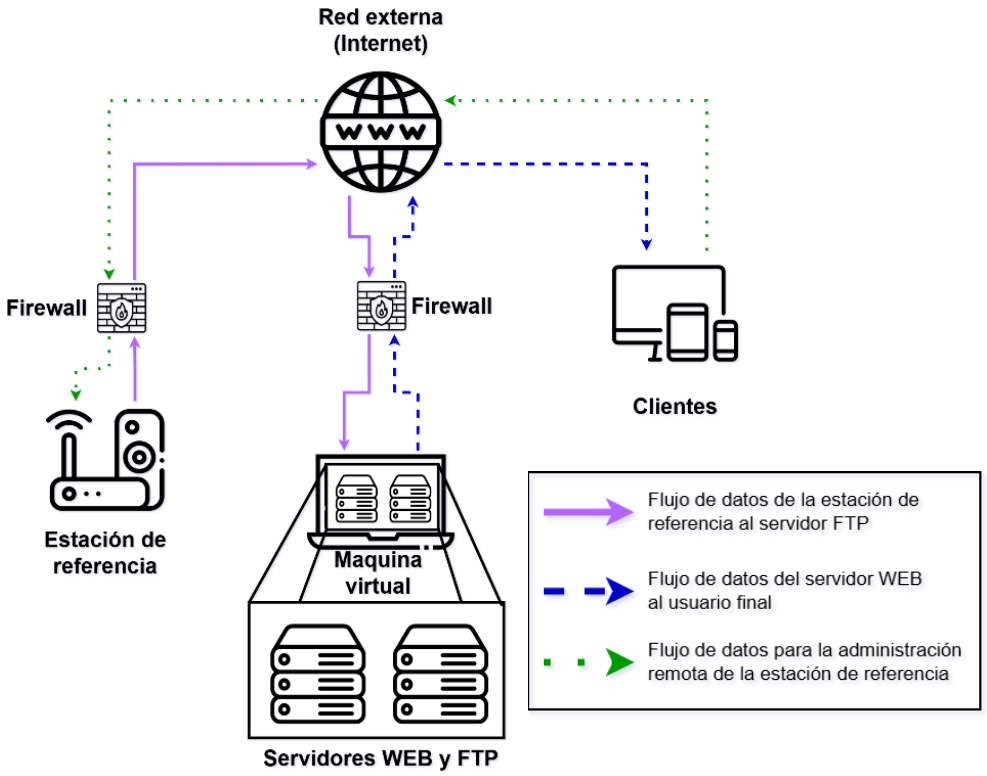


Imagen 13. Flujo de los datos entre la estación de referencia y el usuario final.

El servidor FTP actúa como el punto de ingesta principal, permitiendo que la estación de referencia deposite de forma automatizada y segura los archivos de datos en la partición D: de la máquina virtual, por otro lado, el servidor web entra en función como la plataforma de distribución, ofreciendo una interfaz accesible desde la red local y la red externa para que los usuarios o sistemas autorizados puedan consultar y descargar estos archivos.

Implementación de un servidor FTP

Para gestionar la recepción de archivos provenientes de la estación de referencia, se implementó un servidor de Protocolo de Transferencia de Archivos (FTP) mediante el uso de la plataforma FileZilla Server, una plataforma de código abierto que tiene estabilidad, seguridad y facilidad de administración en sistemas operativos Windows.

Habilitación de puertos y configuración del firewall

Para garantizar la conectividad, fue indispensable configurar tanto el servidor FTP como el firewall del sistema operativo para permitir el tráfico FTP, tomando en cuenta que, para la correcta transferencia de la información a través de este protocolo, se hace uso dos tipos de canales de comunicación:

- **Canal de control.** Este canal se utiliza para la autenticación de usuarios y el envío de comandos dentro del servidor (listar directorios, subir o bajar archivos), normalmente el puerto utilizado para este canal es el puerto 21, por seguridad de la información para este proyecto se ocupó un puerto diferente.
- **Canal de datos (modo pasivo).** En este modo, el servidor indica al cliente a cuáles puertos debe conectarse para transferir los datos, lo cual simplifica enormemente la configuración en redes protegidas por firewalls, por ende, se debe de definir un rango de puertos para la transferencia real de archivos, tomando en cuenta que dichos puertos deben de ser diferentes al puerto de control.

Declarar estos dos canales fue de vital importancia para el correcto funcionamiento del proyecto, dichos canales son por donde la máquina virtual se comunicará con el mundo a través de internet.

Una vez declarados estos puertos dentro de FileZilla Server, fue necesario crear las reglas de entrada en el Firewall de Windows para permitir explícitamente el tráfico en ambos canales, permitiendo el paso de información solamente en el

puerto de control y el rango de puertos de datos declarados, esto con el fin de que el firewall haga el bloqueo de solicitudes de conexiones externas (lo que impediría el correcto funcionamiento del servidor) o ciberataques por medio de puertos que no están en uso real.

Usuarios FTP y asignación de permisos

Siguiendo el principio de mínimo privilegio, para el desarrollo de este proyecto se crearon dos cuentas de usuario con roles y permisos específicos para segmentar el acceso al servidor FTP:

- **Usuario de servicio (estación de referencia).** Cuenta destinada exclusivamente para el uso automatizado por parte de la estación de referencia, donde se le asignó un directorio raíz específico para colocar los archivos de interés, concediéndole únicamente los permisos necesarios para escribir y leer archivos en esa ubicación, restringiendo cualquier otra interacción.
- **Usuario administrador (gestión y administración).** Cuenta con privilegios elevados para la gestión manual de los archivos, este usuario tiene acceso completo al directorio raíz del servidor FTP, permitiendo tareas de supervisión, organización y depuración de los datos recibidos (**Imagen 14**).

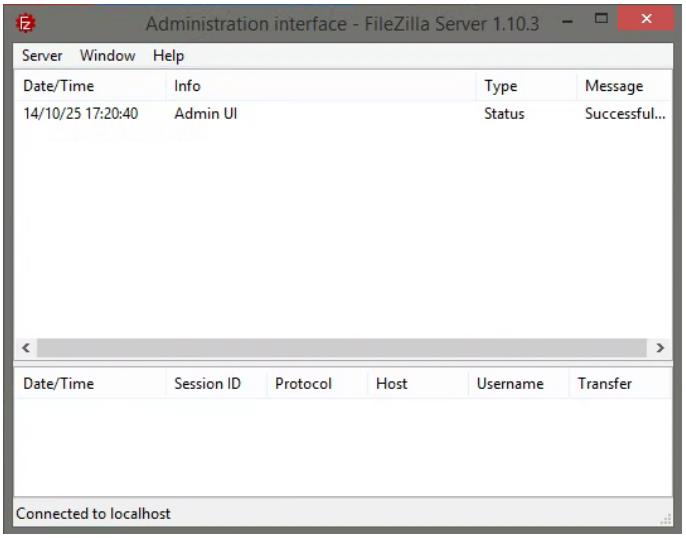


Imagen 14. Interfaz de FileZilla Server.

Actualmente, para garantizar la confidencialidad e integridad en las transferencias de archivos, el estándar recomendado es el uso de FTP explicito sobre TLS (FTPS), este protocolo cifra tanto los comandos como los datos transmitidos, protegiendo eficazmente las credenciales y la información contra ataques de interceptación, no obstante, en la implementación de la estación de referencia se presenta una limitación técnica que impide establecer conexiones cifradas mediante FTPS, ante esta restricción, fue necesario deshabilitar la opción “Forzar FTPS” en FileZilla Server, permitiendo así conexiones mediante el protocolo FTP estándar, el cual no ofrece conexiones cifradas.

Dada esta vulnerabilidad inherente al uso de FTP sin cifrado, fue imprescindible establecer medidas compensatorias para mitigar los riesgos de seguridad, esto se logró configurando FileZilla Server para rechazar indefectiblemente cualquier conexión anónima y permitir exclusivamente el acceso a las dos cuentas de usuario creadas y previamente autenticadas.

Implementación de un servidor web

Para la publicación y descarga de los datos, se implementó un servidor web dentro de la máquina virtual creada, esto con el objetivo de ofrecer un punto de acceso centralizado y sencillo mediante el uso de **Internet Information Services (IIS)**, un servidor web nativo de los sistemas operativos Windows Server y Pro.

El proceso de configuración de este servidor se enfocó en habilitar el acceso público y la descarga de los archivos proporcionados por la estación de referencia de manera fácil y segura, tomando en cuenta la transparencia de la infraestructura creada que provee la información.

Configuración de IIS y creación del sitio web

El primer paso para habilitar el servidor web fue habilitar el rol de “Servidor web (IIS)” a través del panel de control de Windows, específicamente en la sección *Programas y características\Activar o desactivar las características de Windows*, desde este menú se habilitaron las herramientas de administración web, las cuales

incluyen la consola de administración de IIS, scripts y herramientas de administración de IIS y los servicios de administración de IIS.

Mediante el uso de estas herramientas es como se pudo proceder con la configuración de un nuevo sitio web, específicamente desde el Administrador de IIS, donde se agregó un nuevo sitio web, configurándolo de la siguiente manera:

- **Nombre del sitio.** Se asignó un nombre descriptivo para identificar el sitio web dentro de la consola de administración.
- **Ruta de acceso física.** Se vinculó el sitio directamente al directorio donde el servidor FTP deposita los archivos, esta conexión directa entre el servicio FTP y el servicio web es clave para que los datos estén disponibles en tiempo real sin necesidad de procesos de sincronización intermedios.
- **Enlace (Binding).** Se configuró el sitio para escuchar las solicitudes en un puerto especificado dentro de la configuración del sitio, normalmente es el puerto 80 (HTTP), por seguridad de la información para este proyecto se ocupó un puerto diferente (**Imagen 15**).

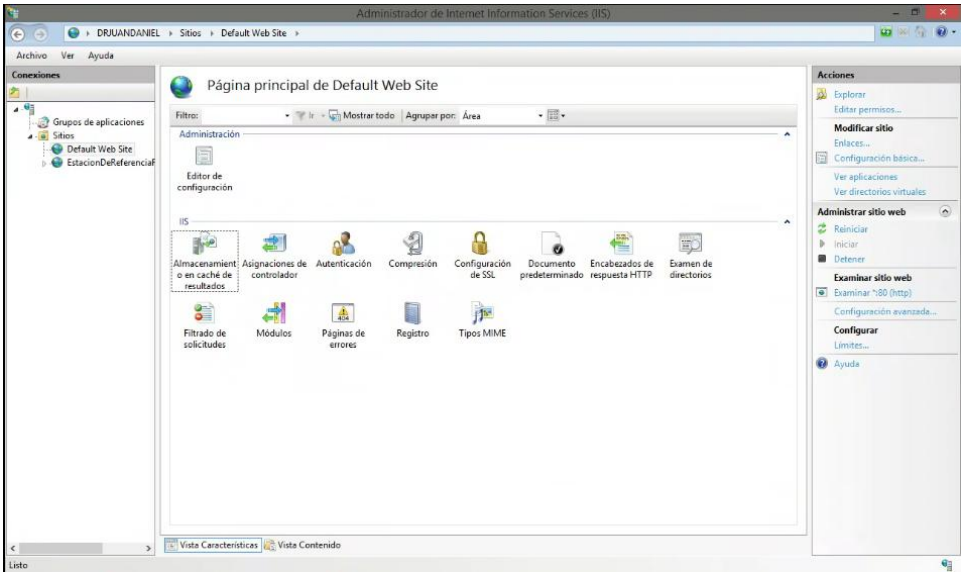


Imagen 15. Interfaz de IIS.

Después de realizar la configuración inicial, y para permitir que los usuarios puedan ver la lista de los archivos disponibles en el directorio, fue necesario realizar

una configuración esencial, la cual es habilitar el examen de directorios dentro del sitio web, por defecto, IIS busca un archivo de índice (como *index.html*) para mostrar el contenido, al no existir tal archivo dentro del directorio de los archivos, hay que habilitar la característica “Examen de directorios”, esto instruye al servidor web para que genere una página HTML que lista el contenido del directorio, permitiendo a los usuarios navegar por las carpetas y hacer clic para descargar los archivos enviados por la estación de referencia.

Como medida de seguridad básica, el archivo de configuración generado al habilitar la característica “Examen de directorios” se configuró como “oculto” desde el explorador de archivos de Windows, esto con el fin de que no aparezca en el listado público del examen de directorios.

Finalmente, fue necesario configurar la conectividad del servidor web desde dentro y fuera de la red local, para esto, nuevamente se creó una regla de entrada dentro del firewall de Windows que permita todo el tráfico entrante en el puerto TCP configurado dentro de la interfaz de IIS para el acceso al sitio web, esta regla es indispensable para que las solicitudes HTTP/HTTPS provenientes de otros equipos en la red local, y las entrantes desde la red externa, puedan llegar al servicio IIS.

Tras reiniciar el sitio web desde la consola de IIS para aplicar todos los cambios, el servidor quedó completamente operativo, cumpliendo su función como la plataforma de distribución de datos del proyecto, accesible tanto para usuarios internos en la red local, como para usuarios externos a través de la dirección IP pública.

Acceso externo a los servidores

La etapa final en el despliegue de la infraestructura correspondiente a la máquina virtual consistió en hacer que los servicios alojados en esta (el servidor FTP, el servidor web y un servidor NTRIP redireccionado de la estación de referencia a la máquina virtual desde la interfaz de configuración de esta) fueran accesibles desde el exterior de la red local.

Dado que la máquina virtual opera con una dirección IP privada dentro de la red de un edificio, esta no es directamente alcanzable desde internet, es decir, la estación de referencia no puede enviar los datos directamente al servidor FTP configurado ni los usuarios pueden acceder al sitio web, debido a esto, fue indispensable el uso del reenvío de puertos (Port Forwarding), para que el router principal de la red del edificio, que posee una dirección IP publica, actúe como traductor y redirija el tráfico entrante a puertos específicos a la dirección IP privada de esta máquina virtual.

Considerando que la administración de la infraestructura de red del edificio recae en un departamento específico, fue necesario realizar una solicitud formal de configuración al personal responsable, donde se detallaron las reglas de reenvío de puertos necesarias para la operatividad correcta del proyecto.

Servidor VPN

Debido a que la administración remota mediante FTP para la estación de referencia quedó inaccesible mediante una conexión externa, se decidió implementar un servidor VPN alojado sobre el firewall implementado, esto previniendo la posibilidad de requerir modificar u obtener datos de la estación de manera masiva sin la necesidad de estar físicamente cerca de la estación.

Para este fin se utilizó la utilidad de openVPN dentro de pfSense, siendo este un protocolo de alta fidelidad para establecer la conexión mediante un túnel cifrado con la red que alberga a la estación de referencia.

Configuración aplicada

Para la creación del servidor VPN fue necesario realizar la creación de una autoridad de certificación y los certificados mediante los cuales se establecerán las conexiones VPN, así como la configuración que esta autoridad certificadora debía tener:

- **Creación de Autoridad de Certificación (CA) y Certificados:** Se generó una infraestructura de clave pública (PKI) interna en pfSense para gestionar

la autenticidad de las conexiones, esto incluye la creación de un certificado raíz (CA) y certificados individuales para el servidor y cada cliente, asegurando que solo los dispositivos con usuarios que tengan certificados firmados y vigentes puedan intentar establecer una sesión.

- **Configuración del Servidor VPN (Túnel y Cifrado):** Se definió el protocolo de transporte (TCP para mayor compatibilidad y fidelidad) y el cifrado de datos mediante el algoritmo **AES-256-GCM**, estableciendo un rango de red virtual (Tunnel Network) independiente de la LAN para el direccionamiento de los clientes conectados, evitando colisiones de IP.
- **Reglas de Firewall en la interfaz WAN (Puerto de Escucha):** Se implementó una regla de entrada específica en la interfaz WAN para permitir el tráfico en el puerto configurado, el cual actúa como la “puerta de entrada” al servicio, permitiendo que el firewall reciba y procese las solicitudes de conexión desde el exterior antes de pasar al proceso de autenticación.
- **Reglas de Firewall en la Interfaz VPN (Control de Acceso):** Se configuraron reglas de filtrado dentro de la interfaz virtual creada por la VPN, que, a diferencia de una red abierta, estas reglas restringen el tráfico de los clientes remotos únicamente a los recursos necesarios (como la IP de administración de la estación de referencia o a la de estación para alcanzar el servicio FTP que provee), bloqueando el acceso al resto de la red interna por defecto.
- **Configuración de Autenticación de Usuarios:** Se estableció un método de autenticación de doble factor o basado en bases de datos locales/LDAP. Esto requiere que el usuario no solo posea el certificado digital, sino también un nombre de usuario y una contraseña válida, añadiendo una capa de seguridad extra.
- **Definición de Rutas y DNS:** Se configuró el envío de rutas específicas hacia los clientes remotos para que estos “conozcan” el camino hacia la red LAN, asimismo, se forzó el uso de resolutores DNS internos para permitir la

resolución de nombres de dominio locales de la infraestructura sin exponerlos a la red pública.

- **Exportación de Paquetes de Configuración:** Se utilizó el módulo de exportación de clientes para generar archivos de configuración unificados (.ovpn), estos paquetes incluyen los certificados, la dirección IP pública del servidor VPN y los parámetros de seguridad necesarios para que el software cliente establezca el túnel de manera automática y segura.

Creación de usuarios VPN

Para garantizar la integridad y el control estricto de los accesos a la infraestructura de la estación, se implementó un modelo de autenticación basado en el **Local User Manager** de pfSense, este componente actúa como la base de datos de identidad centralizada, donde se definen las credenciales y privilegios de cada operador.

- **Directorio de Usuarios Locales:** Se configuró el servidor VPN para que utilice exclusivamente la base de datos interna de pfSense como fuente de autenticación, esto implica que el acceso está restringido únicamente a las cuentas de usuario creadas manualmente por el administrador del sistema, eliminando la posibilidad de accesos mediante cuentas genéricas o externas al entorno controlado.
- **Vinculación por Certificado Digital (Autenticación de Dos Factores Lógica):** Cada usuario registrado en pfSense está vinculado a un certificado de usuario único generado por la Autoridad de Certificación (CA) interna, el sistema requiere una validación dual, donde el cliente debe presentar un certificado válido para autenticarse con las credenciales (usuario y contraseña) almacenadas en la base de datos local, si existe una discrepancia entre el certificado y la cuenta de usuario, el firewall rechaza la conexión de inmediato.
- **Control de Privilegios y Grupos de Seguridad:** Los usuarios no se gestionan de forma aislada, sino que se integran en grupos con permisos específicos, a través del sistema de privilegios de pfSense, se limita que

cuentas con acceso remoto puedan poseer facultades de administración sobre la interfaz web del firewall, a menos que sea estrictamente necesario.

- **Auditoría y Monitoreo de Sesiones:** Al utilizar usuarios locales, pfSense registra en sus logs detallados cada intento de inicio de sesión, asociando la dirección IP de origen, el nombre de usuario y la estampa de tiempo, facilitando la trazabilidad de las acciones realizadas dentro de la red y permitiendo la identificación rápida de posibles intentos de acceso no autorizados o ataques de fuerza bruta.

Culminando de manera exitosa la implementación de la infraestructura para la gestión de los datos generados por la estación, dejándola operativa y permitiendo comenzar la verificación de funcionamiento de los servicios alojados en la máquina virtual, así como el comportamiento del flujo de los datos, quedando a la espera de la aprobación del INEGI para integrar la estación de referencia a la RGNA.

CAPÍTULO 4

VERIFICACIONES FINALES Y ENTREGA

Capítulo 4. Verificaciones finales y entrega.

Para concluir el desarrollo de este proyecto, se realizó una verificación final de la infraestructura implementada, centrándose en la resiliencia de lo virtualizado y la fiabilidad del flujo de los datos de la estación, con el objetivo de garantizar que la transición entre la captura de las señales en la antena y la disponibilidad de los archivos para el usuario final fuera un proceso seguro, reparando y evitando los errores técnicos detectados.

Para comenzar dicha verificación, se revisó la salud del hipervisor implementado (**Imagen 16**), asegurando que la gestión de recursos físicos y virtuales cumpliera con las exigencias de operación que demanda una estación de esta naturaleza (operación continua).

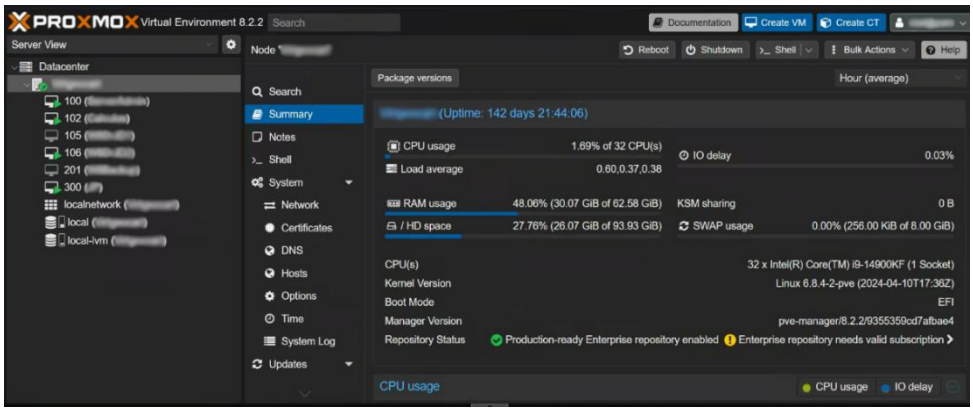


Imagen 16. Recursos utilizados y disponibles del servidor de máquinas virtuales.

Dichos recursos toman en cuenta 4 máquinas virtuales con propósitos diferentes ejecutándose simultáneamente, de la siguiente manera:

- Una máquina virtual encargada de gestionar los datos de este proyecto.
- Una máquina virtual para que el departamento pueda realizar pruebas de software.
- Una máquina virtual para administrar remotamente el servidor de virtualización.
- Una máquina virtual para realizar cálculos y procesamiento de datos.

El despliegue de estos cuatro entornos virtuales que operan de manera simultánea y concurrente permite una segmentación lógica de tareas que optimiza la integridad del sistema, no obstante más allá de la operatividad individual, la estabilidad del ecosistema se hace evidente al analizar las métricas de rendimiento del hipervisor, como se observa en la **Imagen 17**, los niveles de carga en el procesador, el tráfico de red y el consumo de memoria RAM demuestran que las máquinas virtuales conviven de manera armoniosa sin presentar conflictos de recursos o cuellos de botella que comprometan la disponibilidad del servicio.

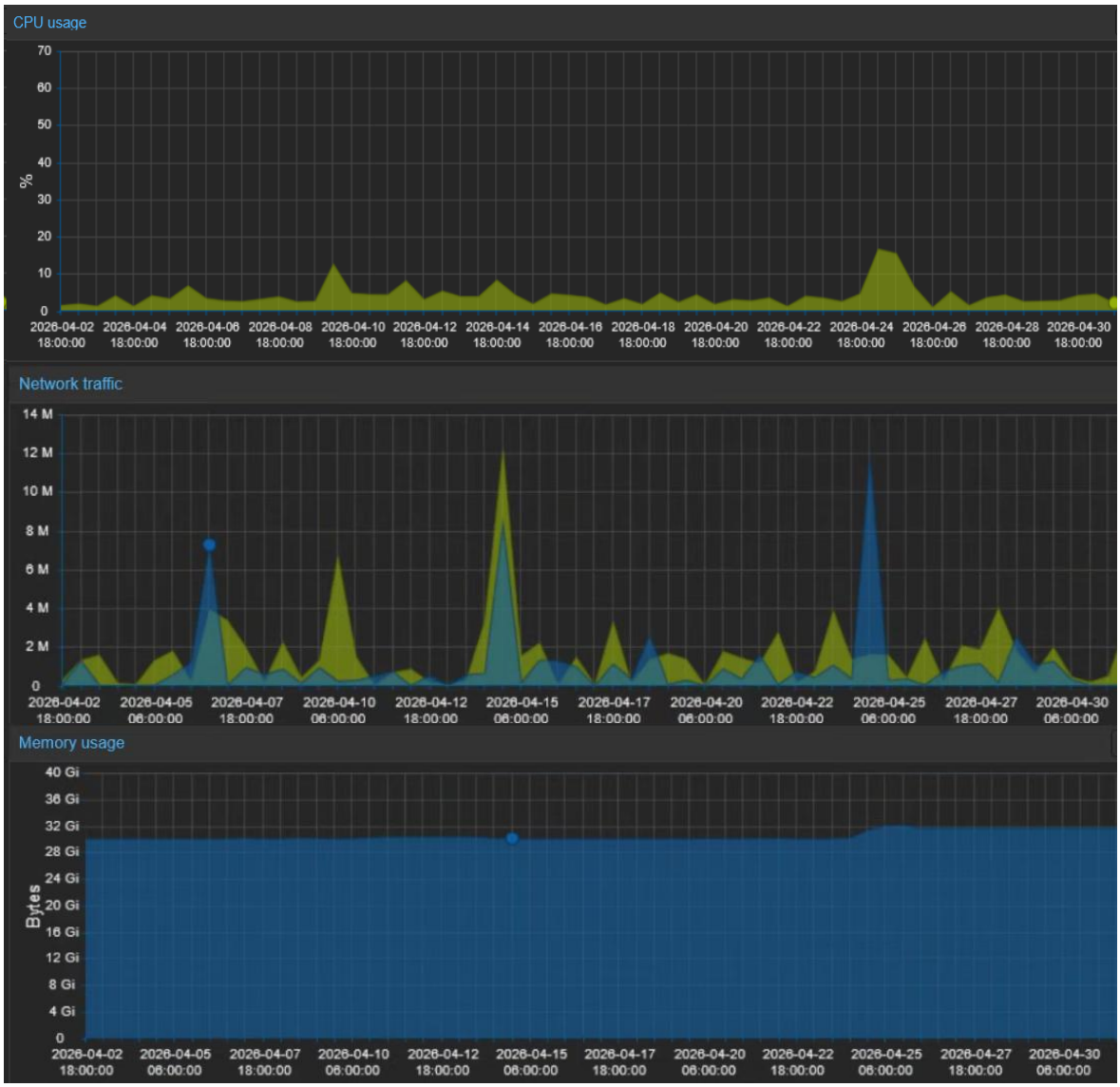


Imagen 17. Vista gráfica del rendimiento del servidor al momento de la ingesta de los datos.

Esta eficiencia en la gestión de recursos físicos no solo validó que la arquitectura actual es apta para el procesamiento de datos de la estación de referencia, sino que también confirma la escalabilidad de la infraestructura al mantener un margen de capacidad excedente que deja al sistema preparado para la implementación de futuras instancias que el Departamento de Geodesia y Cartografía requiera, asegurando que cualquier nuevo proyecto pueda integrarse sin interferir con la estabilidad y el flujo de información ya consolidado.

Una vez culminada la revisión del hipervisor, se procedió con la verificación de la continuidad operativa de la máquina virtual encargada de la gestión de los datos de la estación de referencia (**Imagen 18** e **Imagen 19**).

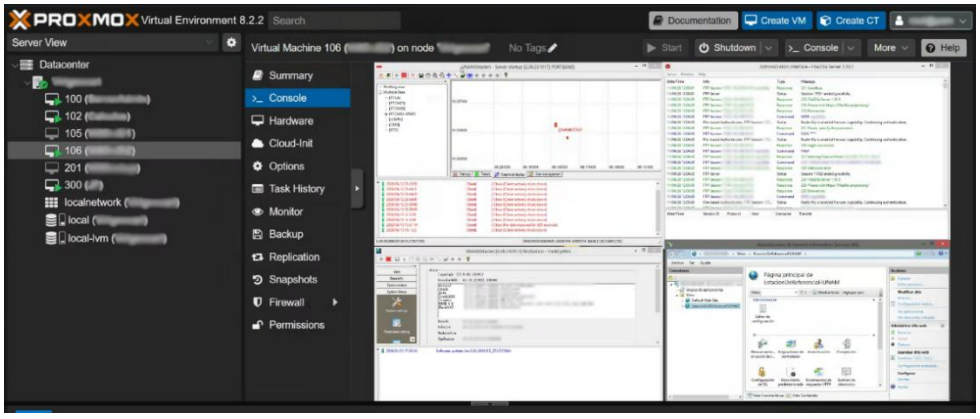


Imagen 18. Máquina virtual del proyecto vista desde la interfaz de Proxmox.

Imagen 19. Gráficas de los recursos (CPU, memoria, disco y red) de la máquina virtual en operación

Validando que esta máquina virtual mantendrá la ejecución de los dos servicios fundamentales para el ciclo de vida de la información proporcionada por la estación de referencia: el servidor FTP y el servidor web. Como se aprecia en la **Imagen 20**, el servidor FTP actúa como la puerta de enlace para la ingesta de datos provenientes de la estación mediante una transferencia de archivos constante que evita en gran medida la pérdida de paquetes.

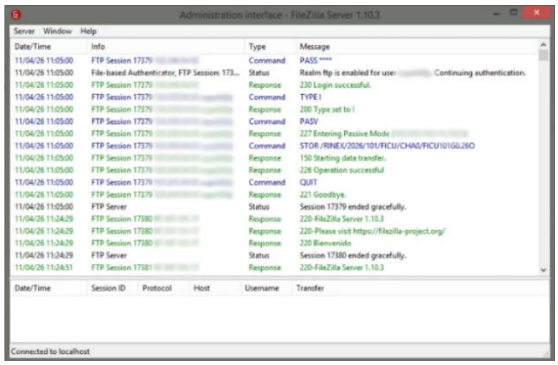


Imagen 20. Servidor FTP encargado de recibir los datos de la estación.

Complementariamente, la configuración del servidor web (visualizada en la **Imagen 21**) gestiona la etapa final del flujo, permitiendo la publicación y consulta de los datos procesados mediante un índice de directorios nativo expuesto por el servidor a través de una interfaz accesible para los usuarios finales.

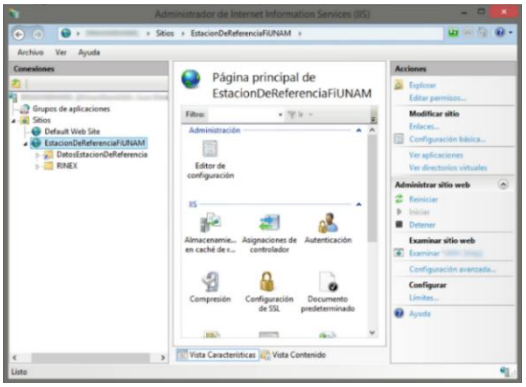


Imagen 21. Servidor web encargado de publicar los datos de la estación.

La sincronía entre ambos servicios garantiza que la infraestructura no solo almacene información, sino que la mantenga disponible para su explotación inmediata, cumpliendo así con los criterios de continuidad y eficiencia establecidos para el proyecto.

Tras haber validado la infraestructura de servicios, se procedió con la verificación de la correcta implementación del redireccionamiento de puertos (Port Forwarding) en el firewall pfSense (**Imagen 22**). Lo que garantizó que el tráfico externo fuera debidamente filtrado y dirigido de manera exclusiva hacia los puertos autorizados.

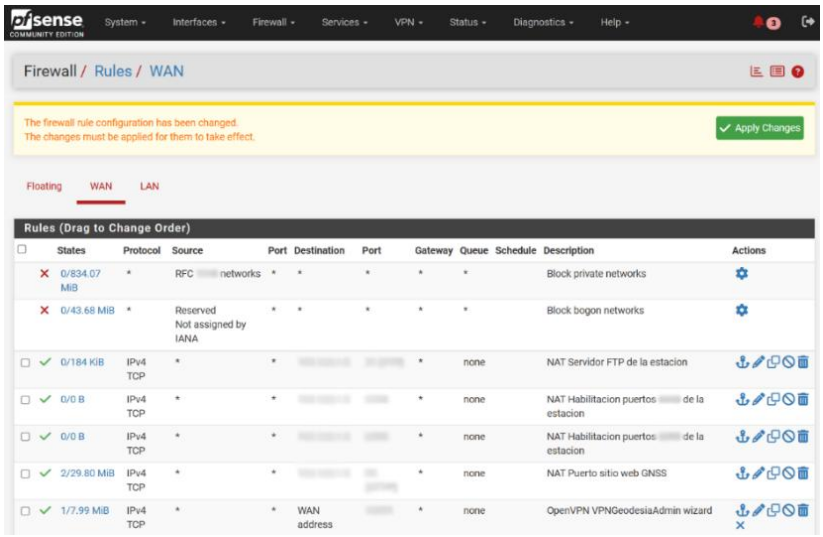


Imagen 22. Redireccionamiento de puertos en pfSense.

Para constatar dicha conectividad y evaluar los puertos de interés, se emplearon herramientas de diagnóstico de red conocidas como tracert, utilizando traceroute y nmap en Linux (**Imagen 23**) y Test-NetConnection en Windows (**Imagen 24**), estas herramientas fueron las que permitieron verificar que existe comunicación entre un nodo externo a la red de la estación de referencia y los servidores virtuales.

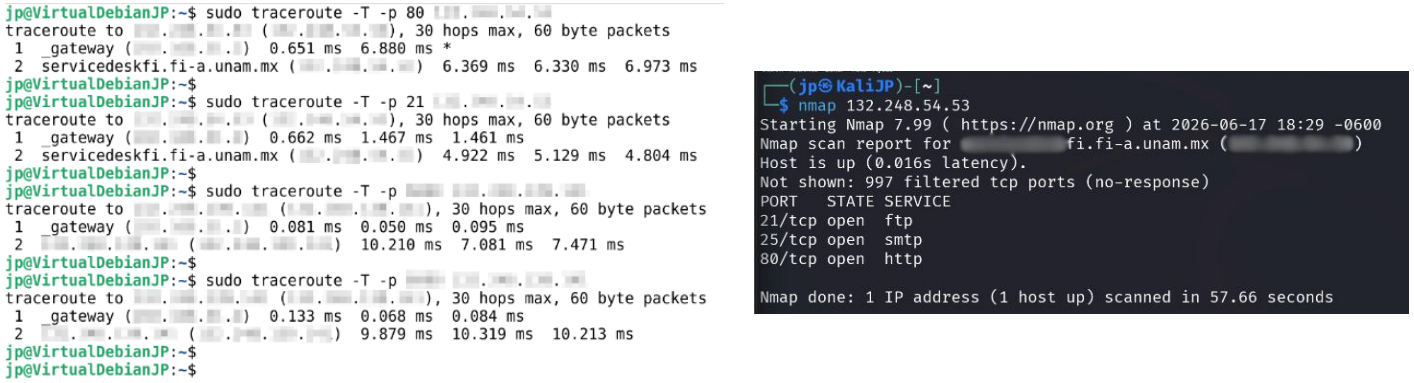


Imagen 23. Pruebas de escucha de los puertos (traceroute) y escaneo de estos.

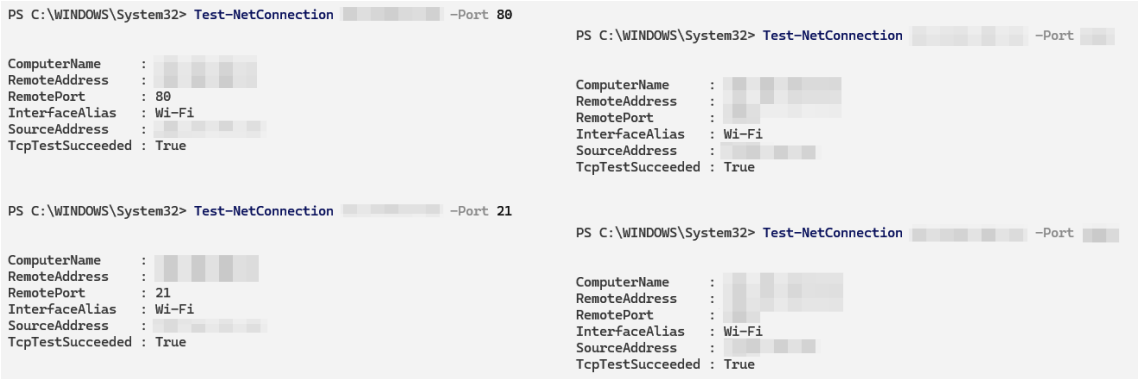


Imagen 24. Prueba de escucha de los puertos (Test-NetConnection).

Asimismo, en la interfaz de pfSense se confirmó el estado activo del servidor VPN destinado a la administración remota de la estación de referencia (**Imagen 25**), un componente crítico, ya que de él depende la gestión a distancia del sistema.

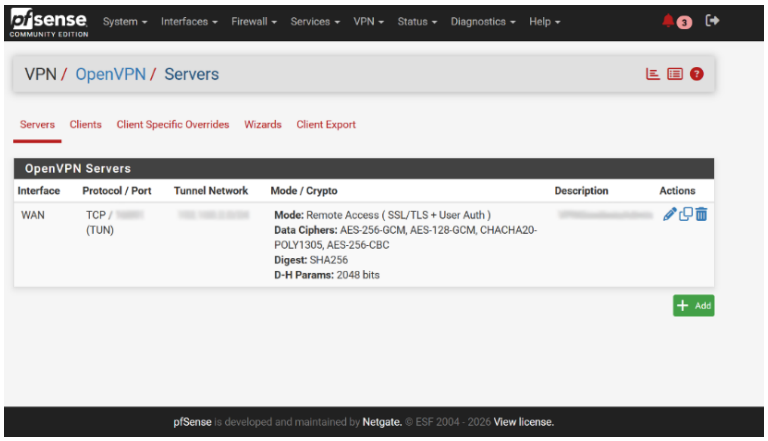


Imagen 25. Servidor VPN para administración remota de la estación.

Finalmente, se llevó a cabo la prueba crítica de acceso desde un cliente externo ubicado fuera del segmento de la red local del servidor web (**Imagen 26**).

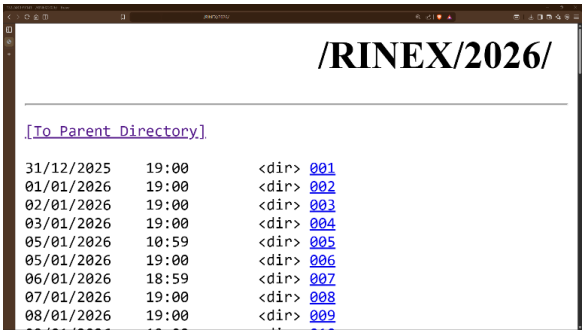


Imagen 26. Visualización del sitio web desde un cliente externo.

Confirmando así que la interoperabilidad buscada desde el inicio del proyecto es funcional. Permitiendo que un usuario externo a las redes (que alojan la estación de referencia, así como los servidores FTP y web) consulte la información de la estación a través de un navegador web de manera fluida, segura y estable.

Es importante destacar que la culminación de esta revisión no representa únicamente el fin de una etapa de desarrollo, sino la consolidación de una infraestructura diseñada para desarrollar múltiples proyectos proporcionando estabilidad y precisión en el manejo de los datos de la estación de referencia.

Concluyendo con la entrega formal del proyecto al Dr. Juan Daniel Castillo Rosas (**Imagen 27**), que simbolizó la transición de una visión técnica hacia una herramienta operativa de alto impacto dentro del departamento, operativa y a la espera de integrarse a la Red Geodésica Nacional Activa, entregando no solo un servidor o un simple servicio, sino una plataforma de alta disponibilidad capaz de sostener el procesamiento de datos críticos sin interrupciones. De este modo, el trabajo se establece como una base sólida para el desarrollo de futuras implementaciones tecnológicas dentro del departamento, las cuales podrán integrarse de manera independiente sin afectar la operatividad de este proyecto titulado "**Infraestructura de virtualización para la gestión de datos de una estación de referencia de operación continua**".

Imagen 27. Entrega formal del proyecto al Dr. Juan Daniel Castillo Rosas.

CONCLUSIONES, GLOSARIO Y REFERENCIAS

Conclusiones

La implementación de esta infraestructura demostró que la virtualización es una herramienta de ingeniería de gran calibre, capaz de transformar recursos físicos limitados en una arquitectura de alta disponibilidad y eficiencia, al desplegar un hipervisor bare-metal, se logró una abstracción de hardware que garantizó el aislamiento total de procesos críticos, haciendo posible que mediante la optimización de un solo equipo de cómputo se pudieran ejecutar de forma concurrente cuatro máquinas virtuales independientes dedicadas a tareas diferenciadas, tales como la gestión de datos, pruebas de software especializado y administración remota, este enfoque no solo resultó en una solución técnicamente superior para el desarrollo de proyectos dentro del Departamento de Geodesia y Cartografía, sino que también permitió economizar recursos monetarios de manera significativa.

La gestión dinámica de recursos aseguró que la máquina virtual de control operara con un rendimiento óptimo sin desperdiciar memoria física, esta capacidad aportó una escalabilidad que antes era inexistente cuando la estación GNSS operaba como un activo aislado, al integrar una zona desmilitarizada (DMZ) y aplicar reglas estrictas de redireccionamiento de puertos mediante pfSense, se logró robustecer la conexión con la estación de referencia, protegiéndola mediante un perímetro de seguridad sólido.

Como se validó en las pruebas finales, esta arquitectura permite que usuarios externos consulten la información de manera segura, garantizando la integridad de los datos en todo momento, para finalmente, cumplir con los rigurosos requerimientos técnicos del INEGI, logrando que la estación se posicione como un nodo activo y fiable de la Red Geodésica Nacional Activa.

Este proyecto no solo resuelve las necesidades actuales de procesamiento y consulta, sino que deja una plataforma preparada para el desarrollo de futuros proyectos, consolidando un ecosistema digital moderno al servicio del Departamento de Geodesia y Cartografía.

Glosario

- **Autoridad de Certificación CA (CA):** Entidad o infraestructura encargada de emitir y gestionar certificados digitales para validar la autenticidad de las conexiones en una red, como en el caso de la Red Privada Virtual (VPN por sus siglas en inglés).
- **CORS (Estación de Referencia de Operación Continua):** Estación de Sistema Global de Navegación por Satélite (GNSS por sus siglas en inglés) que opera de forma permanente para proporcionar datos de posicionamiento geodésico de alta precisión.
- **DHCP (Dynamic Host Configuration Protocol):** Protocolo de red cliente-servidor que asigna dinámicamente direcciones IP y otros parámetros de configuración a los dispositivos conectados a una red.
- **DMZ (Zona Desmilitarizada):** Segmento de red perimetral que funciona como una capa de seguridad adicional entre una red interna confiable y una red externa no segura.
- **Firewall:** Dispositivo o software de seguridad que monitorea y filtra el tráfico de red entrante y saliente basándose en reglas preestablecidas para bloquear accesos no autorizados.
- **Firmware:** Software de bajo nivel que proporciona instrucciones directas al hardware de un dispositivo electrónico para controlar su funcionamiento.
- **FTP (File Transfer Protocol):** Protocolo de la capa de aplicación utilizado para la transferencia de archivos entre un cliente y un servidor a través de una red.
- **GNSS (Global Navigation Satellite System):** Sistemas satelitales que proporcionan posicionamiento y sincronización horaria con cobertura global, como el *Global Positioning System* (Sistema de Posicionamiento Global (GPS por sus siglas en ingles).
- **GPT (GUID Partition Table):** Estándar de la arquitectura informática para el diseño de la tabla de particiones en un dispositivo de almacenamiento físico, el cual reemplaza al Registro de Arranque Maestro (MBR por sus siglas en ingles) tradicional y permite gestionar volúmenes superiores a 2 TB.
- **Herramienta de diagnóstico de red ‘tracert’:** Es una herramienta de diagnóstico de red en la línea de comandos que mapea la ruta exacta que siguen los paquetes de datos desde tu equipo hasta un destino.

- **Hipervisor:** Software que crea una capa de abstracción sobre el hardware físico, permitiendo ejecutar y gestionar múltiples máquinas virtuales de forma independiente.
- **IIS (Internet Information Services):** Servidor web flexible y seguro creado por Microsoft para su uso con la familia Windows NT.
- **Imagen ISO:** Archivo que contiene una copia exacta de un sistema de archivos, utilizado comúnmente para la distribución e instalación de sistemas operativos.
- **ISO/IEC 27002.** Estándar internacional de mejores prácticas que funciona como una guía de referencia para implementar controles de seguridad de la información, ciberseguridad y protección de la privacidad
- **Lightweight Directory Access Protocol (LDPA):** Protocolo de red estándar que permite el acceso y mantenimiento de servicios de directorio distribuido, utilizado comúnmente para la autenticación centralizada de usuarios.
- **Máquina Virtual (VM):** Representación de un sistema mediante software.
- **Modelo Cliente-Servidor:** Arquitectura de red donde los clientes solicitan recursos o servicios que son proporcionados por un servidor central.
- **NAT (Network Address Translation):** Mecanismo de red que permite traducir direcciones IP privadas en una única dirección IP pública, facilitando que múltiples dispositivos de una red local accedan a internet de forma segura.
- **NTRIP (Networked Transport of RTCM via Internet Protocol):** Protocolo estándar diseñado para la transmisión en tiempo real de datos de corrección diferencial GNSS a través de internet.
- **OpenVPN:** Software de código abierto que permite implementar técnicas de red privada virtual (VPN) para crear conexiones seguras punto a punto o de sitio a sitio.
- **pfSense:** Sistema operativo de código abierto utilizado como firewall y enrutador.
- **PKI (Public Key Infrastructure):** Conjunto de componentes de hardware, software, políticas y estándares necesarios para crear, gestionar, distribuir, usar y revocar certificados digitales.

- **Redirección de Puertos (Port Forwarding):** Técnica que redirige solicitudes de comunicación desde una dirección IP y puerto externos hacia un dispositivo o servicio específico dentro de una red privada.
- **RGNA (Red Geodésica Nacional Activa):** Conjunto de estaciones de monitoreo continúo operadas por el INEGI y terceros que constituye el marco oficial para el posicionamiento geodésico en México.
- **TCP:** Protocolo que define las reglas para la transferencia de datos desde el origen hasta el destino, no se envía el mensaje hasta estar seguros de que el destinatario está listo, y se confirma la recepción.
- **Test-NetConnection (Windows):** Herramienta de diagnóstico de red que reemplaza y combina de forma avanzada las funciones de comandos tradicionales de la consola de Windows como ping, tracert y herramientas de escaneo de puertos.
- **Traceroute (Linux):** Herramienta de diagnóstico y monitoreo de redes orientada a la capa de red del modelo OSI con el propósito de determinar la ruta lógica y secuencial que siguen los paquetes de datos a través de una red basada en el Protocolo de Internet (IP) desde un host de origen hasta un nodo de destino.
- **UEFI (Unified Extensible Firmware Interface):** Interfaz de firmware estándar que conecta el sistema operativo con el hardware del equipo, diseñada para reemplazar a la BIOS tradicional ofreciendo mayor seguridad y tiempos de arranque más rápidos.
- **Virtualización:** Crear la representación virtual de un recurso físico.
- **VPN (Virtual Private Network):** Tecnología que crea una conexión cifrada y segura (túnel) sobre una infraestructura de red pública (internet).

Referencias

[1] Tanenbaum, A. S., & Wetherall, D. J. (2012). *Redes de computadoras* (5ª ed) Pearson.

[2] Tanenbaum, A. S., & Van Steen, M. (2008). *Sistemas distribuidos: Principios y paradigmas* (2ª. ed.). Pearson.

[3] Portnoy, M. (2023). *Virtualization Essentials* (3ª. ed.) John Wiley & Sons.

[4] Red Hat Enterprise Linux. (s. f.). *26.5.13. Reenvío de puertos | Guía de diseño del sistema*. Recuperado el 15 de mayo de 2026, de https://docs.redhat.com/es/documentation/red_hat_enterprise_linux/8/html/system_design_guide/port-forwarding_using-and-configuring-firewalld

[5] Instituto Nacional de Estadística y Geografía. (s.f.). *Quiénes somos*. Recuperado el 15 de mayo de 2026, de https://www.inegi.org.mx/inegi/quienes_somos.html

[6] Instituto Nacional de Estadística y Geografía. (s.f.). *Geodesia activa*. Recuperado el 16 de mayo de 2026, de https://www.inegi.org.mx/temas/geodesia_activa/

[7] *Understanding ISO Images: A comprehensive guide | Lenovo US*. (2023, 28 mayo). Recuperado el 17 de mayo de 2026, de https://www.lenovo.com/us/en/glossary/iso-image/

[8] Buxton, O. (2025, 10 diciembre). *¿Qué es el firmware y cómo funciona?* ¿Qué Es el Firmware y Cómo Funciona? Recuperado el 17 de mayo de 2026, de https://www.avg.com/es/signal/firmware

[9] Robinharwood. (s. f.). *Test-NetConnection (NetTCPIP)*. Microsoft Learn. Recuperado el 18 de mayo de 2026, de https://learn.microsoft.com/en-us/powershell/module/nettcpip/test-netconnection?view=windowsserver2025-ps

[10] Debian Packages. (s. f.). *Package: traceroute.* Recuperado el 18 de mayo de 2026, de *https://packages.debian.org/es/sid/traceroute*

[11] Kaushika-Msft. (s. f.). *Introducción a los servicios y requisitos de puerto de red para Windows - Windows Server*. Microsoft Learn. Recuperado el 18 de mayo de 2026, de https://learn.microsoft.com/es-es/troubleshoot/windows-server/networking/service-overview-and-network-port-requirements