UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

Modelo de almacenamiento distribuido seguro mediante mini NAS y conexión VPN para entornos de protección información crítica

AUTOR

CARVAJAL NUÑEZ JAMES JOSUE

EXAMEN COMPLEXIVO

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

Lsi. DANIEL QUIRUMBAY Y. MSIA

Santa Elena, Ecuador

Año 2025

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino. Mgt.
DIRECTOR DE LA CARRERA

Lsi. Daniel Quirumbay Yagual. Msia.
TUTOR

Ing. Iván Coronel Suárez. Mgt.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez. Mgti.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Modelo de almacenamiento distribuido seguro mediante mini NAS y conexión VPN para entornos de protección información crítica, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 14 días del mes de Noviembre del año 2025

TUTOR

Daniel Ivan Quirumbay Yagual
Time Stamping Security Data

Lsi. DANIEL QUIRUMBAY, MSIA

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **CARVAJAL NUÑEZ JAMES JOSUE**

El trabajo de Titulación, Modelo de almacenamiento distribuido seguro mediante mini NAS y conexión VPN para entornos de protección información crítica previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 14 días del mes de Noviembre del año 2025

EL AUTOR

James Carvajal

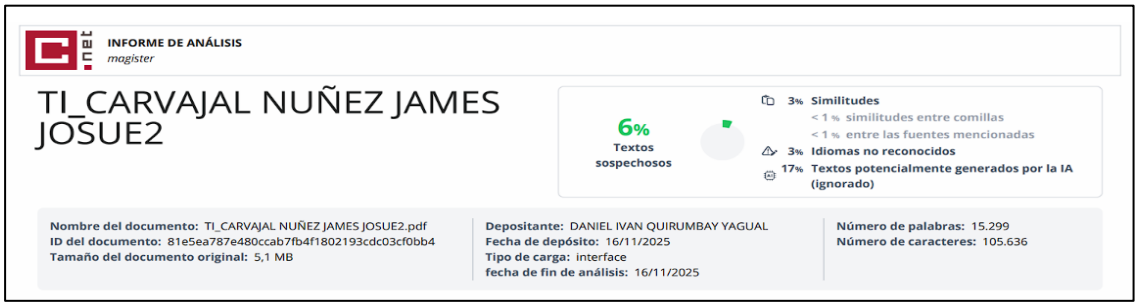
JAMES JOSUE CARVAJAL NUÑEZ

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado, presentado por el estudiante, CARVAJAL NUÑEZ JAMES JOSUE fue enviado al Sistema Anti plagio, presentando un porcentaje de similitud correspondiente al 6%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



INFORME DE ANÁLISIS
magister

TI_CARVAJAL NUÑEZ JAMES JOSUE2

6% Textos sospechosos

3% Similitudes
< 1 % similitudes entre comillas
< 1 % entre las fuentes mencionadas
3% Idiomas no reconocidos
17% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: TI_CARVAJAL NUÑEZ JAMES JOSUE2.pdf
ID del documento: 81e5ea787e480ccab7fb4f1802193cdc03cf0bb4
Tamaño del documento original: 5,1 MB

Depositante: DANIEL IVAN QUIRUMBAY YAGUAL
Fecha de depósito: 16/11/2025
Tipo de carga: interface
fecha de fin de análisis: 16/11/2025

Número de palabras: 15.299
Número de caracteres: 105.636

TUTOR

Daniel Ivan Quirumbay Yagual
Time Stamping Security Data

Lsi. DANIEL QUIRUMBAY, MSIA

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **CARVAJAL NUÑEZ JAMES JOSUE**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales del presente trabajo de titulación con fines de difusión pública, además apruebo la reproducción dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 14 días del mes de Noviembre del año 2025

EL AUTOR

James Carvajal

CARVAJAL NUÑEZ JAMES JOSUE

AGRADECIMIENTO

Agradezco profundamente a Dios por ser mi guía constante que me dio fortaleza en momentos difíciles e iluminó mi camino en este proceso académico. A mi familia por su amor incondicional, su apoyo incondicional y por ser mi columna vertebral en cada etapa de mi vida. Gracias por creer en mí cuando dudaba, por sus palabras de aliento y por estar siempre ahí. A mis amigos y colegas de la Universidad Estatal Península de Santa Elena quienes compartieron conmigo innumerables experiencias, desafíos y lecciones. Su compañía y cooperación fueron fundamentales para la consecución de este objetivo. Finalmente, me gustaría agradecer a todos aquellos que han contribuido de una forma u otra a la realización de este proyecto. Cada gesto, palabra y lección ha dejado una huella imborrable en mi formación profesional y personal.

JAMES JOSUE CARVAJAL NUÑEZ

DEDICATORIA

Dedico este logro de todo corazón a mi padre y a mi abuelo, quienes ya no están físicamente conmigo, pero cuya memoria y enseñanzas han sido una fuente constante de inspiración. Ojalá estuvieran ahí para compartir este momento y creo que están orgullosos de mí desde el cielo. A mi madre por su incansable esfuerzo, sacrificio y amor incondicional. Gracias por ser mi mayor apoyo, por nunca rendirme y siempre darme la fuerza para seguir adelante. Este triunfo también es tuyo. A todos los que han creído en mí, esta dedicatoria es un pequeño reflejo del agradecimiento que llevo en el alma.

JAMES JOSUE CARVAJAL NUÑEZ

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INDICE DE ANEXOS

RESUMEN

La falta de un sistema centralizado para proteger la información crítica en entornos académicos con pocos recursos puede provocar pérdida de datos y un rendimiento deficiente. En el laboratorio cibernético de la Universidad Estatal de la Península de Santa Elena, esta deficiencia se hizo evidente debido a los métodos tradicionales e inseguros para compartir archivos. El objetivo del proyecto es lanzar un sistema de almacenamiento compartido seguro a través de un mini-NAS (Terramaster F2-212), complementado con una conexión VPN para garantizar un acceso remoto seguro y una mejor gestión de los activos digitales. El enfoque Cisco PPDIOO se implementa en cuatro fases: preparación, planificación, implementación y operaciones. Se realizo análisis de infraestructura, encuestas a estudiantes, se configuro NAS con RAID 1 se estableció usuarios y permisos, se aplicó VPN (ZeroTier/OpenVPN) y sincronización con Google Drive mediante Google Apps Script y CloudSync. Los resultados muestran que la información está centralizada, el acceso remoto es seguro, existen copias de seguridad automáticas y el acceso a los roles está controlado. El sistema demostró un rendimiento superior al 90 %, baja latencia (26 ms) y alta disponibilidad, lo que garantiza estabilidad, tolerancia a fallas y administración sin necesidad de presencia física.

PALABRAS CLAVES: ALMACENAMIENTO CONECTADO A LA RED (NAS), DISCOS DUROS, RED VIRTUAL PRIVADA (VPN), LABORATORIO CONTROLADO.

ABSTRACT

The lack of a centralized system to protect critical information in resource-poor academic environments can lead to data loss and poor performance. In the cyber lab at St. Helena Peninsula State University, this shortcoming became apparent due to traditional and insecure file-sharing methods. The goal of the project is to launch a secure shared storage system through a mini-NAS (Terramaster F2-212), complemented by a VPN connection to ensure secure remote access and better management of digital assets. The Cisco PPDIOO approach is implemented in four phases: preparation, planning, implementation, and operations. Infrastructure analysis, student surveys, NAS with RAID 1 were configured, users and permissions were set, VPN (ZeroTier/OpenVPN) was applied, and synchronization with Google Drive was applied using Google Apps Script and CloudSync. The results show that information is centralized, remote access is secure, there are automatic backups, and access to roles is controlled. The system demonstrated over 90% performance, low latency (26ms), and high availability, ensuring stability, fault tolerance, and management without the need for physical presence.

KEYWORDS: NETWORK-ATTACHED STORAGE (NAS), HARD DRIVES, VIRTUAL PRIVATE NETWORK (VPN), CONTROLLED LABORATORY.

INTRODUCCIÓN

En este argumento se continua la innovación, las soluciones de almacenamiento tradicionales como los dispositivos físicos portátiles (discos duros externos, unidades flash USB, CD) han comenzado a mostrar limitaciones debido a las crecientes demandas de seguridad, disponibilidad, escalabilidad y acceso remoto.

Esta transformación también ha logrado un área de educación en la que las universidades y los centros de capacitación técnica enfrentan el desafío de adaptarse a nuevas formas de trabajo, enseñanza y administración de conocimiento. En este sistema panorámico de almacenamiento de redes (NAS), ha sido importante como soluciones efectivas para centralizar, proteger y organizar información digital.

Muchos entornos académicos, especialmente aquellos con recursos limitados o que carecen de una estrategia formal de transformación digital, todavía utilizan métodos de almacenamiento de datos tradicionales y menos seguros que exponen la información debido a la pérdida de privilegios, el almacenamiento de archivos que requiere un uso intensivo de recursos y fallas de seguridad.

La Universidad Estatal de Santa Elena ha contribuido al uso de modernas tecnologías en el proceso de aprendizaje a través de su sistema de telecomunicaciones y su personal docente. Sin embargo, los laboratorios en red enfrentan desafíos únicos sin un sistema de almacenamiento centralizado. Actualmente, la información creada por profesores y estudiantes, como prácticas de laboratorio, configuraciones, documentos técnicos y proyectos académicos, se distribuye localmente en unidades individuales o dispositivos externos sin políticas de seguridad ni soporte automatizado, lo que limita la disponibilidad y afecta la integridad de la información.

Para esta necesidad, se plantea usar un Mini NAS (Terrramaster F2-21) con una conexión remota utilizando VPN. El objetivo de esta propuesta es garantizar una infraestructura tecnológica eficiente, segura y de bajo costo, lo que permite el almacenamiento de datos centralizado, facilitando el trabajo de cooperación, optimizar el acceso remoto a la información y promover el uso responsable de los activos digitales institucionales. El sistema se implementará de acuerdo con la metodología Cisco PPDIO reconocida por su enfoque estructurado para los proyectos de redes y tecnología que tienen un desarrollo común en cinco etapas: preparar, planificar, implementar, guiar y optimizar.

CAPITULO I

1. ANTECEDENTES

Con la aparición de las TIC (Tecnologías de Información y Comunicación) se generan oportunidades que facilitan el progreso hacia una gestión pública más plural, dinámica y abierta, en la vida del ser humano posmoderno, las tecnologías digitales han superado los problemas relacionados con el espacio, el tiempo y el almacenamiento de información. Cuando estas herramientas se utilizan correctamente en las instituciones, promueven el surgimiento de nuevas prestaciones, estas son: la conectividad entre los prestadores y los beneficiarios, la accesibilidad y la portabilidad sin importar dónde se encuentre el interesado, la localización geográfica para facilitar la ubicación hacia o desde cualquier destino, la transparencia constante y sistemática y el almacenamiento virtual ilimitado que permite construir una visión realista de los hechos [1].

Las TIC hacen posible que se implementen estrategias educativas y comunicativas para crear nuevas maneras de aprender y enseñar, utilizando enfoques de gestión más sofisticados en un mundo cada vez más competitivo y exigente, donde la improvisación no tiene lugar, las tecnologías de la información y la comunicación son el conjunto de procesos y productos que resultan de las herramientas modernas (hardware y software), los medios informativos y los canales de comunicación asociados con el almacenamiento, procesamiento y transmisión digitalizada de datos [2].

La expansión de las TIC en todos los ámbitos de nuestra sociedad se ha producido a gran velocidad y es un proceso que continua, ya que van apareciendo sin cesar nuevos elementos tecnológicos, a pesar de estas magníficas credenciales que hacen de las TIC instrumentos altamente útiles para cualquier centro, existen diversas circunstancias que dificultan su más amplia difusión entre todas las actividades y capas sociales, que hacen que el uso de las TIC no funcione correctamente, sino también la capacitación en el uso adecuado de las TIC, reduciendo así las desigualdades tecnológicas, ellas han contribuido a acentuar cada día más la brecha digital, que está basada en aspectos de acceso pero también en los relacionados con el uso de las TIC [3].

Los avances en las Tecnologías de la Información y la Comunicación (TIC) y la existente interacción entre la educación superior ecuatoriana es el principal objetivo del presente artículo. Se estudiará el aporte de las TIC al campo educativo. Las TIC en la educación superior toman un aspecto tecnológico e investigativo que ayuda a formar profesionales

en cada rama de especialidad, con una visión amplia e íntegra para estar acorde con los cambios tecnológicos que se produce a consecuencia de la globalización [4].

La tecnología digital, como un motor en constante funcionamiento, avanza. La academia, al ser la principal fuente de conocimiento, debe ir a la par de estos cambios mediante la creación de espacios y el fomento de investigaciones que le posibiliten crear propuestas que satisfagan lo que se requiere para la gestión empresarial y estén alineadas con los tiempos actuales [5]. Las tecnologías de información juegan un papel importante, en especial cuando se trata de manejar los datos de forma adecuada y proporcionar la información correcta en el momento que se requiere, hecho que permite a todo tipo de organización alcanzar ventajas competitivas y sobrevivir a la competencia [6].

La Universidad Estatal Península de Santa Elena tiene como objetivo formar profesionales íntegros, creativos y con mentalidad emprendedora en su Facultad de Telecomunicaciones, que estén comprometidos con la ética, la solidaridad y el progreso sostenible del país. Su objetivo es promover la participación de los ciudadanos y ayudar a robustecer las instituciones democráticas mediante el uso de la innovación tecnológica y el conocimiento [7]. En esta institución se sitúa la carrera de tecnología de la Información (TICS) .A través de un enfoque práctico y actualizado, se busca dotar a los estudiantes de competencias sólidas que les permitan responder eficazmente a las demandas del entorno digital y contribuir al desarrollo tecnológico y productivo de la región y del país, la carrera buscan crear profesionales capaces de liderar proyectos innovadores que impulsen la transformación digital y fortalezcan la competitividad tecnológica del país

La tesis hecha por MORENO PAICO CRISTIAN habla sobre la IMPLEMENTACIÓN DE UN SERVIDOR NAS NETWORK ATTACHED STORAGE PARA EL ÁREA DE PROYECTOS DE LA EMPRESA VGM CONSTRUCCIONES S.A.C - HUARAZ; 2020, se concluye que la empresa tiene falencias con la forma de cómo está organizando, compartiendo y almacenando la información, porque se evidencia que los procesos que tienen implementados actualmente dificulta el desarrollo de las actividades de los trabajadores, lo cual, junto con la falta de un servicio de almacenamiento como un servidor NAS para el almacenamiento [8].En el caso específico de la empresa VGM Construcciones S.A.C., se identificaron falencias significativas en la forma de organizar, compartir y almacenar los datos, lo que repercute directamente en la eficiencia operativa

de los trabajadores. Por lo tanto, se propone la puesta en marcha de un servidor NAS como una opción eficaz para centralizar los datos, optimizar la cooperación entre áreas y asegurar que los datos estén disponibles y sean seguros.

En tanto a la Tesis de PROPUESTA DE UN SISTEMA DE ALMACENAMIENTO NAS PARA EL CONTROL DE LA INFORMACION EN EL ÁREA ADMINISTRATIVA DE LA UNIVERSIDAD PERUANA DE CIENCIAS E INFORMATICA La tesis propone un sistema NAS para mejorar el control de información en el área administrativa de la Universidad Peruana de Ciencias e Informática, se identificaron problemas en la administración, manejo y seguridad de archivos, los respaldos se realizaban manualmente con un disco duro externo conectado al servidor [9]. Esta práctica era ineficaz y tenía un impacto negativo en el desempeño de la institución. Sin embargo, ahora se muestra una buena satisfacción con los resultados obtenidos, se determinó que implementar un Sistema de Almacenamiento NAS mejoraría la gestión de información en el área administrativa de la Universidad Peruana de Ciencias e Informática.

En el tema de titulación de DESARROLLO DE UN SERVIDOR NAS CON RASPBERRY PI PARA ALMACENAMIENTO Y RESPALDO DE DATOS EN LA EMPRESA SU ECONOMÍA, se habla del desconocimiento y la complejidad en el respaldo de archivos administrativos o multimedia, y la falta de hardware para su almacenamiento en un servidor adecuado, suscitan falencias en la construcción del mueble y producen pérdidas de tiempo en las búsquedas de datos solicitados por los trabajadores, para elaborar los proyectos diseñados [10]. La propuesta busca implementar una solución económica y funcional mediante un servidor NAS basado en Raspberry Pi, optimizando así el almacenamiento y acceso a la información.

1.1. DESCRIPCION DEL PROYECTO

En el laboratorio de REDES de la Universidad Estatal Península de Santa Elena (UPSE), se detectó el requerimiento de optimizar la administración y salvaguarda de la información producida por profesores y alumnos. En la actualidad, no existe un sistema de almacenamiento centralizado, lo que complica el almacenamiento seguro y el acceso eficaz a los datos.

Para la implementación de esta propuesta, se utilizará el modelo Cisco PPDIOO [11], ajustado a las demandas del contexto académico. Las etapas que se realizarán incluyen lo siguiente:

Fase I: Preparar.

En esta etapa, se recopila información detallada sobre el estado actual del laboratorio de redes, que incluye: inventario de hardware, infraestructura de red y almacenamiento, se analizan las tecnologías actuales para determinar su idoneidad para la solución mini NAS propuesta, se tienen en cuenta los requisitos del usuario y los factores del entorno de trabajo potencialmente importantes. Esta evaluación proporciona una base técnica sólida para el desarrollo del sistema y toda la información recopilada se registrará y utilizará durante la fase de planificación.

- Se realiza una encuesta a los estudiantes que cruzan las materias dentro del laboratorio de REDES para identificar necesidades, limitaciones y expectativas relacionadas con el almacenamiento de datos.
- Se lleva a cabo un análisis de compatibilidad tecnológica entre la infraestructura actual y los requerimientos del sistema NAS.
- Se detectan las limitaciones operativas, los riesgos y las condiciones institucionales que tienen el potencial de perjudicar la puesta en marcha del sistema.

Fase II: Planificar.

En esta etapa, el sistema NAS está configurado. Con base en los requisitos previamente definidos, se establecen los parámetros de configuración y segmentación necesarios del servidor mini-NAS, se definen estrategias de seguridad y se organizan procesos de respaldo automático. De manera similar, se crea un sistema VPN de acceso remoto para proporcionar conexiones seguras desde ubicaciones remotas.

- Se espera conectar el sistema NAS a la red del laboratorio, teniendo en cuenta tanto la topología como las necesidades de conectividad existentes.
- Garantizar las políticas de seguridad necesarias para proteger la información, incluido el cifrado, el acceso y la copia de seguridad automática.
- El esquema de acceso remoto se implementa mediante una VPN, lo que garantiza conexiones seguras y controladas desde ubicaciones externas.

Fase III: Implementar.

Luego, se instalan servicios básicos como direcciones IP estáticas, acceso a carpetas compartidas y protocolos de copia de seguridad automática. Los perfiles de usuario se

crean para proporcionar permisos individuales según el nivel de acceso requerido. Además, el acceso remoto es posible a través de VPN, lo que garantiza conexiones seguras desde ubicaciones remotas. Finalmente, si implementa una función de evaluación para confirmar que el sistema está funcionando correctamente y documentar los objetivos anteriores, es fundamental establecer un sistema de monitoreo continuo y aplicar mantenimiento preventivo, con el objetivo de anticiparse ante posibles fallos, garantizar la estabilidad operativa y optimizar el rendimiento del sistema a largo plazo.

- Mini NAS se instala por etapas, se integra físicamente con el entorno del laboratorio y se conecta a la red corporativa.
- Configurar usuarios y crear carpetas compartidas, descentralizar según el nivel de acceso requerido.
- El acceso remoto VPN está habilitado, lo que garantiza conexiones seguras desde ubicaciones externas.
- Están disponibles los servicios de red necesarios, como direcciones IP estáticas, copias de seguridad y protocolos para compartir.

Fase IV: Operar.

En esta fase el mini NAS sigue funcionando de manera constante dentro de un laboratorio controlado, para garantizar que todos los servicios como el acceso a archivos, las copias de seguridad y las conexiones remotas, funcionen sin interrupciones, se supervisan continuamente, asi mismo se comprueba que cada usuario tenga los permisos apropiados de acuerdo con su función para prevenir accesos no autorizados. Simultáneamente, se implementan métodos de seguridad como la autenticación segura y el cifrado, y se llevan a cabo pruebas para evaluar la estabilidad y el rendimiento del sistema bajo diversas cargas laborales. Todo este procedimiento posibilita el reconocimiento de mejoras y la verificación de que el sistema se encuentre preparado para ser implementado en un ambiente real. Se realiza un manual de funcionamiento el cual está proporcionando información del cual se guiarán estudiantes y docentes dentro del laboratorio controlado.

- El Mini NAS se prueba diariamente para garantizar el funcionamiento normal de los servicios de acceso remoto, respaldo y conectividad.
- Se monitorean los accesos de los usuarios y se ajustan los permisos según sea necesario para mantener la seguridad y el orden.

- Todos los eventos importantes, como accesos, errores o cambios de configuración, se registran para su posterior análisis.
- Se aplica un manual de funcionamiento para el uso de futuros usuarios y administradores del dispositivo para un buen manejo guiándose correctamente para varias instancias.

1.2 OBJETIVOS

1.2.1 OBJETIVO GENERAL

Optimizar el sistema de almacenamiento del laboratorio de REDES a través de un mini NAS que posibilite un acceso seguro a distancia a través de una conexión VPN para potenciar la protección de activos digitales.

1.2.2 OBJETIVOS ESPECÍFICOS

- Elaborar un plan para implementar el sistema mini NAS, seleccionando el equipo apropiado, ajustando adecuadamente la red y estableciendo normas claras de acceso y seguridad.
- Configurar el servidor mini NAS, crear usuarios con permisos diferenciados, establecer políticas de seguridad y realizar la configuración de conectividad VPN, con el objetivo de garantizar un funcionamiento seguro, eficiente y controlado del sistema.
- Administrar el funcionamiento continuo del sistema mini NAS en el laboratorio, garantizando la disponibilidad de los servicios, el control de accesos y la estabilidad operativa mediante monitoreo diario y ajustes técnicos menores.
- Elaborar un manual de uso para el sistema mini NAS que incluya instrucciones claras y detalladas sobre el acceso, la gestión de archivos, la administración de usuario el mantenimiento básico con el fin de facilitar su utilización por parte de los usuarios del laboratorio y asegurar el aprovechamiento eficiente del sistema.

1.3 JUSTIFICACIÓN

Hoy en día en el ámbito laboral como resguardar la información de manera privada y segura, las organizaciones han visto la necesidad de buscar soluciones para realizar esta tarea de manera eficiente y sin complicaciones [12]. En estos tiempos actuales donde el teletrabajo se ha convertido en la principal forma de trabajar, garantizar seguridad a la red de las empresas es una prioridad [13].

Este proyecto satisface esta demanda, sugiriendo una solución que posibilite a los estudiantes tener acceso a sus archivos de manera segura desde cualquier lugar, asegurando a la vez la integridad y disponibilidad de la información. Esta sugerencia no solo optimiza la infraestructura tecnológica del laboratorio, sino que también potencia las habilidades prácticas de los alumnos en campos como redes, ciberseguridad y gestión de sistemas.

Los enlaces privados antes de la aparición de las Redes Privadas Virtuales, Presenta un breve enfoque de las tecnologías WAN tradicionalmente implementadas, tanto dedicadas como conmutadas, entre las que se encuentran Clear Channel, Frame Relay, ATM, líneas análogas y líneas digitales RDSI, VPNs: Describe la tecnología, sus casos de uso y sus partes, arquitecturas VPN: Profundiza en cada una de las soluciones que se pueden implementar con VPNs: Acceso Remoto, autenticación y Cifrado: Explica los conceptos de seguridad en que se basan todas las tecnologías actuales para establecer una VPN [14].

El proyecto proporciona una respuesta concreta al problema del acceso y la protección de datos en el contexto educativo mediante la introducción de un sistema NAS capaz de acceso remoto a través de VPN. Esto simplifica las copias de seguridad automatizadas, administra usuarios con diferentes niveles de acceso y garantiza que la información esté siempre disponible fuera del laboratorio.

PLAN DE DESARROLLO AL NUEVO ECUADOR 2025-2029

Eje Ambiente, Agua, Energía y Conectividad

Objetivo 7: Impulsar el desarrollo de infraestructuras sostenibles y resilientes; y de la conectividad física y digital, que brinde condiciones de crecimiento y desarrollo económico [15].

Política 7.1: Impulsar el desarrollo digital a través de la mejora en tecnología y la expansión de la conectividad en áreas geográficas no atendidas o con conectividad limitada en el país [15].

1.4 ALCANCE DEL PROYECTO

La carga de trabajo de este título tiene como objetivo optimizar la gestión y protección de los activos digitales en el laboratorio de redes de la Península del Estado de la Universidad de Santa Elena (UPSE), desarrollando e introduciendo un modelo de almacenamiento distribuido seguro con un servidor Mini NAS (Terramaster F2-212), complementado por

una conexión VPN para proporcionar un mayor acceso seguro. El objetivo de esta propuesta es resolver la falta actual de almacenamiento centralizado y sistema de reserva, lo que afecta negativamente la productividad académica de los estudiantes, y la protección de la información. Las siguientes fases que se aplicaran en esta propuesta se describen a continuación:

PRIMERA FASE: diagnóstico y recopilación de información. Se realizará un estudio de información técnica sobre la infraestructura de laboratorio de red, que incluirá topología de red y opciones de almacenamiento actuales. Las entrevistas de estudiantes se utilizarán para identificar necesidades y problemas actuales almacenamiento y seguridad académica de archivos. Esta etapa nos permite comprender el entorno operativo y crear una base técnica estable para el diseño del sistema.

SEGUNDA FASE : Planificación del sistema y análisis de compatibilidad. Se especifica la configuración del NAS, los requisitos de red y los elementos de seguridad necesarios, como políticas de acceso, cifrado y políticas de mantenimiento. Se desarrollará un esquema de conexión VPN para garantizar el acceso seguro desde ubicaciones externas.

TERCERA FASE: Implementación del sistema de almacenamiento distribuido. se requiere la configuracion de usuarios, carpetas compartidas, políticas de seguridad y la conexión VPN. Se crearán perfiles de acceso diferenciados y los servicios de monitoreo del sistema se activan para probar su estabilidad. Esta etapa termina con evidencia funcional para confirmar el cumplimiento de los objetivos propuestos.

CUARTA FASE: acción del sistema y documentación. El sistema NAS opera constantemente en el laboratorio de red. Se introducirá el proceso de monitoreo diario para garantizar el funcionamiento adecuado del acceso, el soporte y la conexión remota. También se desarrollará un manual de uso para estudiantes con instrucciones claras sobre el uso, la entrada y el mantenimiento básico del sistema. En esta etapa, habrá recomendaciones para mejoras adicionales y la repetición del modelo en otras áreas académicas de la institución.

Este proyecto no incluye la implementación de otros laboratorios, ya que está limitado al entorno especial del laboratorio de red. Las buenas prácticas se aceptan en la gestión de datos seguros. Finalmente, la propuesta pretende ser escalable y se repite en un contexto similar y, por lo tanto, fortalece la infraestructura digital de la universidad y promueve el uso efectivo de las tecnologías disponibles.

CAPITULO II

2.1 MARCO CONCEPTUAL

2.1.1 TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN (TIC)

Las tecnologías de la información y comunicación (TIC) son las principales herramientas del mundo científico actual; engloban todas aquellas tecnologías que permiten procesar, transmitir y almacenar información y que facilitan la comunicación [16]. La tecnología de la información y la comunicación (TIC) es un ámbito de estudio que se debate frecuentemente en casi todas las comunidades del mundo. Los investigadores de todo el planeta han analizado adecuadamente las TIC en la vida comunitaria y su función en el suministro de un ambiente favorable [17].

2.1.2 ALMACENAMIENTO DE DATOS

El sistema de almacenamiento de datos incluye una memoria, un disco duro y una unidad de procesamiento, una primera dirección lógica y una segunda dirección lógica en un primer bloque lógico de la memoria corresponden a datos duplicados, que se almacenan en dos páginas físicas del disco duro [18]. El sistema y el método de almacenamiento de datos ofrecen las ventajas de aumentar la eficiencia de las consultas de datos comerciales y la velocidad de escritura de las entradas de datos y los datos de índice en la segunda unidad [19].

2.1.3 MINI NAS

La invención describe un sistema de almacenamiento NAS basado en un sistema de almacenamiento distribuido Ceph, El sistema de almacenamiento NAS comprende varios nodos de puerta de enlace desplegados fuera de un clúster Ceph de sistemas de almacenamiento distribuido, estos nodos de puerta de enlace incluyen al menos nodos líderes y no líderes, los nodos líderes se determinan mediante bloqueos exclusivos en el clúster Ceph del sistema de almacenamiento distribuido, y los nodos líderes se utilizan para gestionar los no líderes [20].

2.1.4 VPN (RED PRIVADA VIRTUAL)

Las redes privadas virtuales son un campo que ha tenido un desarrollo significativo en cuanto a tecnologías para el empleo seguro de sistemas informáticos interconectados, tanto en el sector privado como en la administración pública. En el sector tecnológico, por su parte, se han registrado inversiones relevantes por parte de los proveedores e

integradores de sistemas. En el ámbito tecnológico, donde se aprecian inversiones significativas de proveedores e integradores de sistemas, así como en el sector privado y la administración pública, que emplean tecnologías para la utilización segura de sistemas informáticos interconectados. [21].

2.1.5 CISCO PPDIOO

PPDIOO es un método de Cisco que establece la secuencia constante de los servicios requeridos para una red [22]. Este método permite una introducción sistemática. reduce los errores y proporciona eficiencia del sistema, este proyecto ha sido adoptado por preparación, planificación, implementación y etapas operativas, adaptado al contexto académico UPSE y las necesidades de laboratorio de redes.

2.1.6 AUTENTICACIÓN Y CONTROL DE ACCESO

El control de acceso es un elemento esencial de seguridad que determina quién puede acceder a ciertos datos, aplicaciones y recursos, y en qué circunstancias, de la misma forma que las claves y listas de invitados con aprobación previa protegen los espacios físicos, las directivas de control de acceso protegen los espacios digitales [23]. El control de acceso evita la información confidencial, como los datos del cliente y la propiedad intelectual que los delincuentes u otros usuarios no autorizados roban. Asimismo, contribuye a garantizar la integridad y disponibilidad de los sistemas, reduciendo riesgos operativos y fortaleciendo la confianza en la infraestructura tecnológica.

2.1.7 CONEXIÓN DE RED

Las conexiones de red son fundamentales para el funcionamiento de la infraestructura digital en el mundo moderno, la interconexión de dispositivos a través de redes ha transformado la forma en que no comunicamos, trabajamos y consumimos información. En este artículo, profundizaremos en qué son las conexiones de red, qué tipo de red es internet, los diferentes tipos de conexiones a internet, cómo funcionan las redes conectadas y su importancia en nuestra vida cotidiana [24].

2.1.8 CLIENTE

Se considera un cliente a una persona o entidad que pide los servicios o el consejo de otra persona o compañía, generalmente a cambio de una retribución, con el fin de cumplir con un objetivo o necesidad específica, los clientes pueden estar presentes en diferentes sectores e industrias, como la financiera, la empresarial, la sanitaria, la jurídica y la

tecnológica, entre otros. Pueden ser individuos que necesiten servicios personales como sesiones de terapia o cortes de pelo, o empresas grandes que busquen soluciones complejas de consultoría o desarrollo de software [25].

2.1.9 MONITORIZACIÓN Y ALERTAS

La monitorización y las alertas automatizadas son componentes cruciales para el éxito de cualquier operación comercial en la era digital actual. Con el rápido avance de la tecnología, las empresas necesitan anticiparse a posibles problemas y amenazas para garantizar la fluidez de sus operaciones y la satisfacción del cliente. [26]. Dado que el sistema de monitoreo del servidor le permite compilar, almacenar y visualizar mediciones, eventos, elementos y pies de tiempo real, puede analizar el panorama general de lo que está sucediendo en su infraestructura de tiempo real. Gracias a estas capacidades, el equipo puede reaccionar ante cualquier anomalía, minimizando interrupciones y asegurando que la infraestructura funcione de manera estable y eficiente.

2.1.10 HERRAMIENTAS TECNOLOGICAS A UTILIZAR.

- **Discos duros (HDD/SSD):** almacena información, archivos multimedia instaladores, manuales, almacena los logs de red de forma segura y con alta disponibilidad [27].
- **Cableado Cat6/Cat7:** Asegura una transmisión de datos rápida y estable entre dispositivos [28].
- **Zerotier (VPN):** Para acceso remoto seguro al NAS [29].
- **NAS:** sirve para almacenar y estén conectado a la red, su tarea es crear copias de seguridad de los archivos que le indiques en la configuración, ya sean del ordenador personal o de cualquier otro dispositivo móvil, sin embargo tiene muchas más funciones; lo único que necesitarás será usar las distintas aplicaciones disponibles para cada fabricante [30].
- **Duple Backups:** Duple Backups ofrece potentes funciones de copia de seguridad y restauración, siendo una herramienta de recuperación ante desastres diseñada para fortalecer la seguridad de los datos de los dispositivos TNAS [31].
- **CloudSync:** Es una aplicación de sincronización de unidades en la nube que permite una rápida y segura sincronización de datos entre el TNAS y las unidades en la nube pertinentes, por lo tanto se trata de una solución completa para recuperarse ante desastres en unidades en la nube, muy eficaz y conveniente [32].

- **Correo gmail:** La sincronización de eventos y contactos se incluye en Gmail, el cual trabaja sin problemas con clientes de escritorio como Mozilla Thunderbird, Microsoft Outlook y Apple Mail, un correo electrónico seguro, privado y que te permite tener el control [33].
- **Drive :** Almacena archivos en la nube con funciones potenciadas por IA para compartirlos sin problemas y mejorar la colaboración [34]. Además, la integración de controles de seguridad y cifrado garantiza que la información compartida se mantenga protegida.
- **Google apps scripts :** Es una plataforma de desarrollo de aplicaciones rápida que permite la creación fácil y veloz de aplicaciones corporativas que se conectan con Google Workspace. Escribirás código en JavaScript moderno y podrás utilizar librerías incorporadas para tus programas preferidos de Google Workspace, como Calendar, Gmail, Drive y otros más [35].
- **SSH :** El uso de SSH encripta la sesión de registro impidiendo que cualquier persona pueda conseguir contraseñas no encriptadas [36].
- **Putty :** Putty es un emulador de terminal gratuito y de código abierto, una aplicación de transferencia de archivos de red y una consola serie para plataformas Windows, permite conectarse a ordenadores o dispositivos remotos mediante varios protocolos [37].
- **OpenVPN :** OpenVPN se autoproclama como la Red Privada Virtual (VPN) más confiable del mundo, y ciertamente cumple con esa afirmación, optimizando software de código abierto, esta VPN ofrece conexiones seguras de punto a punto o de sitio a sitio en configuraciones puente o enrutadas [38].

2.2 MARCO TEÓRICO

2.2.1 USO DE UN DISPOSITIVO NAS PARA CONSTRUIR UN SERVIDOR DE VIDEO DISTRIBUIDO NO CONVENCIONAL

Un servidor de vídeo para comunicar contenido a una pluralidad de clientes, incluyendo uno o más servidores de almacenamiento conectados a red (NAS), cada servidor NAS almacena archivos de contenido para el acceso de uno o más clientes; un conmutador para conectar los clientes a los servidores NAS en respuesta a señales de control, a través de un enlace de comunicación; y una estación de control de gestión conectada a los clientes y a los servidores NAS a través del conmutador, y establece selectivamente un flujo de

datos entre ese cliente y un servidor NAS que almacena el archivo de contenido solicitado, de tal manera que el servidor NAS proporciona el archivo de contenido al cliente a través del flujo de datos, independientemente de otros servidores NAS [39].

2.2.2 EQUIPOS NAS Y SISTEMAS Y MÉTODO DE PROCESAMIENTO DISTRIBUIDO

La invención proporciona un equipo NAS y un sistema y método de procesamiento distribuido, el equipo NAS comprende un enrutador y múltiples módulos de almacenamiento conectados al enrutador; cada módulo de almacenamiento de los múltiples módulos de almacenamiento cuenta con un microcontrolador, un dispositivo de comunicación inalámbrica y un disco magnético; el dispositivo de comunicación inalámbrica y el disco magnético se conectan al microcontrolador por separado; el microcontrolador se utiliza para detectar fallos en el disco magnético durante la lectura de datos y para enviar una instrucción de fallo cuando se detectan fallos en él; el dispositivo de comunicación inalámbrica se utiliza para transmitir datos de lectura y escritura del disco magnético y la instrucción de fallo [40].

2.2.3 ACCESO REMOTO DE DATOS DESDE NAS

Se describen sistemas y métodos para acceder a datos a través de una red de almacenamiento distribuido, un dispositivo de almacenamiento conectado a red (NAS) incluye un módulo de memoria no volátil que comprende una primera porción de almacenamiento para almacenar datos locales de usuario asociados a un dispositivo informático host y una segunda porción compartida para almacenar datos de terceros, el NAS incluye un controlador configurado para proporcionar copias de una porción de los datos de usuario a uno o más NAS para su almacenamiento, recibir datos de terceros de cada uno de estos NAS y almacenarlos en la segunda porción de almacenamiento [41].

2.2.4 SISTEMA DE ALMACENAMIENTO REMOTO QUE UTILIZA UN DISPOSITIVO DE ALMACENAMIENTO CONECTADO A RED (NAS)

Un sistema y un método de almacenamiento remoto que emplea un dispositivo NAS se ofrece, el cual posibilita a un aparato terminal cargar o descargar datos de almacenamiento en el dispositivo NAS por medio de una red. El sistema de almacenamiento remoto que utiliza el dispositivo NAS incluye: un dispositivo NAS diseñado para almacenar la información cargada o descargada por el equipo terminal, a la que se conoce como "información de almacenamiento" [42].

2.2.5 ARCHIVADO DE SERVIDORES NAS EN LA NUBE

Una técnica para archivar servidores NAS (almacenamiento conectado a red), compatibles con los respectivos sistemas de archivos de un servidor NAS, en los respectivos volúmenes con respaldo en la nube, respaldados por un almacén de datos en la nube, una vez que la replicación actualiza los volúmenes con respaldo en la nube con el contenido de los volúmenes locales, la técnica también incluye la realización de una instantánea grupal en los volúmenes con respaldo en la nube [43].

2.2.6 PROPORCIONAR LA CAPACIDAD DE TRABAJAR DE FORMA REMOTA EN EL SERVIDOR LOCAL A TRAVÉS DE VPN

La tunelización VPN cifrada permite que el dispositivo se conecte en una ubicación remota a la red local de la empresa y utilice sus recursos como si estuviera conectado a la red local con un medio de transmisión físico, la solución a las necesidades de acceso remoto a archivos y servicios de servidor puede ser el uso de nubes y servidores privados virtuales (VPS), sin embargo, esto implica altos costos y requiere confiar los datos de la empresa a los proveedores de estos servicios [44]. Tanto por razones de seguridad de los datos como por los altos costos, las empresas a veces no pueden utilizar estas tecnologías. La solución al problema puede ser el uso de tunelización VPN cifrada [44].

2.2.7 ACCESO SEGURO A APLICACIONES DETRÁS DEL FIREWALL

Un usuario que tiene un dispositivo remoto desea acceder a una aplicación que se ejecuta en una computadora servidor de aplicaciones que está detrás de un firewall Durante una fase de configuración, otro firewall y una computadora de enlace se configuran frente al firewall original, creando una zona desmilitarizada (DMZ) que tiene la computadora de enlace. Durante la fase de registro, los dispositivos remotos de los usuarios se configuran con datos de seguridad [45].

2.2.8 POLÍTICAS DE CONTROL DE ACCESO

Se trata de un conjunto de políticas, instrucciones y restricciones que especifican quién puede acceder a sus datos, cuándo y hasta qué nivel, estas políticas deben implementarse adecuadamente en todos los niveles de la organización, las políticas de control de acceso deben aplicarse a todas las personas que acceden a los datos de la organización, incluyendo a los consumidores, productores y demás partes interesadas. Estas personas pueden incluir a sus empleados, socios, contratistas o becarios, Controles de acceso

basados en las normas y regulaciones establecidas por la autoridad, en otras palabras, el acceso es exclusivo del propietario y sus supervisores [46].

2.2.9 RED DE ÁREA AMPLIA (WAN)

Las WAN se fundamentan en diversas tecnologías de red que funcionan en variadas capas o niveles de la red, lo que posibilita su funcionamiento, en esencia las WAN se sustentan sobre el intercambio de datos que comprende tres componentes esenciales: paquetes de datos, enrutadores y endpoints, estas redes son un conjunto de redes más pequeñas e interconectadas entre sí, formadas por computadoras y otros dispositivos menores conocidos como redes de área local [47].

2.3 METODOLOGÍA DEL PROYECTO

2.3.1 METODOLOGÍA DE LA INVESTIGACIÓN

Este proyecto cubrirá cuatro pasos principales para implementar correctamente un sistema de almacenamiento NAS. Su desarrollo se basa en la metodología utilizada en estudios de casos similares de soluciones de almacenamiento seguro de datos en instituciones educativas y gubernamentales. La propuesta se divide en cuatro fases principales: preparación, planificación, implementación y operaciones, para garantizar un acceso seguro, eficiente y centralizado a la información. Los pasos le servirán como guía para poner en funcionamiento su sistema NAS en el laboratorio de redes.

Con en el método escogido, el proyecto se centrará en cuatro etapas personalizadas específicamente para la puesta en marcha de un sistema de almacenamiento automatizado a través de mini NAS con acceso remoto por medio de VPN. En este proyecto se desarrollará la metodología PPDIOO [48], empleadas en proyectos similares y se detallan más adelante como orientación para el desarrollo e implementación de la solución sugerida.

2.3.2 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

En esta etapa, se llevará a cabo una encuesta a los estudiantes de diferentes semestres que cruzan y hayan cruzado por el laboratorio de REDES(Anexo1), con el objetivo de recolectar datos significativos sobre las necesidades, vivencias y percepciones vinculadas al almacenamiento de datos, la protección digital y el acceso a distancia en el laboratorio REDES. Esta metodología facilitará la adquisición de una perspectiva contextual y minuciosa de los retos presentes y de las posibilidades de mejora.

Se toma en cuenta las practicas preprofesionales realizadas dentro de la Universidad Península de Santa Elena para entender las necesidades y como se llevarían a cabo la forma de implementarlo dentro de esta institución y dar eficacia de este proyecto para una eficaz implementación.

Materia	Semestre	Total Estudiantes	Estudiantes Por Encuestar
FUNDAMENTO DE REDES	TERCERO	24	14
COMUNICACIÓN Y ENRUTAMIENTO DE DATOS	CUARTO	28	15
INGENIERÍA DE SOFTWARE	CUARTO	44	22
ETHICAL HACKING	SEXTO	27	14
INTERNET DE LAS COSAS	SEXTO	27	14
ARQUITECTURA Y PLATAFORMA TI	SEXTO	23	12
COMPUTACIÓN FORENSE	SEPTIMO	25	10
SEGURIDAD DE TI	SEPTIMO	22	10

TABLA 1 ESTUDIANTES A ENCUESTAR SEGÚN MATERIA Y NIVEL ACADÉMICO

La información recolectada se utilizará como fundamento para valorar la factibilidad y el posible efecto de un sistema de almacenamiento en red (NAS) con acceso a distancia a

través de VPN. Esta recopilación de información cualitativa para el análisis técnico del proyecto, facilitando la solución sugerida con las circunstancias verdaderas del ambiente académico.

2.3.3 ENFOQUE METODOLÓGICO APLICADO.

La metodología PPDIOO se basa en los lineamientos establecidos en el ciclo de vida PPDIOO, que Cisco utiliza para la administración de redes [49]. que organiza el ciclo de vida de una red en cinco etapas, Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar. En esta situación, se llevarán a cabo las fases más ajustadas al ambiente del laboratorio, específicamente. Elaboración, que comprende la instalación y configuración del sistema min NAS. Operar, donde se pone en marcha el sistema y se monitorea su funcionamiento. Este procedimiento promueve una aplicación ordenada, minimiza errores y asegura que la solución sea efectiva, segura y en consonancia con los objetivos del laboratorio.

2.3.4 METODOLOGÍA DE DESARROLLO

Este proyecto cubrirá cuatro pasos básicos para implementar correctamente un sistema de almacenamiento conectado a la red (NAS), para su desarrollo se tomó como referencia el método utilizado en casos de estudio similares sobre soluciones de almacenamiento seguro en instituciones educativas y públicas, la propuesta se estructura en cuatro etapas esenciales: preparación, planificación, implementación y operación, que deben garantizar el acceso seguro, eficiente y centralizado a la información.

Con en el método escogido, el proyecto se centrará en cuatro etapas personalizadas específicamente para la puesta en marcha de un sistema de almacenamiento automatizado a través de mini NAS con acceso remoto por medio de VPN. Estas etapas se han diseñado utilizando metodologías PPDIOO [48], empleadas en proyectos similares y se detallan a continuación como orientación para el desarrollo e implementación de la solución sugerida.

- Fase 1: Preparar. Esta fase se busca establecer una justificación para la estrategia de red [48]. Permite identificar las necesidades específicas del entorno y los objetivos que se desean alcanzar. Con ello se garantiza que la estrategia propuesta sea coherente viable y alineada con los requerimientos técnicos y operativos del proyecto.

- Fase 2: Planificar: Este segundo paso consiste en determinar las necesidades de la red a través de una caracterización y evaluación, así como un análisis de las falencias en comparación con los estándares arquitectónicos más efectivos [48]. Se establecen los criterios técnicos y se organiza la incorporación del NAS en la infraestructura ya existente.
- Fase 3: Implementar. Al añadir nuevos dispositivos sin detener la red, se acelera el retorno sobre la inversión, aprovechando el trabajo realizado en las dos fases anteriores [48]. Se establecen los usuarios del sistema, se otorgan permisos de acceso de acuerdo con roles y se implementan medidas de seguridad, asegurando un ambiente resguardado y regulado.
- Fase 4: Operar. Esta etapa conserva el estado de la red de un día para otro, esto abarca la supervisión y administración de los elementos de la red, el mantenimiento, la gestión de las actualizaciones, el manejo del rendimiento, así como la detección y solución de fallos en la red [48]. Se analiza la eficacia del sistema implementado, verificando el cumplimiento de los objetivos planteados y midiendo el rendimiento, la seguridad y la satisfacción de los usuarios.

IDEA A DEFENDER

Se identifica que el 63% de los estudiantes enfrentaban riesgos debido a los pendrives y más del 78% necesitaban almacenamiento compartido. Utilizando VPN (Zerotier/OpenVPN), se realizaron pruebas de conexión remota con una latencia promedio de 26 ms y un pico de hasta 72 ms sin pérdida de paquetes. Las velocidades de transferencia alcanzaron 1,76 MB/s usando CloudSync y el sistema respondió exitosamente a más del 90% de los intentos con copias de seguridad automáticas y alertas de error.

CAPITULO III

3.1 REQUERIMIENTOS

3.1.1 REQUERIMIENTO FUNCIONALES

Requisitos Esenciales de un sistema NAS para acceso remoto protegido. Se describen las funciones fundamentales que el sistema debe llevar a cabo, incluyendo la gestión de archivos de usuarios permitidos en un entorno seguro, la inclusión de un servidor VPN para establecer conexiones encriptadas, la creación de distintos roles de usuario, el envío de alertas automáticas en caso de fallos, y la posibilidad de ampliar el almacenamiento conforme a requerimientos futuros. Estas especificaciones garantizan que el sistema sea seguro, escalable y capaz de adaptarse a diversas modalidades de uso.

Código	Descripción
RF1	El NAS debe de poder acceder a todos los archivos de los usuarios permitidos para que la información importante esté siempre disponible desde un lugar seguro. Esto proporciona un punto único y confiable de acceso a los datos, facilitando su administración y protección contra fallas o accesos no autorizados.
RF2	Se introducirá un servidor VPN integrado, lo que permite a los usuarios autorizados conectarse de forma segura desde lugares externos y cifrar toda la información transmitida.

Código	Descripción
RF3	Se crearán roles de usuario diferenciados (lectura, escritura, administrador) para garantizar que cada persona tenga acceso a información que coincida exclusivamente con su perfil.
RF4	El sistema envía automáticamente un correo ante error de disco, intentos de acceso no autorizados o problemas de beneficios.
RF5	El sistema le permite agregar discos adicionales o expandir su almacenamiento en el futuro y adaptarse a las crecientes necesidades de información.

TABLA 2 REQUERIMIENTO FUNCIONALES

3.1.2 REQUERIMIENTOS DE HARDWARE

Especificaciones de hardware, para establecer un sistema NAS con acceso remoto protegido. Se indican los elementos fundamentales como unidades de almacenamiento diseñadas para un uso prolongado, un enrutador que permita conexiones seguras a través de VPN, cables de red con alta velocidad, una computadora portátil para la gestión del sistema, y componentes esenciales como cables de corriente. Cada dispositivo desempeña un papel crucial para asegurar la eficiencia, la protección y la capacidad de expansión del sistema.

Dispositivo	Especificaciones	Descripción
Discos duros	HDD de 4–12 TB clase NAS (WD Red, Seagate IronWolf), mínimo 2 por nodo; opcional SSD NVMe/SATA para caché	Almacenamiento físico optimizado para operación 24/7, con tolerancia a vibración y mayor vida útil.
Router VPN	Router con soporte OpenVPN/WireGuard,	Crea túneles seguros entre nodos de almacenamiento distribuidos.
Cable de Red (Ethernet Cat 6)	Cable Cat 6 blindado, 1 Gbps.	Conexión estable y rápida entre NAS.
Laptop de Administración	Procesador Intel Core i5, 8 GB RAM, SSD 256 GB.	Gestión remota del NAS, monitoreo de VPN y análisis de logs.
Cable de Alimentación	Cable de alimentación para router con enchufe IEC C13 a toma, longitud de 1,5 a 2 metros, alimentación 250 V / 10 A (estándar AC)	Suministro de energía para NAS, router, switch o UPS.

TABLA 3 REQUERIMIENTOS DE HARDWARE

3.1.3 REQUERIMIENTOS DE SOFTWARE

Requisitos de software para un sistema NAS con acceso remoto seguro. Incluye herramientas esenciales de administración del sistema, incluidos TOS para la

administración de almacenamiento y usuarios del sistema operativo, así como OpenVPN y ZeroTier para conexiones seguras y aplicaciones como Duple Backup para copias de seguridad automatizadas. Además, se tienen en cuenta módulos de control y gestión de archivos, que garantizan una operación y mantenimiento eficiente y seguro del sistema.

Software	Especificación	Descripción
TOS (TerraMaster Operating System)	Sistema operativo del NAS.	Gestión de usuarios, permisos, RAID, compartición de archivos y apps de respaldo.
OpenVPN	Software de red privada virtual.	Creación de túneles cifrados entre nodos NAS distribuidos para transferencia segura de datos.
Administrador de archivos	Gestor de archivos interno del NAS.	Permite explorar, copiar, mover y administrar datos directamente en el sistema.
Panel de control	Módulo de administración principal.	Gestión de usuarios, permisos, almacenamiento, red y servicios del NAS.
Duple Backups	Aplicación de copias avanzadas	Permite backups local, remoto y en la nube con programaciones automáticas.

Software	Especificación	Descripción
ZeroTier	Software de red definida por software (SD-WAN).	Crea una red privada virtual simple entre varios dispositivos distribuidos.

TABLA 4 REQUERIMIENTOS DE SOFTWARE

3.1.4 REQUERIMIENTOS NO FUNCIONALES

El sistema NAS con acceso remoto protegido. Se definen parámetros importantes como la disponibilidad constante de la información, la seguridad en la transmisión utilizando VPN, la integridad a través de replicación y validación, el cifrado de extremo a extremo, una interfaz de gestión fácil de usar y segura, y la posibilidad de ampliar el sistema sin afectar su funcionamiento. Estos requisitos garantizan que el sistema sea fiable, seguro y adaptable a largo plazo.

Código	Descripción
RNF1	El sistema debe garantizar la disponibilidad continua de los datos, permitiendo acceso 24/7 mediante el mini NAS.
RNF2	La transferencia de datos entre nodos del NAS y clientes debe realizarse de manera segura a través de VPN, evitando exposición en redes públicas.
RNF3	La integridad de los datos debe asegurarse mediante replicación y verificación de hashes en los archivos almacenados.
RNF4	El sistema debe ofrecer cifrado de extremo a extremo, protegiendo la información

Código	Descripción
	durante el almacenamiento y la transmisión.
RNF5	La interfaz de administración debe ser intuitiva y segura, mostrando el estado de almacenamiento, nodos conectados y alertas de seguridad.
RNF6	El sistema debe ser escalable, permitiendo agregar nuevos mini NAS sin interrupciones ni pérdida de datos.

TABLA 5 REQUERIMIENTOS NO FUNCIONALES

3.2 COMOPONENTE DE LA PROPUESTA TECNOLOGICA

Esta sección continúa mostrando la parte práctica de la propuesta tecnológica, en la cual, para proteger la información crítica, se desarrolló un sistema de almacenamiento generalizado de forma segura, que se complementa con una conexión VPN. El sistema está diseñado para garantizar la disponibilidad, integridad y confidencialidad de los datos, lo que permite la replicación automática entre nodos, cifrado de archivos y administración de acceso seguro. Además, se introdujo un panel de control interactivo para monitorear el estado de los dispositivos, la sincronización de los archivos y las advertencias de seguridad de tiempo real que facilitan la administración y el monitoreo del entorno de información crítica.

Fase I: Preparar

Fase II: Planificar

Fase III: Implementar

Fase IV: Operar

3.2.1 FASE 1: PREPARAR

En esta primera Fase, se realiza un estudio de laboratorio de red, lo que garantiza que todas las actividades se lleven a cabo en un marco autorizado e institucional, este permiso proporciona acceso a los equipos y recursos necesarios sin interferir con la operación de laboratorio habitual, asegurando que se realice todo de manera controlada y segura.

Esta fase se trata de la preparación del equipo para un buen funcionamiento, este equipo denominado como un servidor de archivo tendra sus diferentes funciones dentro del laboratorio de REDES, y los requisitos para una correcta instalación son :

Requisitos generales para instalación dentro del laboratorio :

- Permisos para instalación de equipo dentro del laboratorio
- Permisos para uso de puertos dentro del laboratorio
- Uso del servidor compacto NAS
- Uso de 2 Disco HDD para el sistema Raid
- Red vía LAN de Switch del laboratorio directo al Nas
- Vpn para conexión externa del Equipo
- Encuesta satisfactoria a estudiantes para sus beneficios con el dispositivo.

ANÁLISIS DE RESULTADOS DE LA ENCUESTA

El objetivo de esta encuesta permitirá fundamentar técnicamente la necesidad de una estrategia de red más eficiente y centrada en el almacenamiento centralizado y seguro.

CONCLUSIÓN 1 :

Los resultados muestran que la mayoría de los encuestados (42,3%) cree que la existencia de plataformas no compartidas para el almacenamiento y consulta de archivos es "posible", mientras que un 29,7% dijo que sí y un 27,9% que no.

1. ¿Hay algúna Plataforma que no sea común donde se pueda guardar y consultar con los archivos?

RESPUESTA	TOTAL	PORCENTAJE
si	**33**	**29,7%**
no	**31**	**27,9%**
Probablemente	**47**	**42,3%**
TOTAL	**111**	**100%**

TABLA 6 PREFERENCIAS DE ALMACENAMIENTO ALTERNATIVO

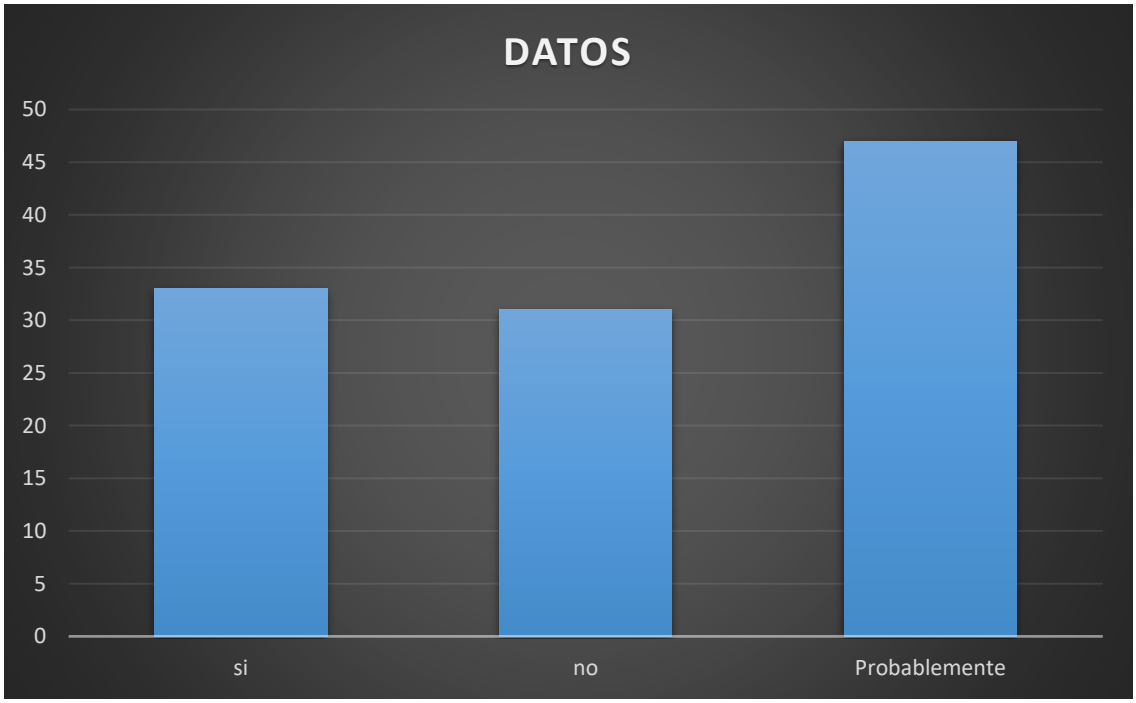


FIGURE 1 RESULTADOS DE OPINIÓN: PLATAFORMAS NO COMUNES

CONCLUSIÓN 2 :

Los resultados muestran que el 36,9% de los encuestados cree que el almacenamiento que utilizan habitualmente es seguro, mientras que el 36% cree que no lo es y el 27% aún no está seguro. Tanto la tabla como el gráfico reflejan un panorama común de la seguridad de los métodos actuales, lo que muestra la necesidad de fortalecer las prácticas y tecnologías que garanticen la protección de la información.

1. **¿ Cree usted que es seguro el almacenamiento que utilizan normalmente ?**

RESPUESTAS	TOTAL	PORCENTAJE
SI	**41**	**36,9%**
NO	**40**	**36%**
PROBABLEMENTE	**30**	**27%**
TOTAL	**111**	**100%**

TABLA 7 CONFIANZA EN EL ALMACENAMIENTO

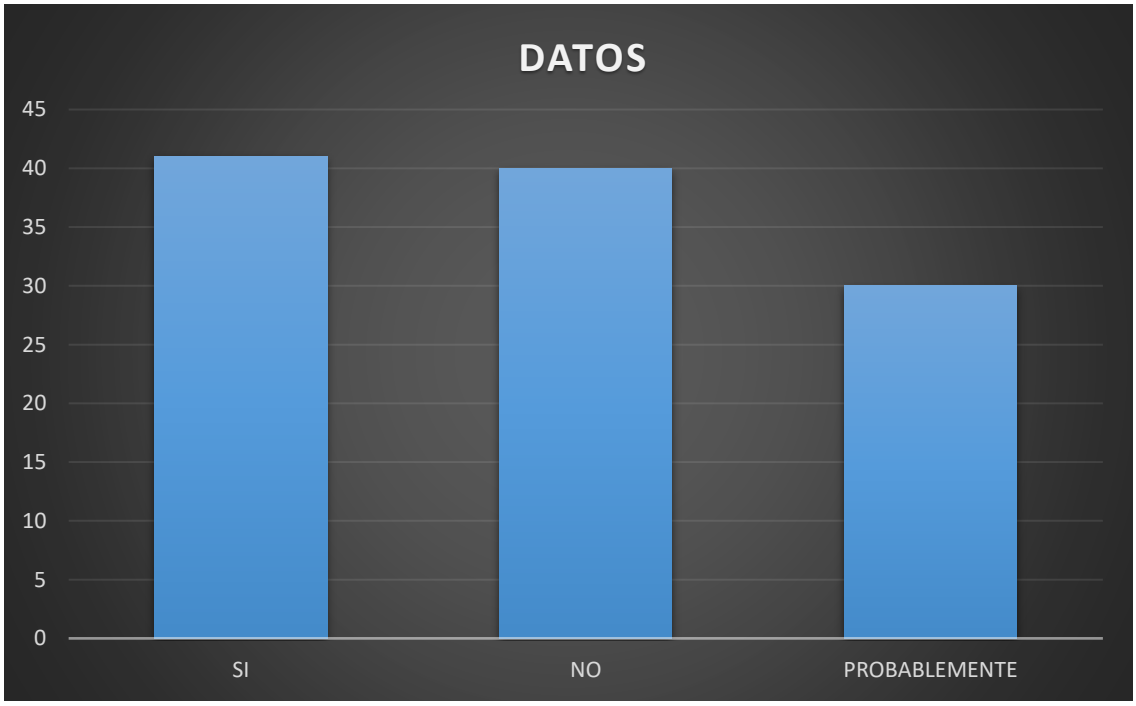


FIGURE 2 CONFIANZA EN EL ALMACENAMIENTO

CONCLUSIÓN 3 :

Los resultados muestran que el 63,1% de los encuestados ha tenido miedo a los virus al utilizar pendrives para compartir archivos, mientras que el 25,2% respondió "Posiblemente" y sólo el 11,7% dijo que no tenía tales preocupaciones. Tanto la tabla como el gráfico reflejan que el uso de dispositivos portátiles todavía se percibe como un riesgo importante, destacando la necesidad de implementar soluciones más seguras para la transferencia de información.

3. ¿Ha Tenido un pendrive para el compartimiento de archivos con el temor de algún virus?

RESPUESTAS	TOTAL	PORCENTAJE
SI	**70**	**63,1%**
NO	**13**	**11,7%**
PROBABLEMENTE	**28**	**25,2%**
TOTAL	**111**	**100%**

TABLA 8 RIESGO EN USO DE PENDRIVE

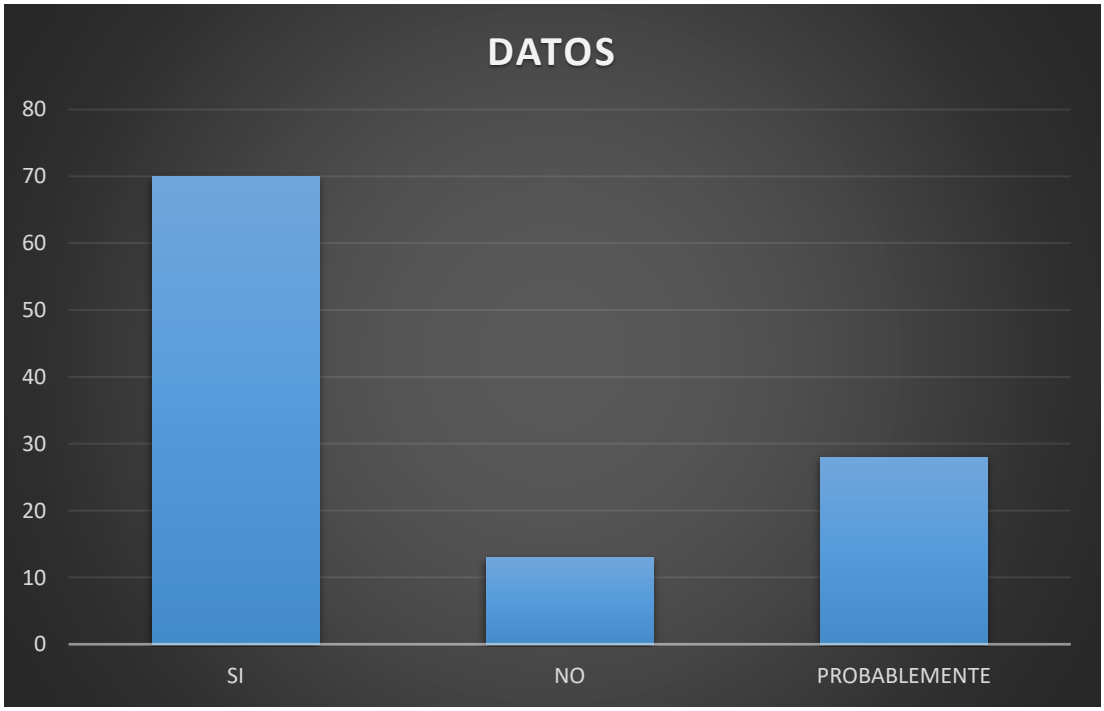


FIGURE 3 RIESGO EN USO DE PENDRIVE

CONCLUSIÓN 4 :

Los resultados muestran que el 78,4% de los encuestados cree que un repositorio compartido para acceder a instaladores, horarios y manuales haría que el trabajo estuviera más organizado. El 16,2% respondió "Quizás", y sólo el 5,4% no lo considera necesario. Tanto la tabla como el gráfico reflejan una clara preferencia por soluciones centralizadas que faciliten la gestión y disponibilidad de recursos en el mundo académico.

4. ¿Crees que sería mejor si existiera un tipo de almacenamiento el cual todos puedan acceder a instaladores, horarios y manuales?

RESPUESTAS	TOTAL	PORCENTAJE
Si sería más organizado	87	78,4%
Tal vez	18	16,2%
No lo veo necesario	6	5,4%
TOTAL	111	100%

TABLA 9 ALMACENAMIENTO SEGURO COMPARTIDO

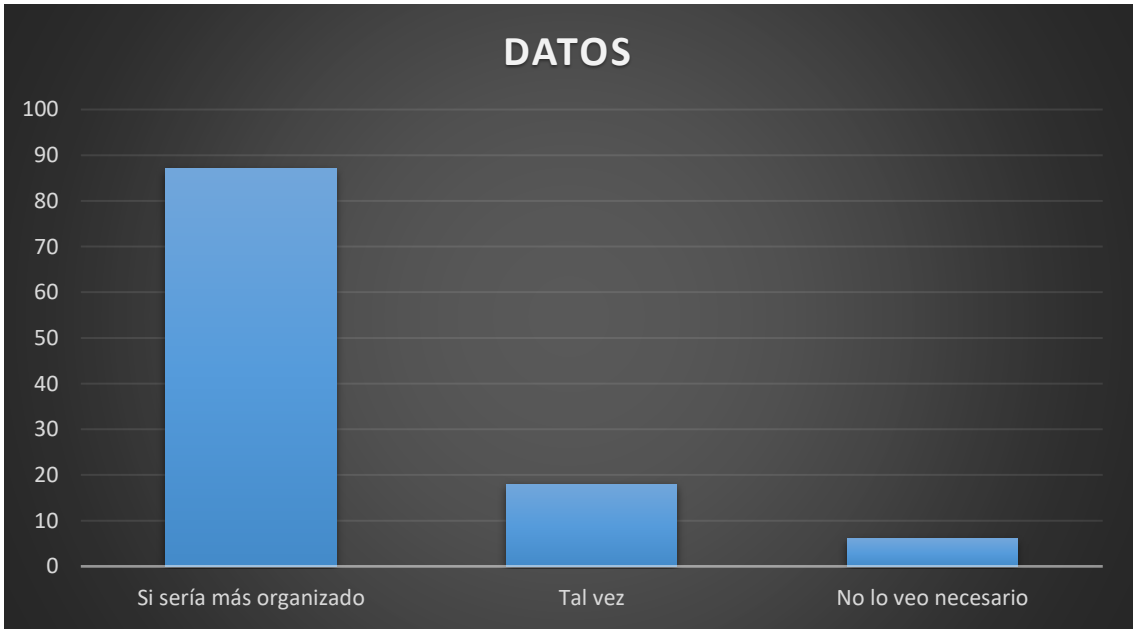


FIGURE 4 ALMACENAMIENTO SEGURO COMPARTIDO

CONCLUSIÓN 5 :

Los resultados muestran que el 55,9% de los encuestados ha tenido que rehacer tareas o configuraciones porque no se encontraban archivos anteriores, mientras que el 27% afirma que esto les ha sucedido en algún momento, y sólo el 17,1% nunca se ha encontrado con una situación así. Tanto la tabla como el gráfico reflejan que la falta de organización en el almacén conlleva pérdidas de tiempo y procesamiento, mostrando la necesidad de implementar sistemas centralizados y seguros.

5. ¿Ha tenido que repetir tareas o configuraciones porque no encontró archivos de instaladores o documentos anteriores?

RESPUESTAS	TOTAL	PORCENTAJE
SI	62	55,9%
NO	30	17,1%
ALGUNA VEZ ME PASÓ	19	27%
TOTAL	111	100%

TABLA 10 RIESGO A PERDIDA DE ARCHIVOS

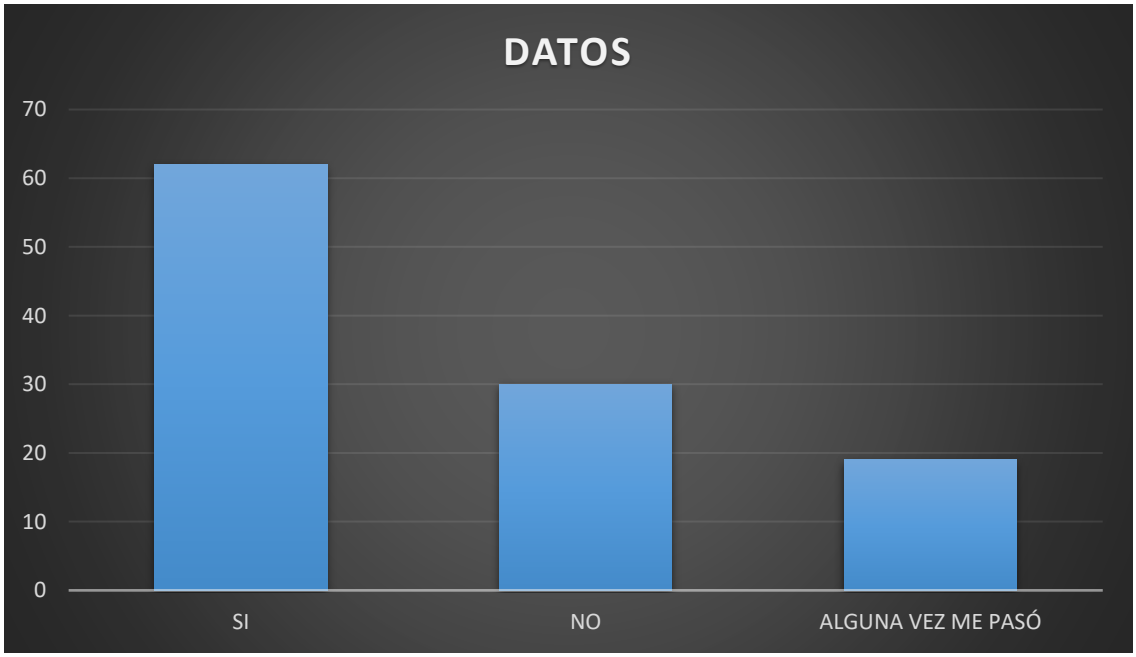


FIGURE 5 RIESGO A PERDIDA DE ARCHIVOS

CONCLUSION 6 :

Los resultados muestran que el 68,5% de los encuestados cree que es muy útil acceder a los archivos del laboratorio de forma remota, mientras que el 28,8% lo utilizaría ocasionalmente y sólo el 2,7% no está interesado en ello. Tanto la tabla como el gráfico reflejan una clara preferencia por la implementación del acceso remoto, lo que muestra la necesidad de soluciones que promuevan el acceso seguro a recursos fuera de la universidad.

6. ¿Desearias poder ingresar archivos locales del laboratorio externamente de la Universidad ?

RESPUESTAS	TOTAL	PORCENTAJE
Si, lo considero muy útil	76	68,5%
Tal vez pero no lo usaría mucho	32	28,8%
No estoy interesado	3	2,7%
TOTAL	111	100%

TABLA 11 INGRESO REMOTO

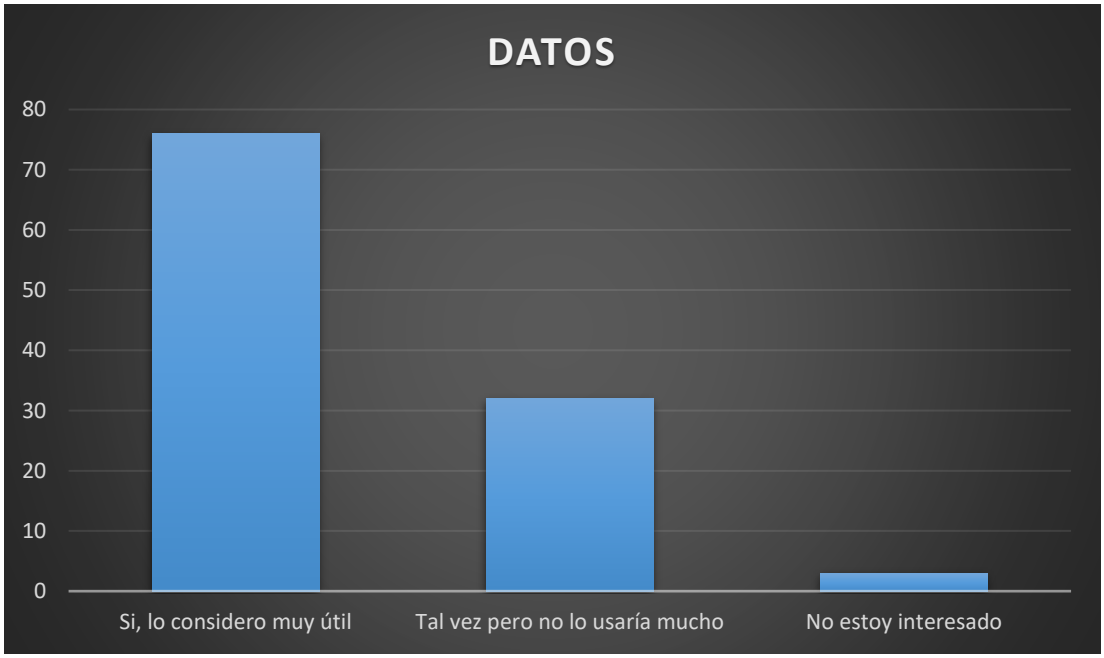


FIGURE 6 INGRESO REMOTO

CONCLUSIÓN 7 :

Los resultados muestran que el 45,9% de los encuestados no puede compartir archivos sin enviarlos directamente, mientras que el 27,9% lo hace sólo algunas veces y el 26,1% tiene esta opción. Tanto la tabla como el gráfico reflejan que la mayoría enfrenta limitaciones para compartir información de manera efectiva, lo que muestra la necesidad de soluciones de colaboración más flexibles y seguras.

7. ¿ Puedes compartir tus archivos con otras personas sin necesidad de enviárselos directamente.?

RESPUESTAS	TOTAL	PORCENTAJE
SI	29	26,1%
NO	51	45,9%
SOLO A VECES	31	27,9%
TOTAL	111	100%

TABLA 12 ENVIO DE ARCHIVOS NO DIRECTAMENTE

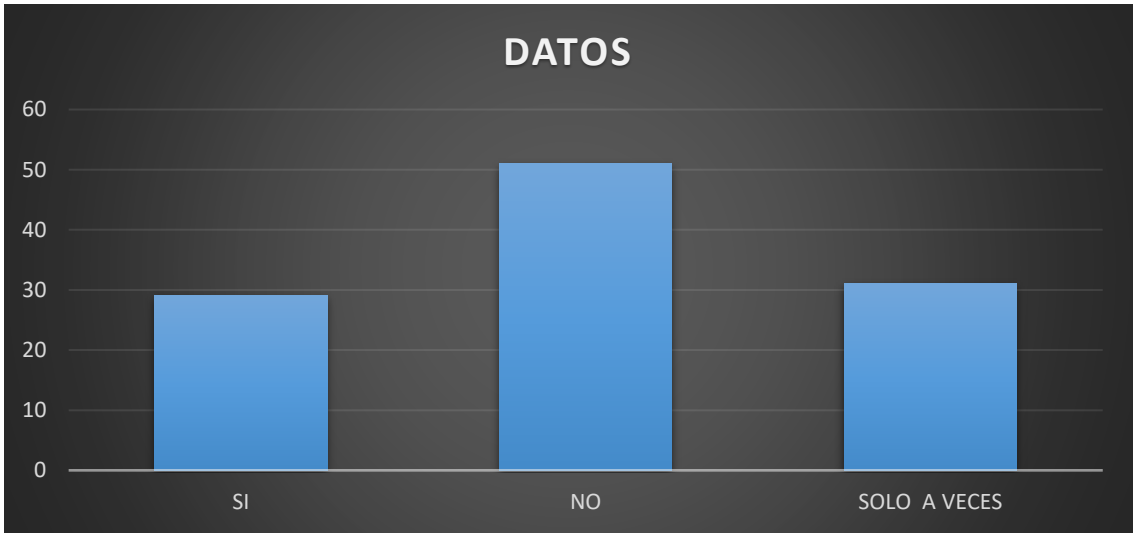


FIGURE 7 ENVIO DE ARCHIVOS NO DIRECTAMENTE

CONCLUSIÓN 8 :

Los resultados muestran que el 70,3% de los encuestados cree que el principal beneficio de un sistema de almacenamiento compartido sería el acceso a sus archivos desde cualquier lugar, mientras que el 18,9% valora trabajar con la misma versión del archivo y el 10,8% evita el uso de dispositivos USB. Tanto la tabla como el gráfico muestran claramente la elección del acceso remoto, enfatizando la importancia de soluciones que faciliten la accesibilidad y la colaboración en entornos académicos.

8. ¿Qué beneficio apreciaría más en el sistema de almacenamiento compartido?

RESPUESTAS	TOTAL	PORCENTAJE
Acceder a mis archivos desde cualquier lugar	78	70,3%
Que trabajemos con la misma versión del archivo	21	18,9%
No tener que usar USB ni discos externos	12	10,8%
TOTAL	111	100%

TABLA 13 ALMACENAMIENTO COMPARTIDO

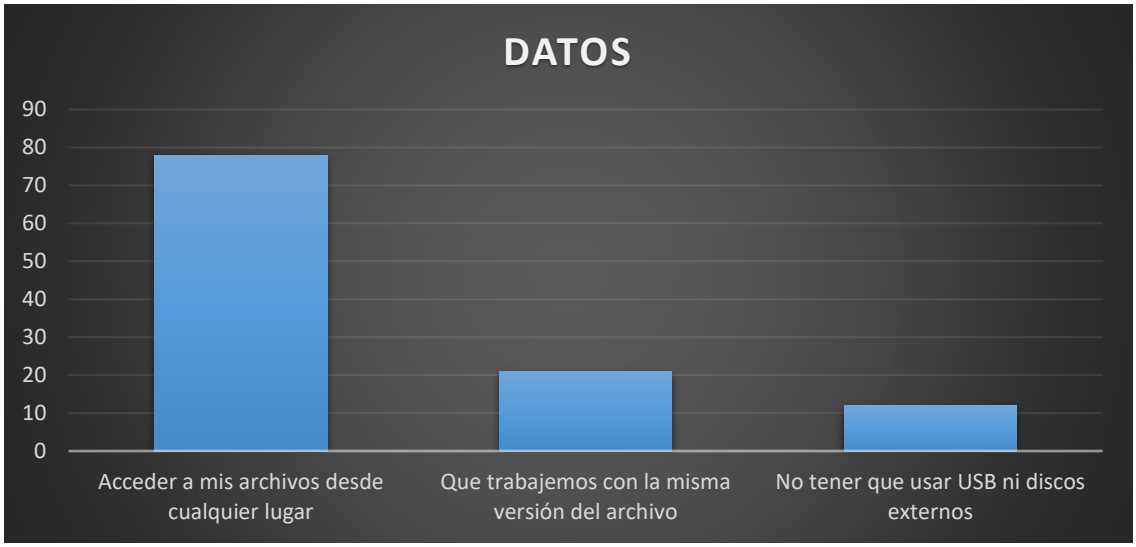


FIGURE 8 ALMACENAMIENTO COMPARTIDO

INSTALACIÓN DE DISCO DUROS AL NAS

El equipo tiene 2 bahías, donde cada una tiene una unidad de 500 GB. Después de la colocación y el seguro, se les reconoce y se les permite crear arreglo (RAID) o que esta esté forma independiente. Proporciona un espacio de almacenamiento central de hasta 1 TB, que está disponible en las unidades conectadas de la red. Usando este paso, los NA están listos para guardar de forma segura y compartir información.

FIGURE 9 INSTALACIÓN DE DISCO DUROS AL NAS

3.2.2 FASE 2 -PLANIFICAR

En la segunda fase, la planificación integrada se desarrolla para implementar un sistema de almacenamiento dividido basado en Mini. El objetivo principal es definir una configuración detallada de red, seguridad y soporte para que la fase de implementación se pueda hacer sin interrupción.

CUADRO COMPARATIVO

Este cuadro de comparación destaca las principales diferencias entre tres opciones para almacenamiento y acceso remoto: Mini NAS con VPN (Zerotier/OpenVPN), NAS convencional y almacenamiento en la nube. Su intención es ilustrar cómo cada alternativa se desempeña en aspectos como seguridad, accesibilidad, gestión de usuarios, gastos, dependencia de internet y capacidad de expansión, facilitando la selección de la opción más apropiada de acuerdo a las necesidades financieras y técnicas.

Tecnología	Propuesta Zerotier / OpenVpn con Mini Nas	Nas Estandar	Almacenamiento En la Nube
ACCESO REMOTO SEGURO	DOBLE CAPA DE SEGURIDAD, ACCESO SEGURO REMOTAMENTE ✓	SOLO ACCESO LOCAL ✓	ACCESO REMOTO NATIVO DEPENDIENDO DEL INTERNET ✗
CONTROL DE USUARIO Y PERMISOS	PERMISO CONFIGURABLES DENTRO DEL NAS Y AUTENTIFICACIÓN DEL NAS ✓	PERMISOS LOCALES Y MENOS FLEXIBLE. ✗	LIMITADO ✗

Tecnología	Propuesta Zerotier / OpenVpn con Mini Nas	Nas Estandar	Almacenamiento En la Nube
COSTO DEL DISPOSITIVO	COSTO INICIAL (NAS + DISCOS) ✓	IGUAL AL COSTO INICIAL SIN VPN INTEGRADA ✓	PAGO MENSUAL Y COSTO RECURRENTE A LARGO PLAZO ✓
DEPENDENCIA DE INTERNET	ACCESO LOCAL SIN INTERNET ✓	SOLO VIA LAN, NO DEPENDE DE INTERNET ✓	REQUIERE CONEXIÓN PERMANENTE PARA PASO DE DATOS ✓
-ESCALABILIDAD	FACIL AMPLIACIÓN DE DISCOS ADICIONALES O CONFIGURACIÓN RAID ✓	AMPLIACIONES POSIBLES PERO LIMITADAS AL HADWARE ✗	ESCALABLE PERO CON MAYOR COSTO MENSUAL ✗

TABLA 14 COMPARATIVO DE SOLUCIONES DE ALMACENAMIENTO Y ACCESO SEGURO.

INFRAESTRUCTURA DE RED

La solución Mini Nas Zerotier se selecciona, ya que permite la introducción de un sistema de almacenamiento controlado con un control completo sobre la infraestructura y los datos. Esta configuración facilita una conexión remota, aumentando la confidencialidad e integridad de la información durante el tránsito.

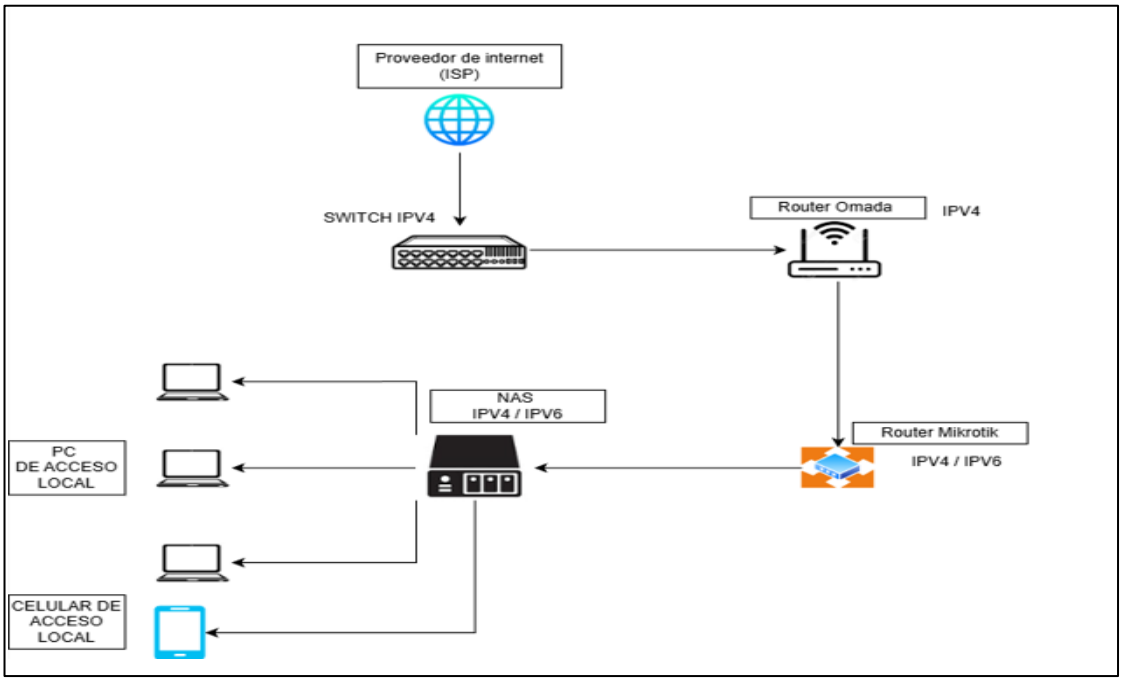


FIGURE 10 INFRAESTRUCTURA ADECUADA AL ENTORNO DE LABORATORIO CONTROLADO

TOPOLOGÍA DE RED HIBRIDA

Topología de red híbrida en la que el proveedor de servicios de internet se conecta al router Mikrotik pasando primero por el router Omada, la red se extiende desde este punto central hacia un NAS y también hacia dispositivos que son inalámbricos y con cable, la estructura mezcla componentes de árbol y estrella, lo que posibilita el acceso a teléfonos y computadoras personales a nivel local.

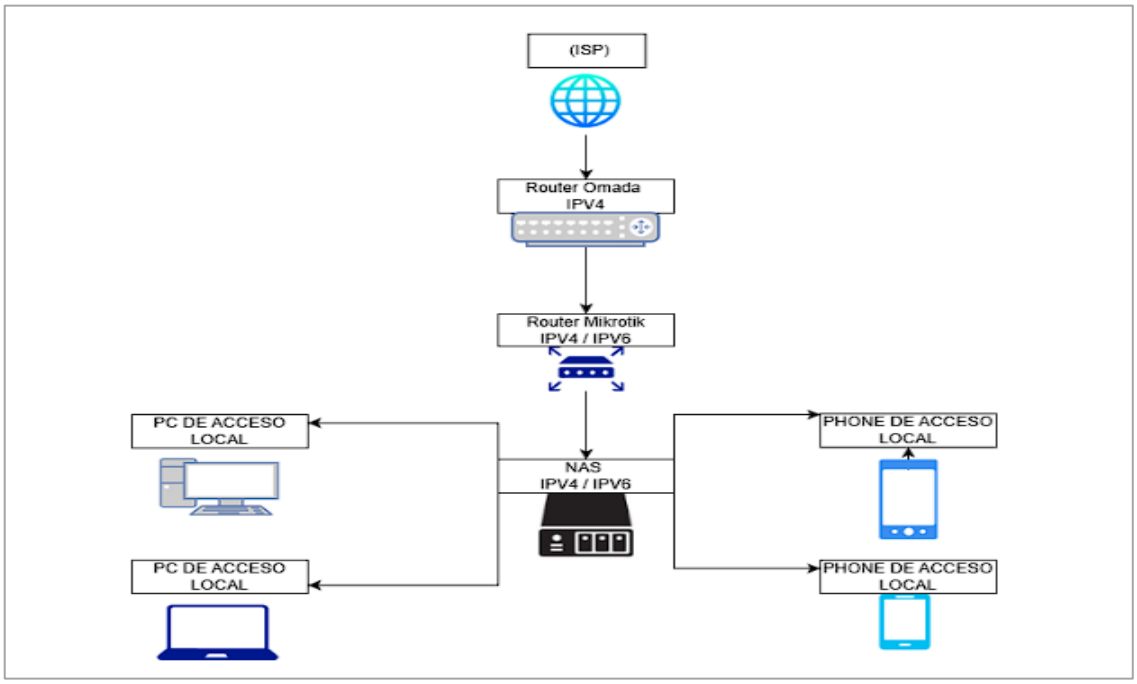


FIGURE 11 TOPOLOGÍA DE RED EN HIBRIDA

INFRAESTRUCTURA DE LA VPN DE CONEXION REMOTA AL NAS

La topología del NAS que se está integrando a una VPN ZeroTier, lo cual posibilita que las PCs y teléfonos accedan de manera segura desde una ubicación remota. Asi mismo, vincula aparatos de diferentes redes para intercambiar archivos y recursos de modo centralizado.

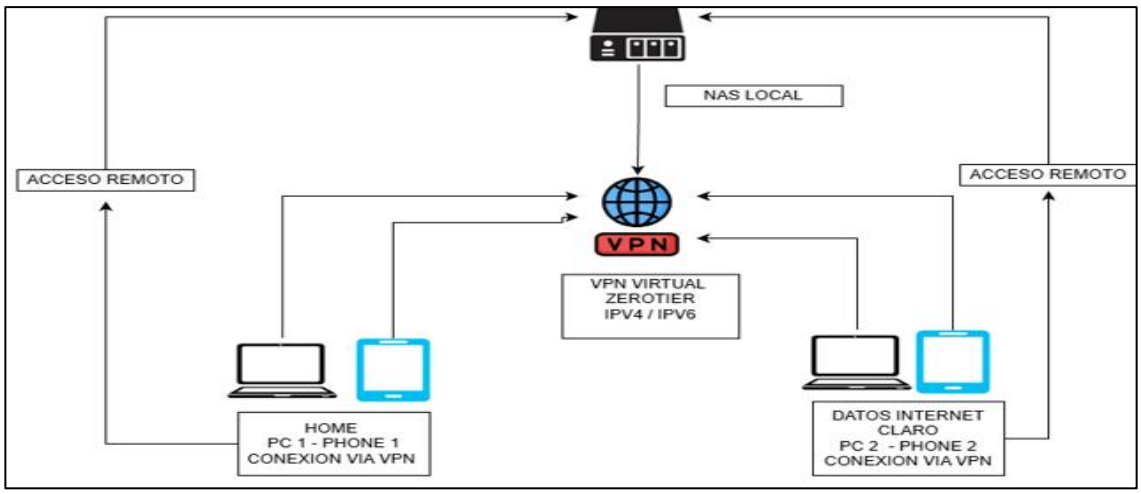


FIGURE 12 INFRAESTRUCTURA VPN DE CONEXION EXTERNA AL NAS

TOPOLOGIA VPN EN ESTRELLA

La imagen muestra la topología en estrella de VPN, en la que el NAS funciona como un nodo central en la red virtual ZeroTier. Los teléfonos y las computadoras personales se conectan directamente al NAS a través de VPN, lo que facilita un acceso centralizado y seguro.

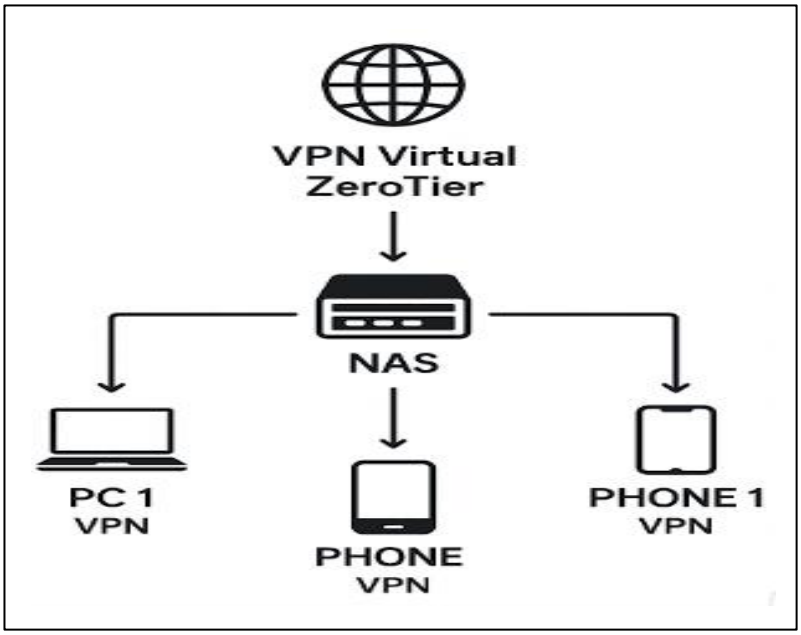


FIGURE 13 TOPOLOGIA ESTRELLA VPN

CONFIGURACIÓN DE RANGO DE IP VIRTUALES

La configuración del intervalo de direcciones IP indica cómo se establece el conjunto de direcciones IP que se otorgarán de forma automática a los dispositivos que estén conectados a la red del sistema NAS. Esta configuración es fundamental para crear una red privada organizada, donde cada dispositivo conectado sean nodos NAS, clientes lejanos o dispositivos de gestión obtenga una dirección única dentro del rango definido.

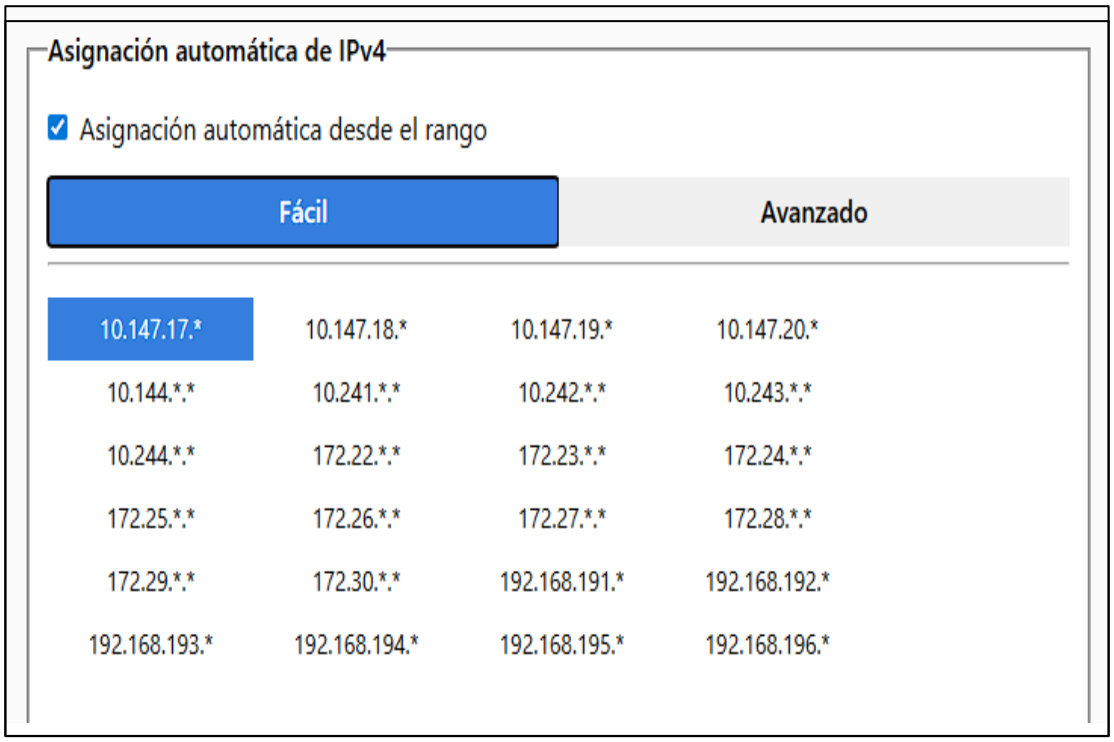


FIGURE 14 CONFIGURACIÓN DE RANGO DE IP EL CUAL ESTARIA ASIGNANDO A LOS DISPOSITIVOS CONECTADOS

IPV6 VIRTUAL

Esta capacidad asegura que todos los dispositivos, ya estén en la misma ubicación o en diferentes funcionen dentro de una red virtual segura y bien organizada sin requerir ajustes manuales. La asignación de IPv6 virtual nos permite tener direcciones únicas para cada servicio.

La asignación automática de IPv6 promueve la capacidad de expansión del sistema, ya que cada nuevo dispositivo que se conecta a la VPN obtiene una dirección virtual sin perturbar la red física que ya existe. Además, el uso de IPv6 mejora la administración de direcciones, disminuye el riesgo de conflictos y asegura una comunicación eficiente entre nodos dispersos. Esta función es esencial para preservar la seguridad, el orden y la interoperabilidad del sistema NAS en escenarios distribuidos y cambiantes.

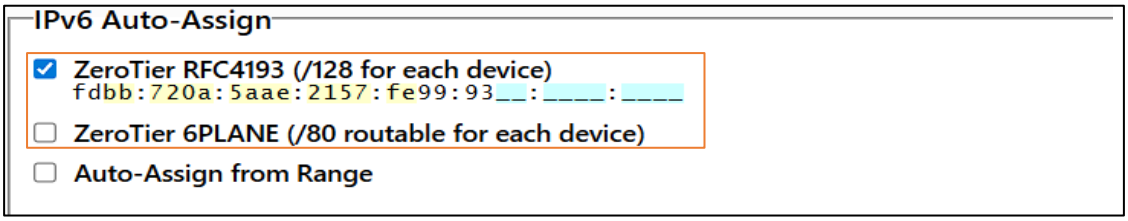


FIGURE 15 ASIGNACIÓN AUTOMÁTICA DE IPV6 VIRTUAL PARA CADA DISPOSITIVO VINCULADO A LA VPN

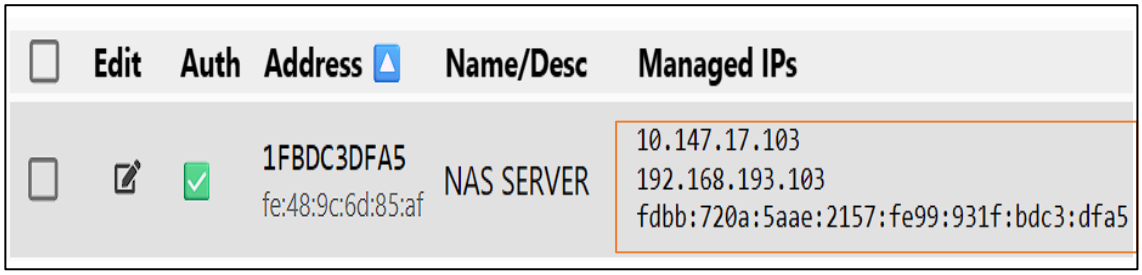


FIGURE 16 VERIFICACIÓN DE IPV6 VIRTUAL ASIGNADO AL NAS

ARREGLO RAID

Además, el uso de RAID 1 y copias de seguridad duplicadas proporcionan una alta disponibilidad y tolerancia a la falla, reduciendo el riesgo de pérdida de datos en el entorno de laboratorio, donde la continuidad de la acción es prioridad. Esta arquitectura también optimiza la gestión de usuarios, determina los permisos diferenciados y las políticas de acceso centralizado, promoviendo un control de activos digitales más eficientes.

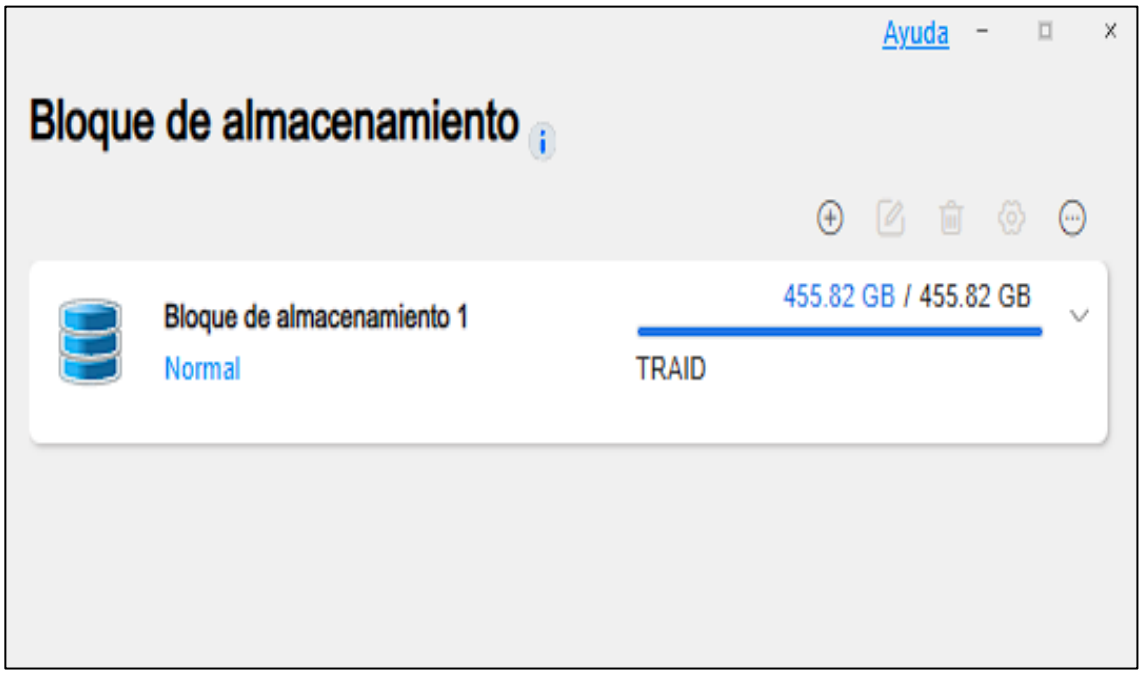


FIGURE 17 ARREGLO RAID AUTOMÁTICO DEL SISTEMA

CREACIÓN DE CARPETAS COMPARTIDAS

Los archivos almacenados en este sistema actúan como una biblioteca ordinaria: todos están reunidos, organizados en carpetas y pueden ser utilizados o cambiados, por otro lado, la nube utiliza protocolos de cifrado avanzados que protegen los datos tanto durante la transferencia como durante el almacenamiento, impidiendo el acceso no autorizado. Los administradores pueden configurar políticas automáticas de copia de seguridad, asignación de espacio y retención de datos y adaptar el sistema a las necesidades específicas de cada organización.

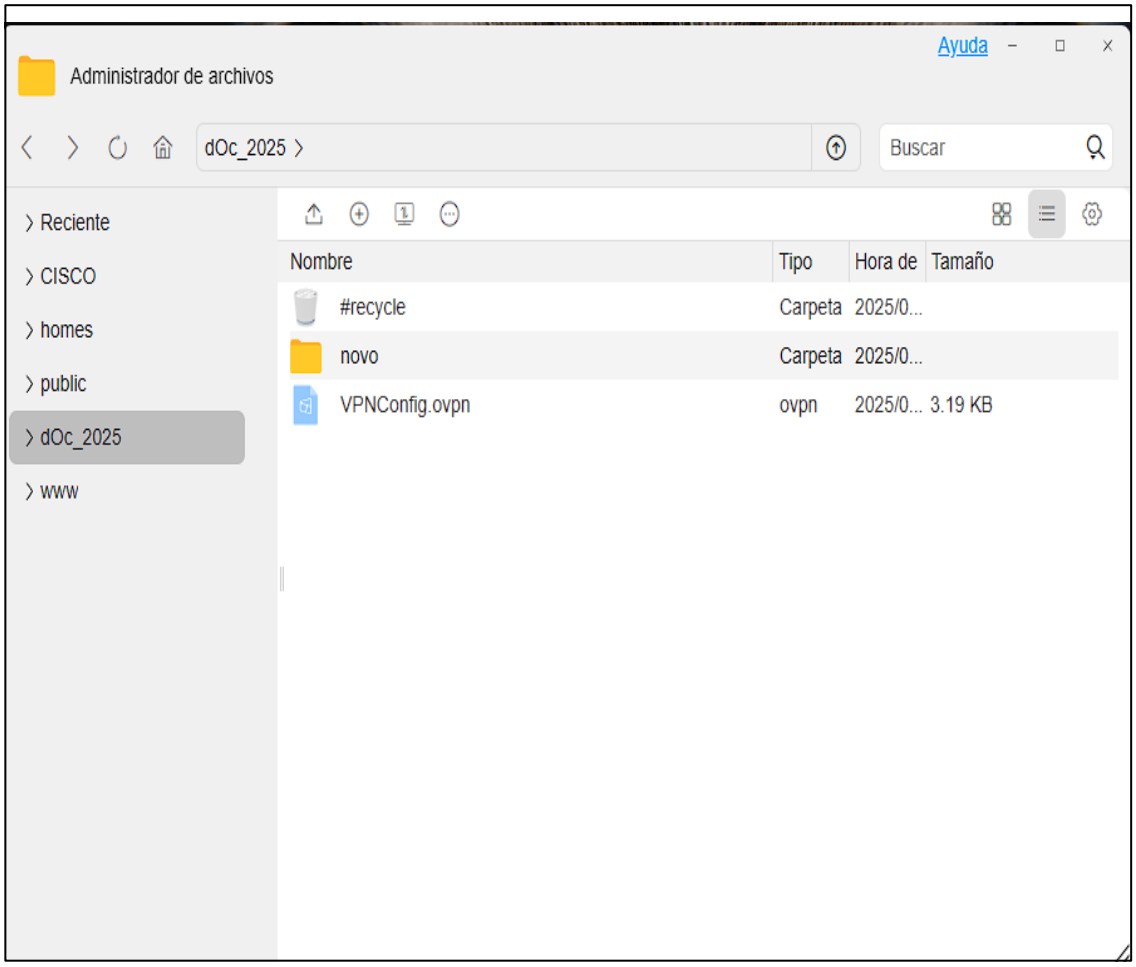


FIGURE 18 CREACIÓN DE CARPETAS COMPARTIDAS

EL CENTRO DE INSTALACIÓN DE SOFTWARE

TPK es el componente del sistema NAS que posibilita la incorporación de aplicaciones o extensiones no presentes en la tienda oficial del sistema operativo (TOS). Esta función resulta fundamental para mejorar las capacidades del NAS mediante el uso de software personalizado o de terceros, permitiendo la integración de herramientas específicas acorde a las preferencias del usuario.

Mediante este centro de instalación, los administradores tienen la opción de cargar manualmente paquetes. tpk, validar su autenticidad y realizar la instalación de manera segura. Esto permite conservar la adaptabilidad del sistema, ajustarlo a configuraciones especializadas y aprovechar innovaciones externas sin depender únicamente del listado oficial. Además, esta opción es esencial en entornos técnicos que demandan software avanzado o experimental que aún no se encuentra disponible en la tienda del proveedor.

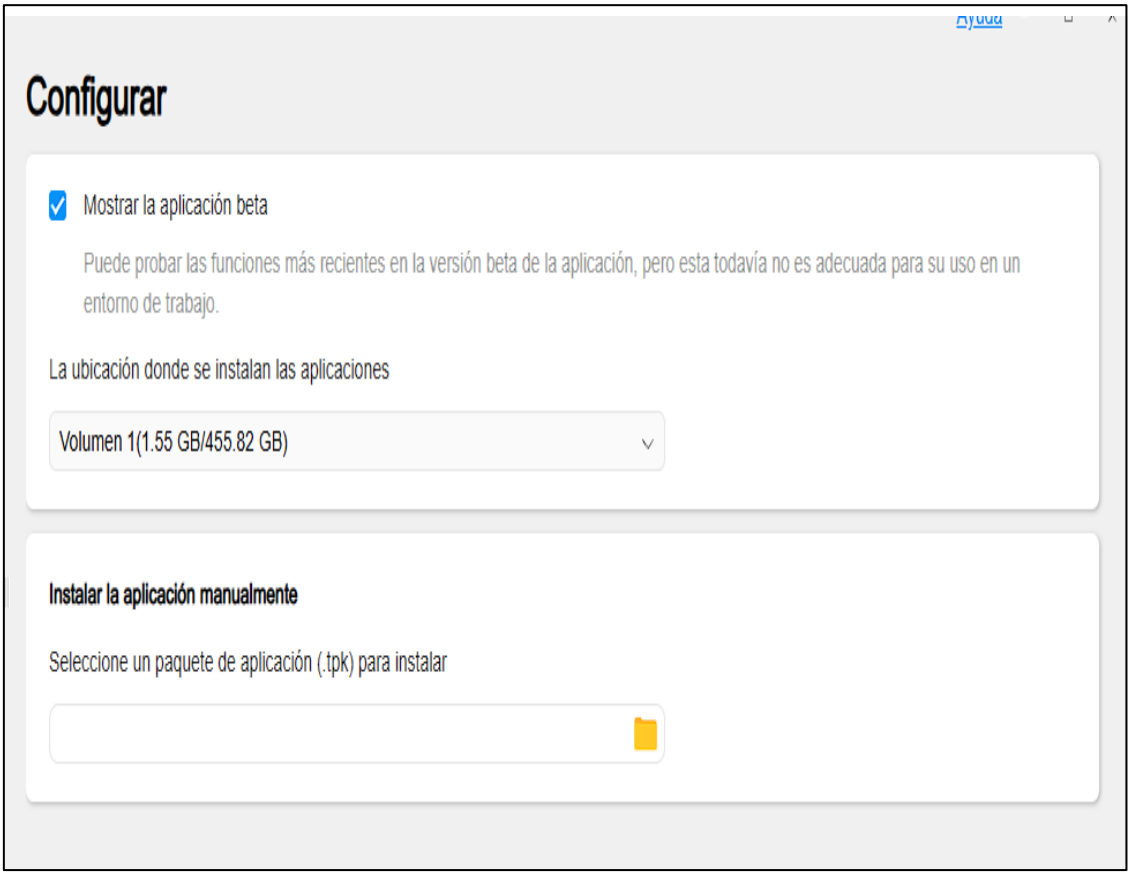


FIGURE 19 CENTRO DE INSTALACIÓN DE .TPK PARA SOFTWARE NO ENCONTRADOS EN LA TIENDA

CREACIÓN DE SCRIPT EN GOOGLE APPS SCRIPT

La configuración se ha realizado para sincronizar automáticamente en un correo a labcisco63@gmail.com en la cuenta: Google Apps Script fue desarrollado un script que establece correos electrónicos entrantes de omada@email.tp-link.com obtiene archivos adjuntos y se almacenó automáticamente en una carpeta llamada Google Drive; Cloudync se configuró luego para sincronizar esta carpeta de accionamiento con una carpeta local, lo que permite que los archivos alcancen el almacenamiento local sin intervención manual, todos funcionan continuamente y automatizados. En esta se usan las credenciales para identificar del correo emisor y correo receptor para la ejecución de la script creada y la carpeta adecuada para la recepción de archivos y logs.

```
function saveOmadaAttachmentsToDrive() {
  var senderEmail = "omada@email.tp-link.com";
  var folderName = "OMADA";

  // Buscar correos no leídos del remitente específico
  var threads = GmailApp.search('from:' + senderEmail + ' is:unread');
  var folder = DriveApp.getFoldersByName(folderName).hasNext() ? DriveApp.getFoldersByName(folderName).next() : DriveApp.
  createFolder(folderName);

  for (var i = 0; i < threads.length; i++) {
    var messages = threads[i].getMessages();
    for (var j = 0; j < messages.length; j++) {
      var message = messages[j];
      var attachments = message.getAttachments();

      for (var k = 0; k < attachments.length; k++) {
        var file = attachments[k];
        folder.createFile(file);
      }

      // Marcar el mensaje como leído después de guardar los adjuntos
      message.markRead();
    }
  }
}
```

FIGURE 20 SCRIPT ASIGNADO PARA EL ALMACEN DE ARCHIVOS MEDIANTE CORREOS A GOOGLE DRIVE

ENLACE DE LA CARPETA ESPECIFICA A DRIVE PARA TRANSFERENCIA DE LOGS

Entre la carpeta de la revista local (/volumen1/syslog) y la carpeta Google Drive (/OMADA) se han sincronizado. La tarea llamada Task_1 está activa y configurada para descargar solo cambia desde la nube. Se indican parámetros como un filtro, ancho de banda ilimitado y una política de conflicto (renombrar archivos). Esta tarea está activa y configurada específicamente para descargar solo cambios desde la nube, asegurando que el contenido local siempre esté actualizado con la última versión disponible en Google Drive sin sobrescribir ni eliminar archivos locales que no están en la nube. Su configuración prioriza la seguridad de los datos, evita la sobrescritura y mantiene las versiones al mismo tiempo. La configuración incluye alertas automáticas de errores o conflictos para que puedas reaccionar rápidamente y evitar la pérdida de información. Se garantiza la compatibilidad con futuras innovaciones de servicios en la nube, manteniendo la integridad de los datos y la disponibilidad a largo plazo, además de una instancia de cada minuto para que se siga ejecutando con normalidad, el mismo se encarga de realizar un análisis si el proceso comienza a fallar y dar el aviso correspondiente.

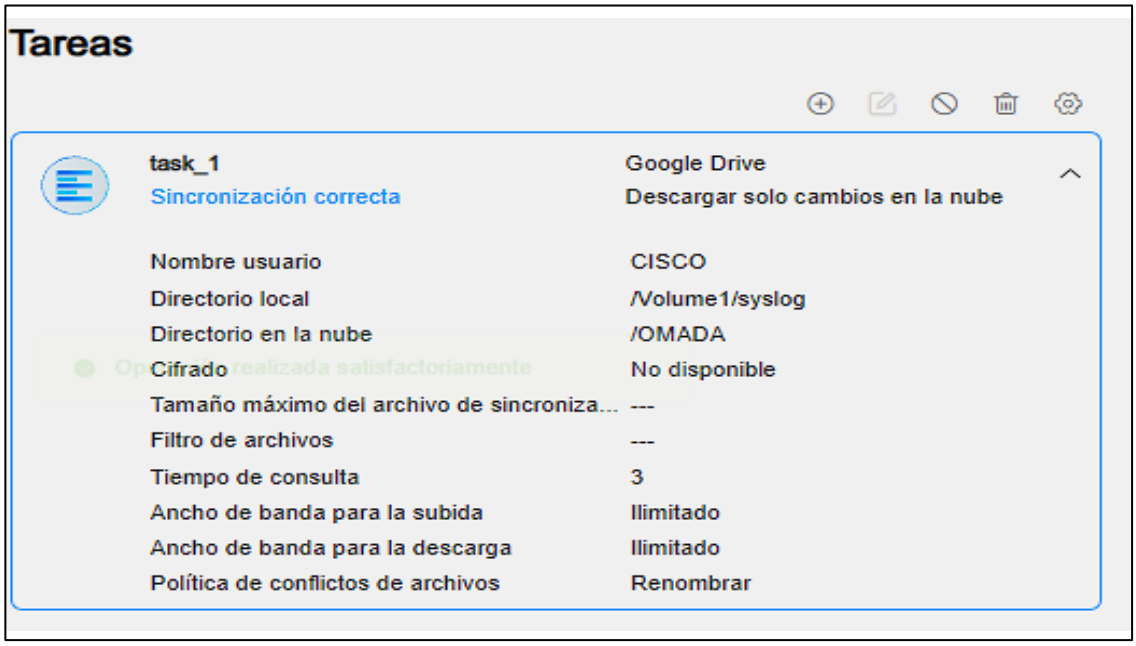


FIGURE 21 FIJAMOS LA CARPETA DE LOGS PARA QUE SE SINCRONICE CON UNA CARPETA EN LA NUBE DRIVE

CREACIÓN DE CARPETA PARA DIRECCIONES DE ARCHIVOS LOG

hemos creado una carpeta específica para guardar los logs que se generen dentro del Router Omada quien se encargara de enviarme los logs en archivos csv o en formatos pdf, para que queden almacenados dentro del NAS

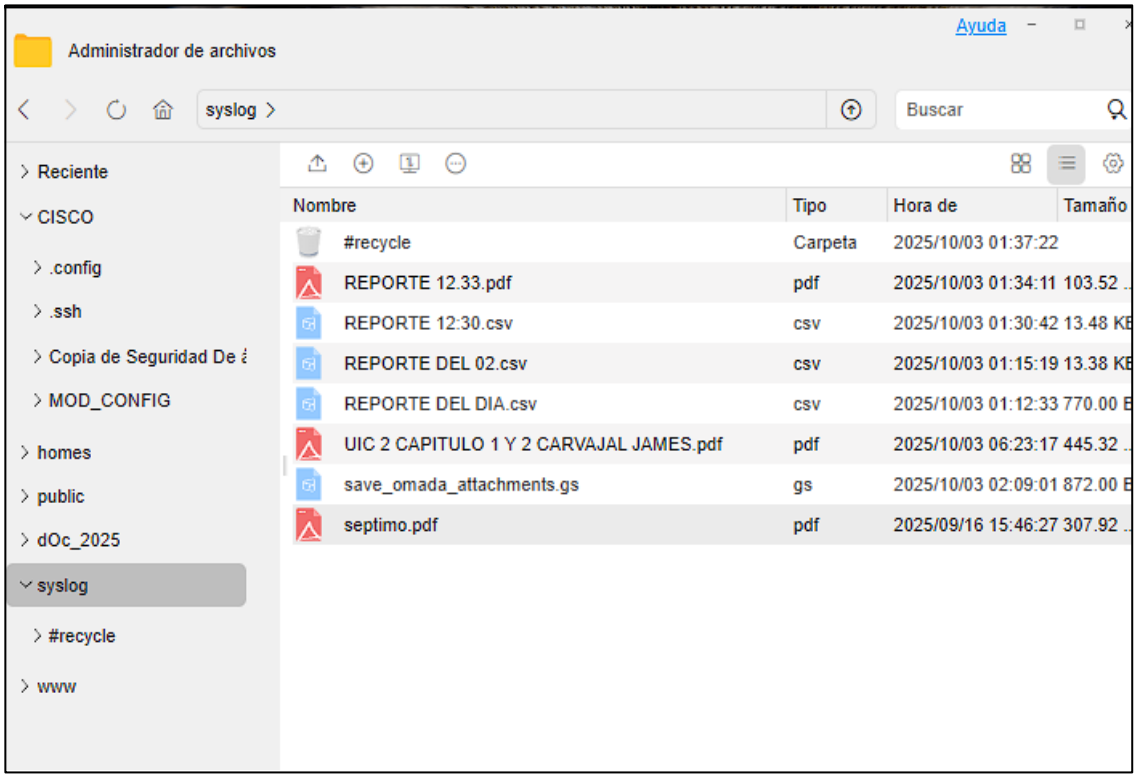


FIGURE 22 CREAMOS UNA CARPETA DE LOGS RECIBIDOS

3.2.3 FASE 3: IMPLEMENTACIÓN

En la Tercera Fase el sistema se lanza, desde la instalación física del Mini NAS en el laboratorio y su conexión con la red institucional, seguida de una configuración de red con direccionamiento IP estático y servicios básicos; Los usuarios y las carpetas compartidas se crean otorgando permisos al nivel de acceso; Los mecanismos de seguridad se activan utilizando copias de seguridad automáticas y protocolos de protección; El acceso remoto seguro se activa utilizando VPN para realizar conexiones externas confiables, y finalmente se realizan pruebas funcionales para verificar si el sistema funciona correctamente y cumple con el propósito de la fase de diseño.

GESTIÓN DE USUARIOS Y PERMISOS

Se centra en la creación de perfiles individuales o grupales para el acceso al NAS, las carpetas compartidas están configuradas con permisos de lectura, escritura o administrativos, asegurando que cada usuario solo pueda procesar información similar que fortalezca la seguridad y la protección de los datos críticos. Además, este sistema facilita la creación de grupos de trabajo, lo que permite una autorización colectiva eficiente y reduce la carga administrativa. Los administradores pueden cambiar o revocar el acceso en tiempo real, monitorear la actividad del usuario y establecer políticas de autenticación sólidas, como contraseñas seguras o autenticación de dos factores.

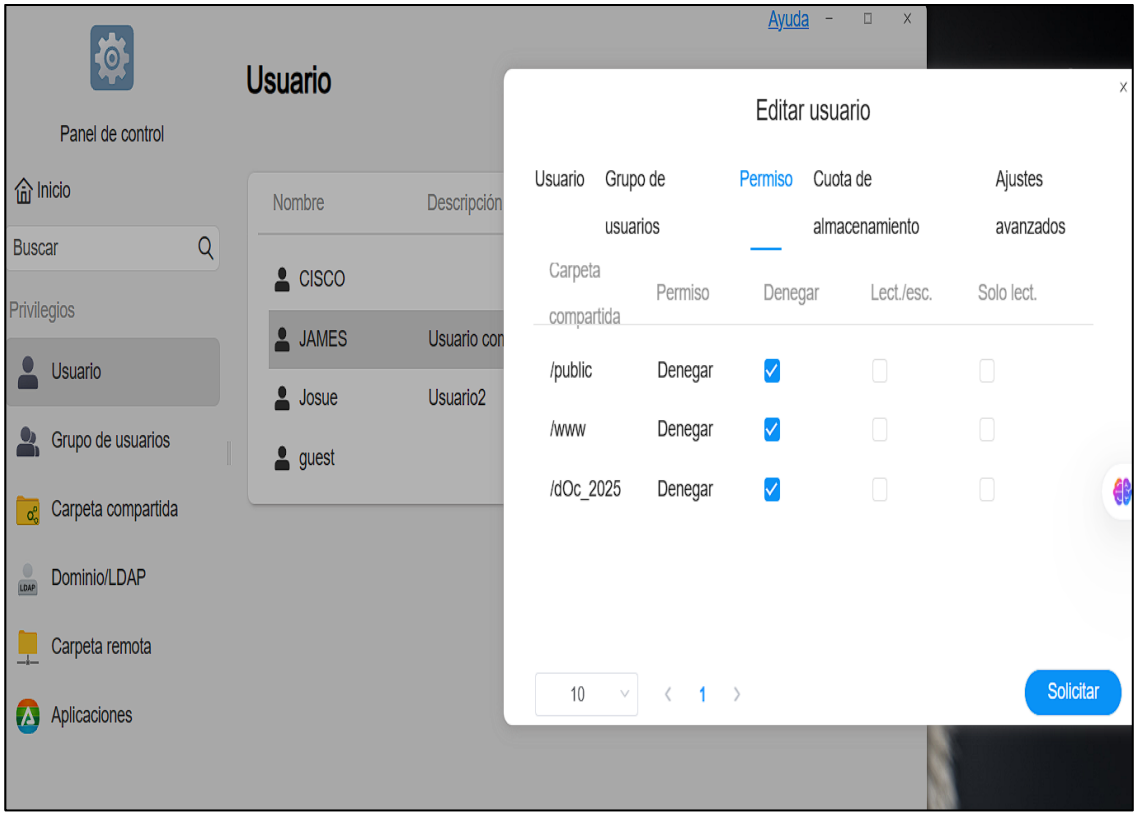


FIGURE 23 PERMISO PARA ACCESO DE CARPETAS COMPARTIDAS A USUARIOS O ADMINISTRADORES

AJUSTE DE RED PARA USO LOCAL DEL DISPOSITIVO

La personalización de la red para el uso tópico de NAS significa una configuración de conexión de equipo adecuada en una red de casa u oficina, lo que permite que las computadoras y otros dispositivos accedan a los archivos almacenados de forma rápida y segura sin confiar en Internet. Esto incluye una asignación de red, permisos de acceso y comunicación con otros dispositivos es estable y confiable.

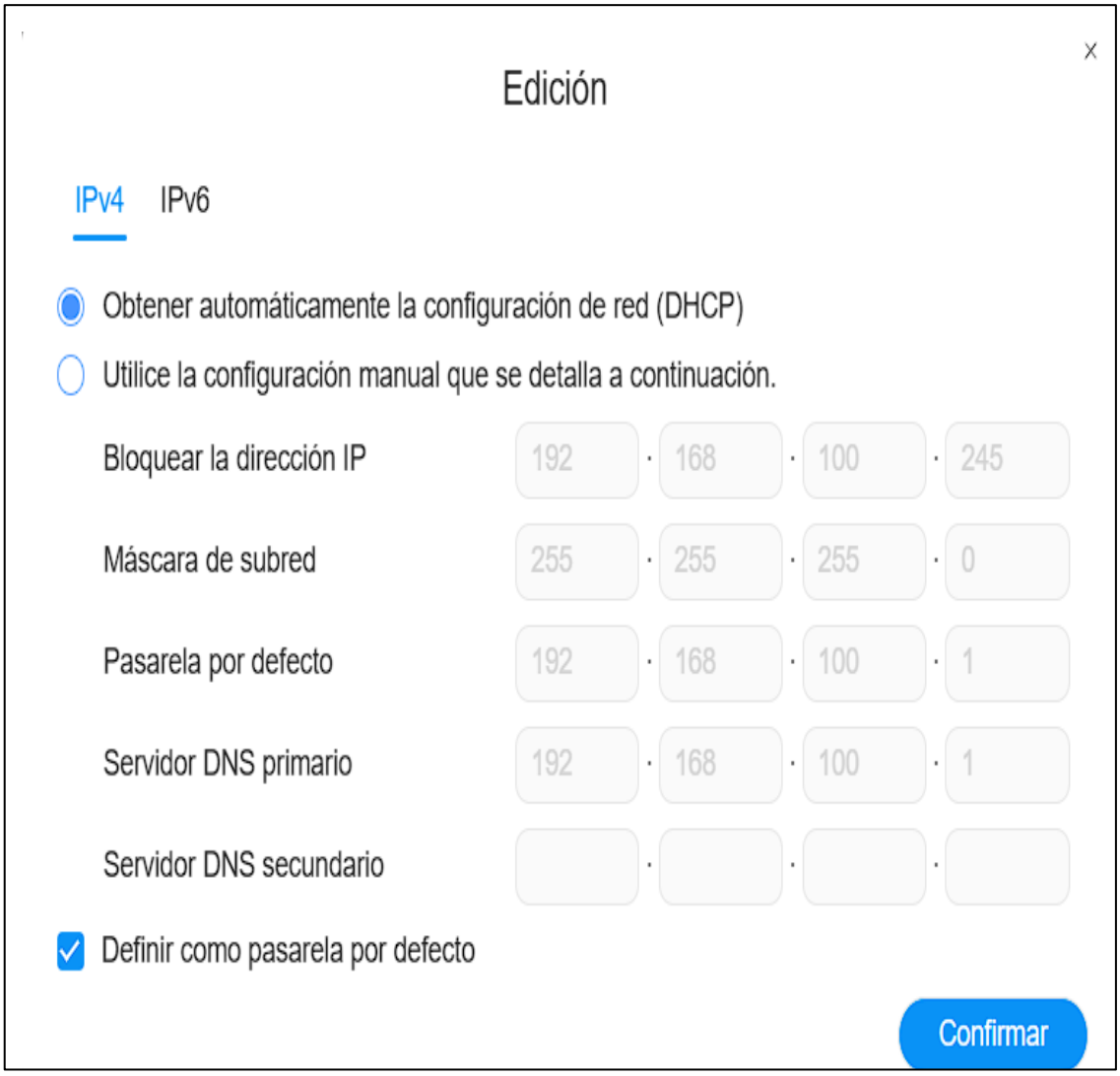


FIGURE 24 AJUSTE DE RED POR DHCP PARA USO LOCAL

PROTECCIÓN Y COPIA DE LA INFORMACIÓN ALMACENADA

El resguardo y la duplicación de la información almacenada comprenden el establecimiento de acciones que mantienen los datos seguros frente a errores, accesos no autorizados o fallas del sistema al generar copias de seguridad que posibiliten recuperar la información si se pierde, asegurando así que los archivos relevantes siempre se encuentren protegidos y disponibles.

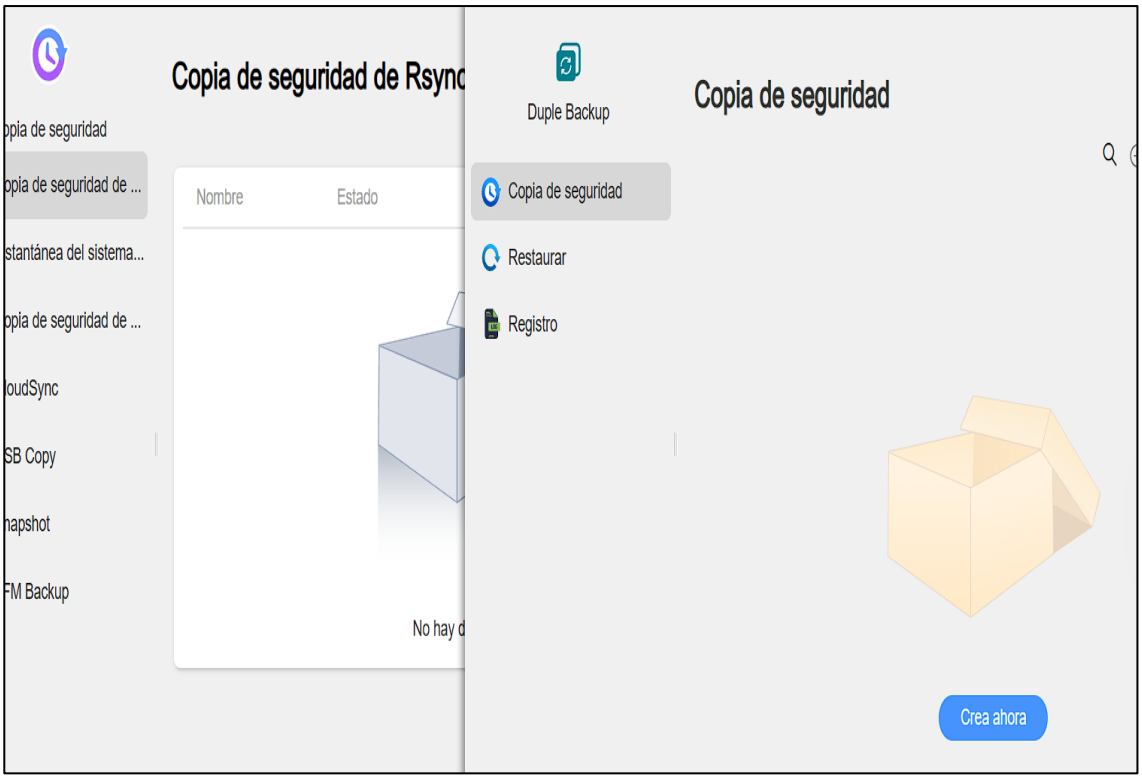


FIGURE 25 SISTEMA DE RESPALDO DE DATOS ALMACENADOS

SINCRONISACIÓN DE ARCHIVOS CON EL SOFTWARE CLOUDSYNC

Esto garantiza que siempre esté trabajando en su última versión de sus documentos copiándolos manualmente.

La imagen muestra la interfaz del software CloudSync durante una tarea de sincronización bidireccional activa con Google Drive. En la sección "Tareas", puedes ver Upload_0101 en progreso con 19 elementos sincronizados. La velocidad de carga es de 1,76 MB/s, mientras que la velocidad de descarga es de 0 B/s, lo que indica que solo se envían datos a la nube. Este panel confirma que la sincronización funciona correctamente y le permite monitorear el progreso en tiempo real.

CloudSync no solo actualiza archivos en tiempo real, sino que también garantiza la integridad y disponibilidad de la información mediante la sincronización bidireccional con servicios en la nube como Google Drive. Esta herramienta incluye funciones avanzadas como reversión, copia de seguridad automática y monitoreo de conflictos, lo que reduce el riesgo de pérdida de datos. Además, su capacidad de ejecutarse continuamente sin intervención manual garantiza que los usuarios siempre estén trabajando con la última versión de sus documentos, optimizando la productividad y la seguridad.

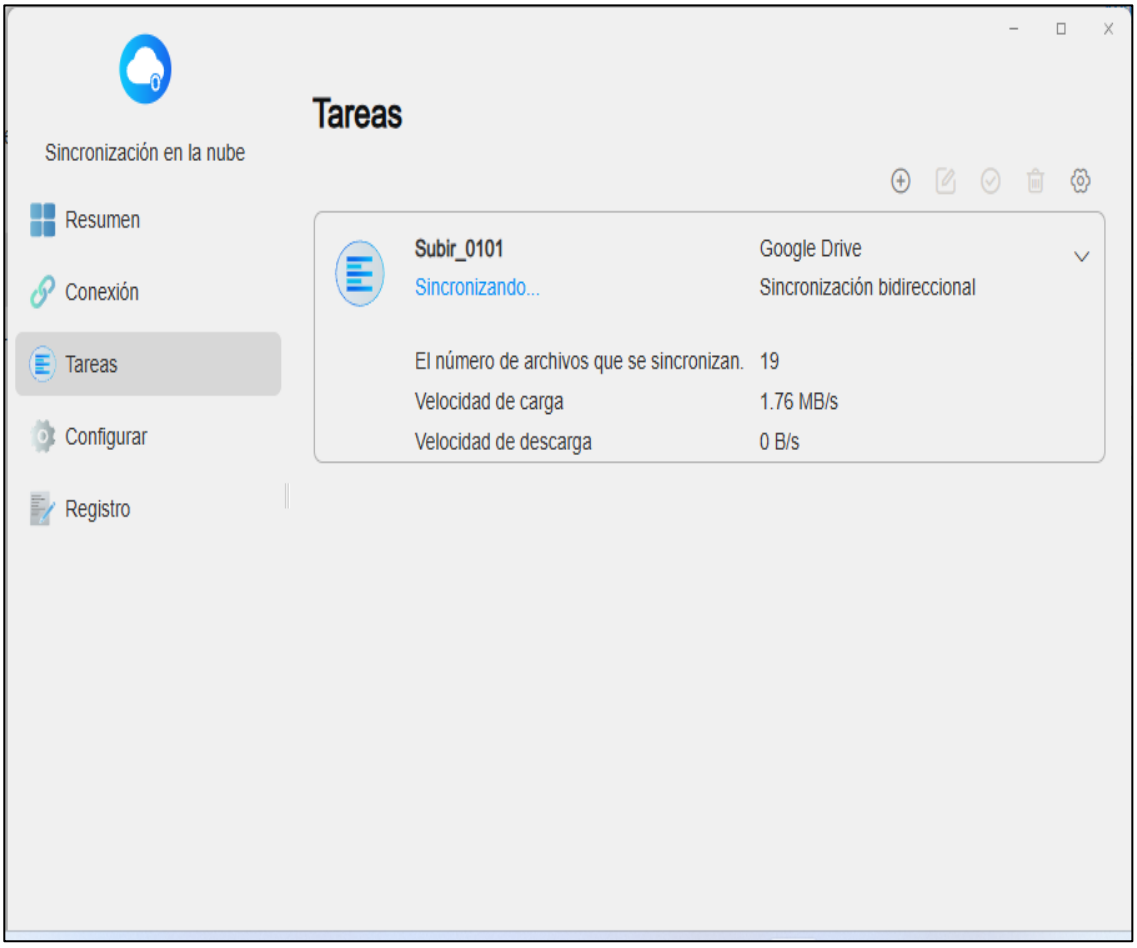


FIGURE 26 SINCRONIZACIÓN COMPLETA A GOOGLE DRIVE PARA ACTUALIZACIONES DE ARCHIVOS

LLEGADA DE ARCHIVO MEDIANTE CORREO(GMAIL) DESIGNADO AL NAS ASIGNADO CON EL SCRIPT

En este punto se envia el archivo desde el Router Omada Hasta el correo asignado al NAS, asi este podria recibir el archivo y se enviaria automáticamente al Google drive y se vincularia con la carpeta asignada en el NAS que se configuró con el software Cloudsync. Este procedimiento automatiza la transferencia de archivos desde el enrutador Omada al sistema NAS mediante un flujo seguro y eficiente. Primero, el enrutador genera un informe en formato PDF o CSV y lo envía al correo electrónico especificado (por ejemplo, labcisco63@gmail.com). Un script desarrollado en Google Apps Script procesa un correo electrónico entrante, extrae el archivo adjunto y lo guarda automáticamente en una carpeta específica de Google Drive. Luego, la aplicación CloudSync sincroniza esta carpeta con el NAS, asegurando que los archivos lleguen al almacenamiento local sin intervención manual. Este mecanismo asegura la continuidad del negocio, reduce el riesgo de pérdida de información y permite actualizar los registros del laboratorio en tiempo real.

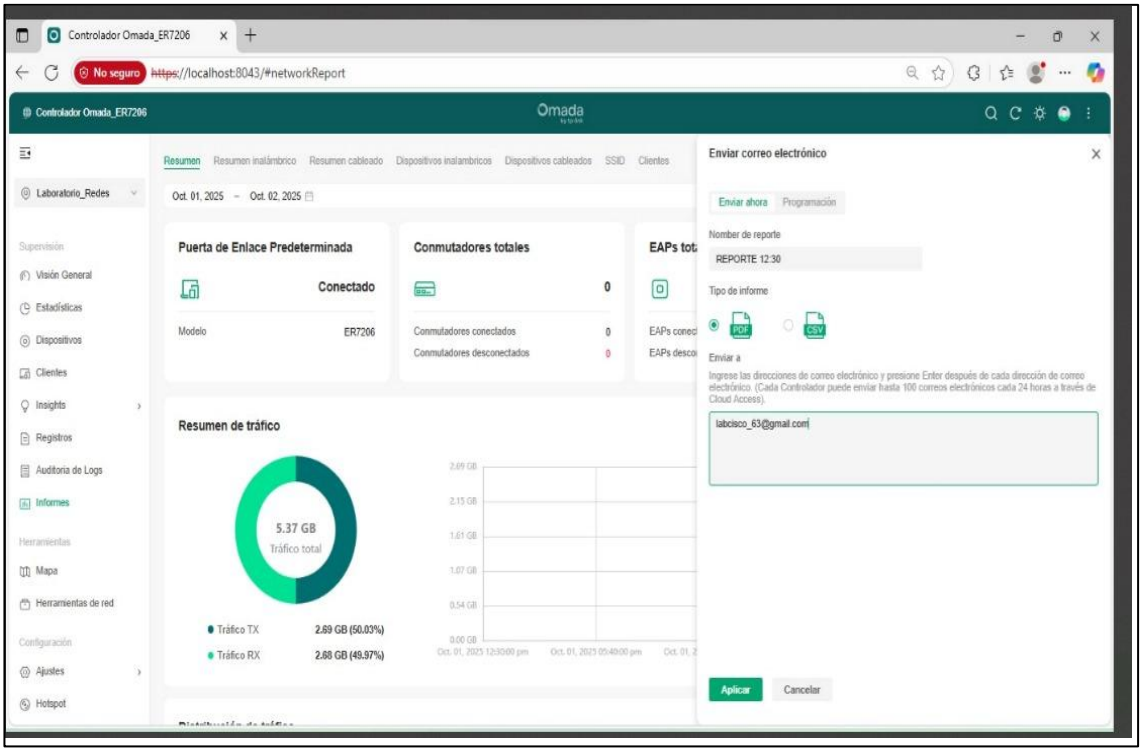


FIGURE 27 ENVIÓ DESDE EL ROUTER OMADA EL ARCHIVO CSV O PDF , HACIA EL CORREO CONFIGURADO

NOTIFICACION DE CORREO ENTRANTE DEL ROUTER OMADA

Llegada de archivo del router omada hacia el drive para que el archivo se envié a la carpeta designada del Drive y se guarde correctamente mediante el script creado anteriormente, y se pueda ejecutar el propósito de el enlace espejo al NAS mediante CloudSync.

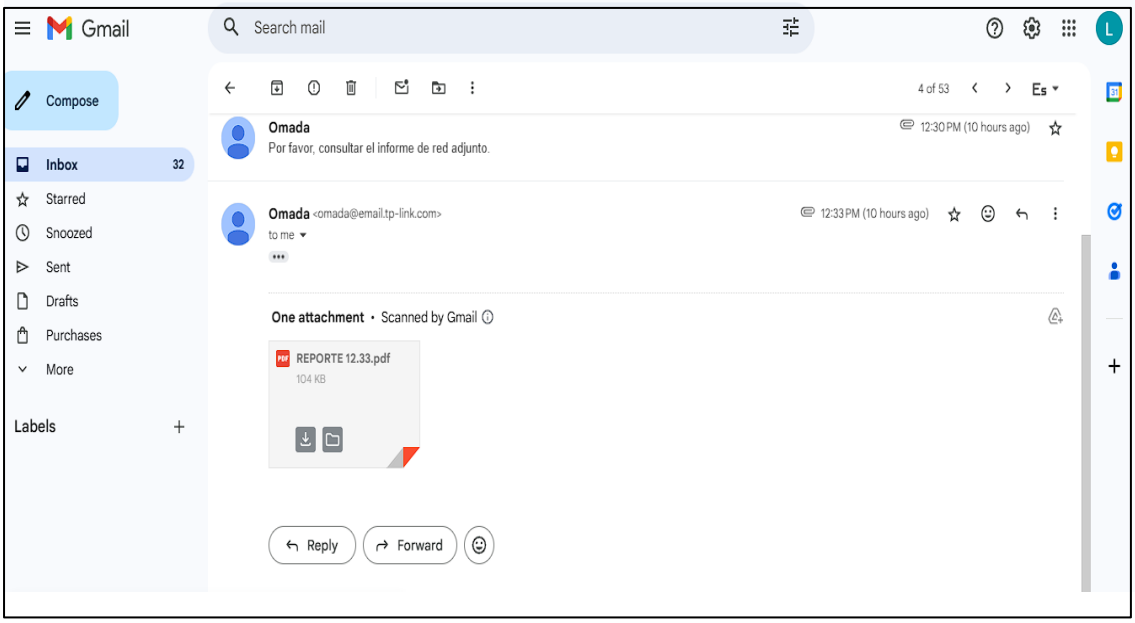


FIGURE 28 LLEGADA DEL CORREO Y VERIFICACIÓN DE UN ARCHIVO PDF DESDE EL ROUTER OMADA

CONFIGURACION DE EJECUCIÓN DEL SCRIPT

Aquí se configura el intervalo de tiempo de minutos que se ejecutara el script, para el envio de archivo por correo a la carpeta designada al drive

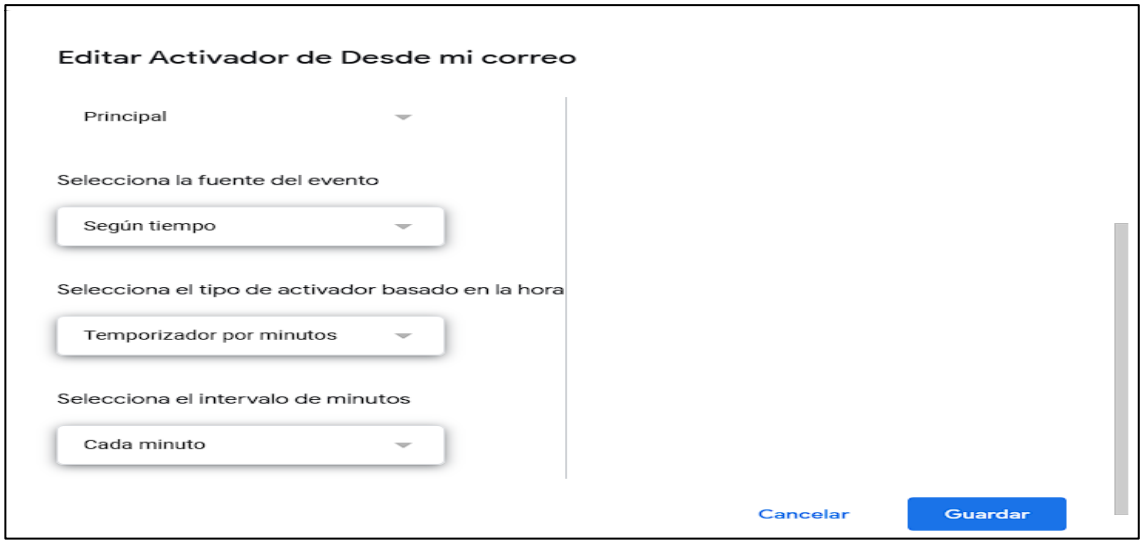


FIGURE 29 EDICIÓN DE INTERVALO DE TIEMPO DE LLEGADA DE ARCHIVOS AL DRIVE MEDIANTE EL SCRIPT CREADO

INSTALACIÓN DE SOFTWARE PARA ACCESO REMOTO SEGURO

La instalación del cliente de ZeroTier se realiza directamente al Mini NAS a través de su centro de aplicaciones o línea de comandos, donde se une a la red virtual utilizando la ID de red generada por Zerotier. Luego se permite el centro NAS de la administración Zerotier, se definen las reglas de tráfico y se asigna la dirección IP virtual correspondiente. Esta configuración garantiza que el tráfico entre usuarios externos y NAS sea extremadamente extrovertido y que solo los dispositivos autorizados puedan crear comunicación.

FIGURE 30 SOFTWARE VIA WEB PARA RED VIRTUAL DE CONFIGURACIÓN VPN

EL SOFTWARE ZEROTIER EN EL NAS

En un NAS permite la creación de una red definida por software (SD-WAN) dentro del mismo. La aplicación ayuda a establecer una red privada virtual entre varios dispositivos, eliminando la necesidad de complejas configuraciones de redes físicas.

Con la instalación de ZeroTier en el NAS, se crea una conexión directa entre dispositivos remotos como computadoras portátiles, servidores o nodos NAS adicionales, simulando una red local a pesar de estar situados en diferentes lugares. Esto posibilita la transferencia de archivos, la realización de copias de seguridad y la gestión del sistema de manera segura y efectiva, utilizando el cifrado incorporado y la versatilidad de la plataforma. Asimismo, esta solución incrementa la capacidad de expansión del sistema, dado que se pueden añadir nuevos dispositivos fácilmente sin modificar la infraestructura actual.

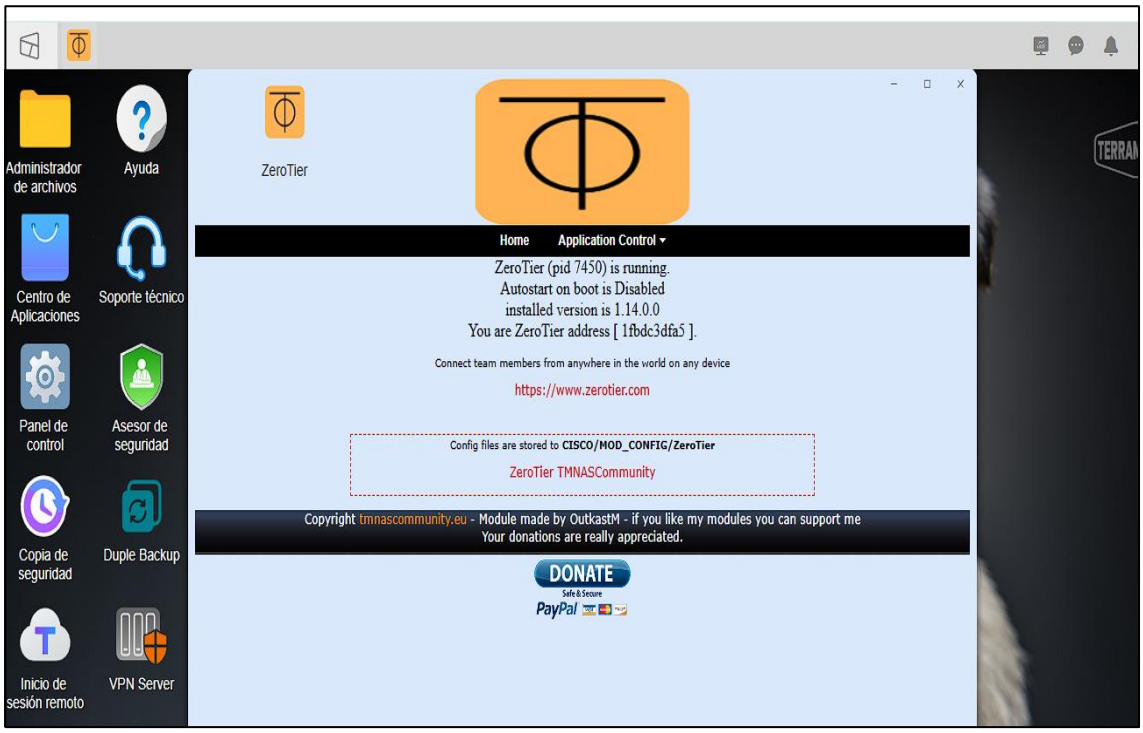


FIGURE 31 SOFTWARE ZEROTIER INSTALADO EN NAS PARA VINCULACIÓN DE DISPOSITIVO A LA RED VIRTUAL

CONEXIÓN POR EL SERVICIO PUTTY VIA IPV6

A través de SSH y asociación por ID y dirección IP describe el método por el cual un administrador o un usuario con permiso puede acceder al sistema NAS de manera remota y segura usando el protocolo SSH. Esta conexión se efectúa mediante PuTTY, una utilidad comúnmente empleada para acceder a dispositivos a través de terminales seguros.

En este proceso, cada aparato en la red privada virtual (VPN) es reconocido por un ID exclusivo y una dirección IP virtual, lo que facilita una interacción directa y segura entre el cliente y el NAS. Es relevante mencionar que este procedimiento de asociación se realiza únicamente una vez, con el fin de incorporar el NAS a la red virtual establecida por ZeroTier. Después de ser asociado, el NAS queda permanentemente conectado a la red, lo que permite su gestión remota y segura sin necesidad de repetir el procedimiento.

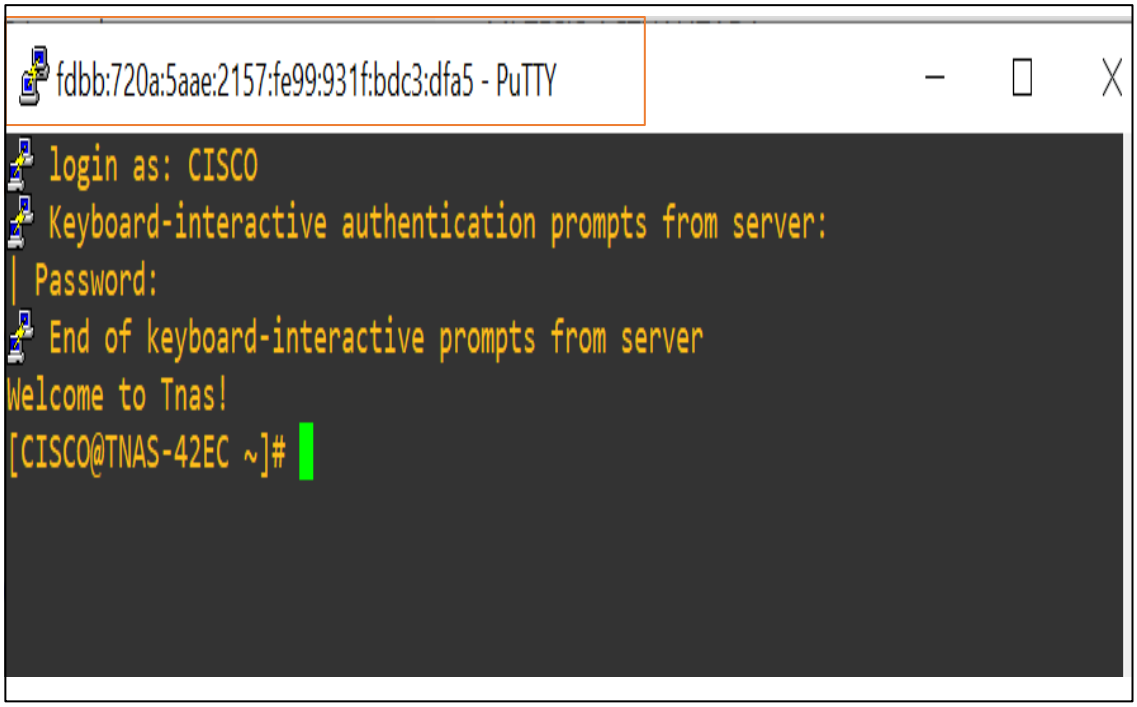


FIGURE 32 ACCESO POR PUTTY SERVICIO SSH IPV6

ESTABLECIMIENTO DE LA DIRECCIÓN IP

En el rango 10. 147. 17. 103 y la comprobación en línea del dispositivo ilustran el procedimiento para asignar una dirección IP virtual concreta a un dispositivo que está enlazado a la red privada virtual (VPN), específicamente dentro del rango señalado por ZeroTier. Esta dirección facilita la identificación única del dispositivo dentro de la red virtual, lo que permite la interacción con otros nodos y servicios del sistema NAS.

Luego de la asignación de la dirección IP, el sistema procede a una verificación del estado en línea del dispositivo, asegurando que esté correctamente conectado y funcionando dentro de la red. Esta verificación es esencial para garantizar que el dispositivo pueda participar en la transferencia segura de información, acceder a recursos compartidos y ser gestionado de forma remota. Además, tal configuración ayuda a mantener una red organizada, segura y que se pueda expandir, donde cada dispositivo conectado está claramente identificado y controlado.

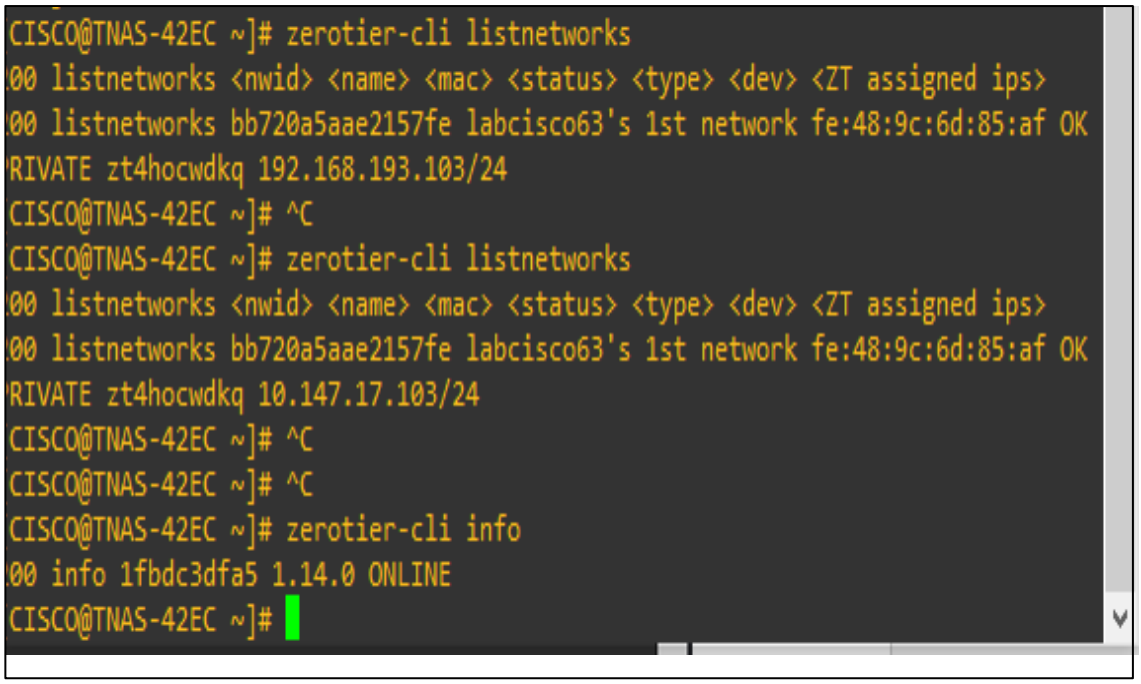


FIGURE 33 CONFIGURACIÓN DE IP DENTRO DEL RANGO 10.147.17.103 Y VERIFICACIÓN DE EN LÍNEA DEL DISPOSITIVO

ESTABLECIMIENTO DE CONEXIÓN VPN (ZEROTIER) CON DISPOSITIVO MOVIL

En Android usando datos móviles hacia el NAS ilustra cómo un teléfono Android puede crear una conexión protegida con el sistema NAS a través de la red privada virtual de ZeroTier. Esta vinculación se efectúa mediante la red móvil, sin requerir una conexión a una red Wi-Fi local, lo que posibilita el acceso remoto desde cualquier ubicación que tenga cobertura de datos. Después de que el dispositivo Android se conecta a la red virtual con su ID y dirección IP proporcionada por ZeroTier, tiene la capacidad de interactuar con el NAS como si estuviese en la misma red local. Esto incluye la posibilidad de acceder a documentos, hacer copias de seguridad, supervisar el sistema o llevar a cabo tareas administrativas, todo ello de manera segura y cifrada. Esta característica es especialmente valiosa para aquellos usuarios que requieren movilidad y acceso continuo a su información, sin poner en riesgo la seguridad ni tener que lidiar con configuraciones de red complejas. La aplicación también se puede instalar y utilizar desde un dispositivo iPhone, proporcionando la autorización adecuada para su funcionamiento. Esto permite que la plataforma sea totalmente accesible tanto para los usuarios de dispositivos Android como Apple, garantizando una experiencia inclusiva y universal. De esta forma, su uso no se limita a una única marca o sistema operativo, sino que con carácter general se aplica a todos los usuarios sin distinción ni limitación.

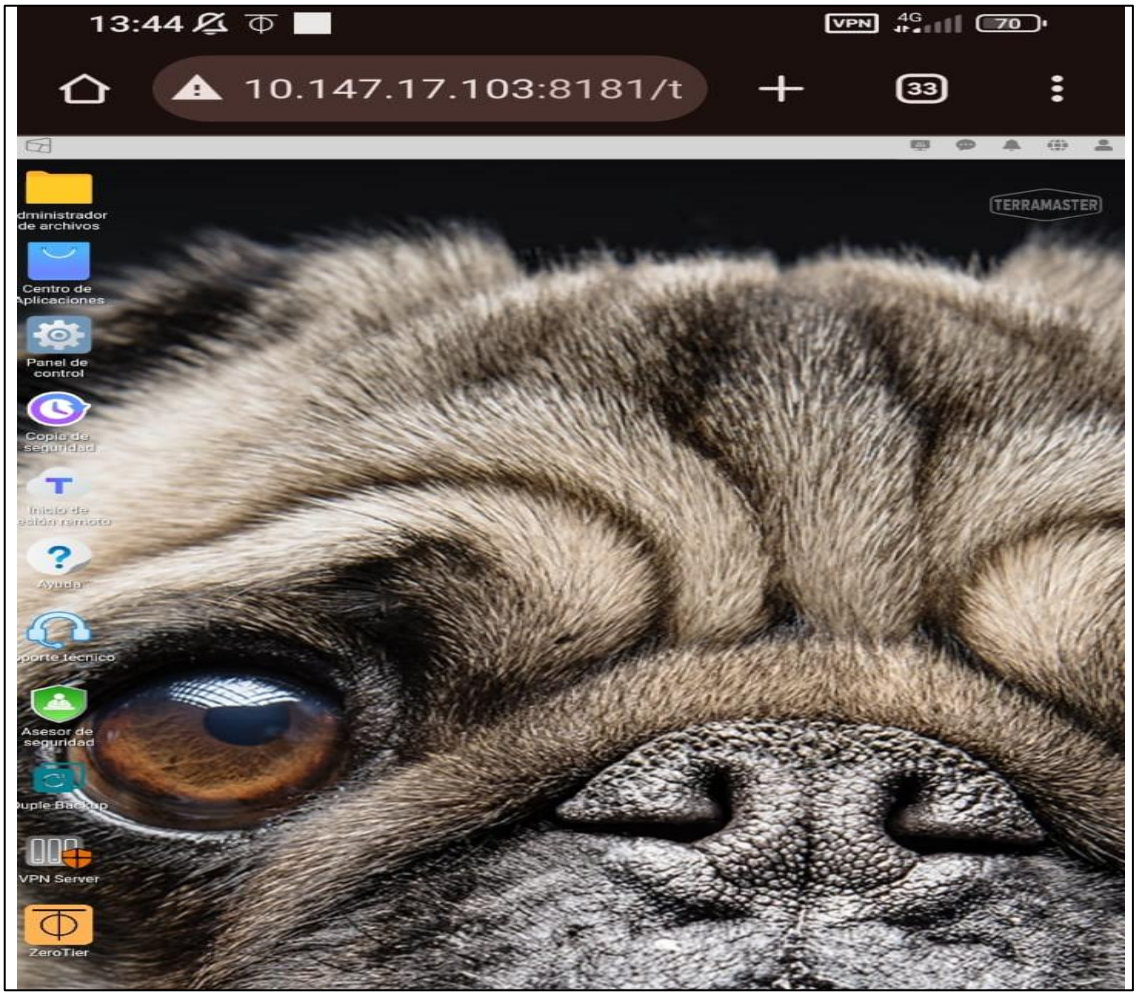


FIGURE 34 CONEXIÓN VPN (ZEROTIER) VIA ANDROID CON DATOS MOBILES HACIA EL NAS

USUARIO QUE NO PRIVILEGIADO DE ADMINISTRADOR

Ejemplifica cómo un ordenador de escritorio o portátil se puede vincular al sistema NAS a través de la red privada virtual establecida con ZeroTier, utilizando la misma dirección IP virtual que fue asignada al NAS previamente. En este escenario, el acceso es proporcionado a un usuario diferente al administrador, lo que ilustra la habilidad del sistema para manejar múltiples cuentas con diferentes niveles de acceso.

Esta conexión habilita a los usuarios con permisos, que no son administradores, a interactuar con el NAS de manera segura y a distancia, permitiendo el acceso a los recursos que les han sido designados de acuerdo a su función. Gracias a la plataforma de ZeroTier, la comunicación se mantiene segura y confiable, emulando una red local entre dispositivos dispersos. Esta característica es esencial en entornos colaborativos donde varios usuarios deben tener acceso al sistema al mismo tiempo sin comprometer la seguridad o integridad de la información.

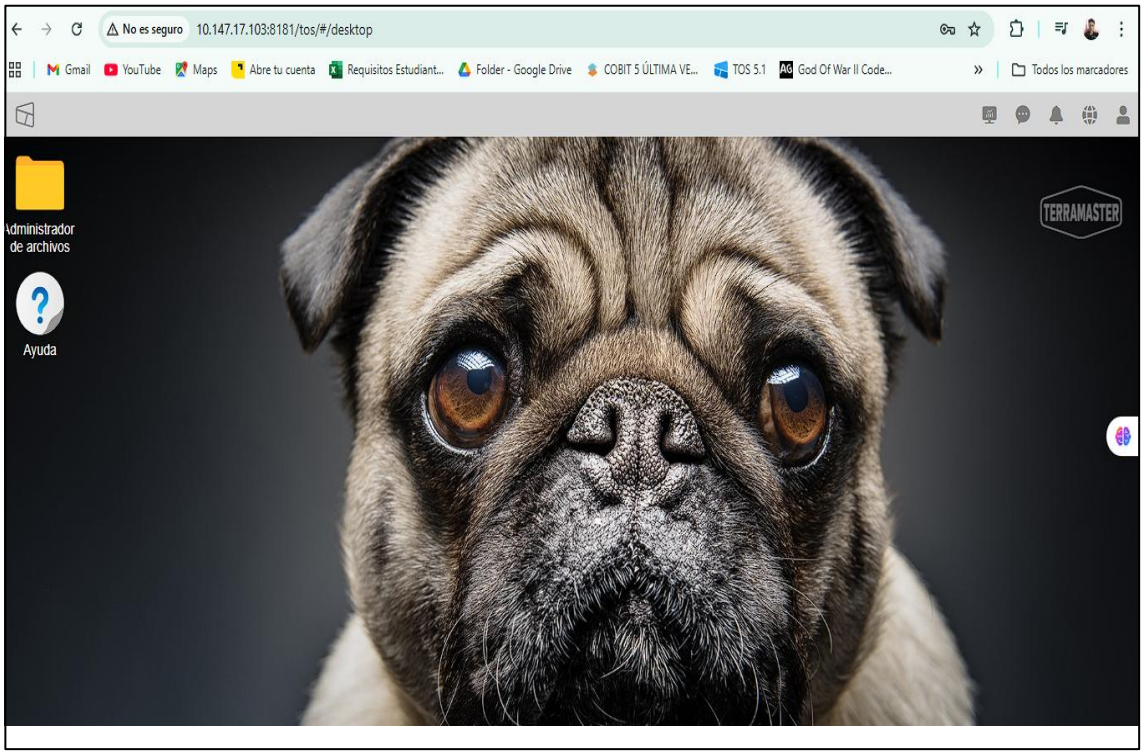


FIGURE 35 CONEXIÓN VPN (ZEROTIER) VIA PC CON LA MISMA IP ASIGNADA AL NAS CON USUARIO NO ADMINISTRADOR.

3.2.4 FASE 4: OPERAR

Durante la fase de operación, se realizará un monitoreo continuo del sistema NAS para verificar el estado de servicios críticos como el acceso remoto. Se utilizarán herramientas integradas para monitorear el rendimiento del hardware. Ver **(ANEXO 16)** – MANUAL.

MONITOREO DE HARDWARE

La supervisión de hardware del dispositivo presenta la interfaz del sistema NAS dedicada a observar la condición física y operativa de sus elementos internos. Esta herramienta brinda al administrador la capacidad de monitorear en tiempo real factores importantes como el uso del procesador, memoria RAM, temperatura de los discos, tasa de transferencia, estado de los ventiladores y bienestar general del almacenamiento.

La supervisión de hardware es crucial para asegurar el funcionamiento constante del sistema, identificar fallos potenciales antes de que impacten en la operación y tomar decisiones fundamentadas sobre mantenimiento o expansión. Asimismo, esta característica puede vincularse con alertas automáticas que informan al usuario sobre situaciones críticas, como el sobrecalentamiento, fallos en los discos o uso excesivo de recursos. Gracias a este monitoreo continuo, el entorno NAS se mantiene estable, seguro y listo para satisfacer las necesidades de los usuarios conectados.

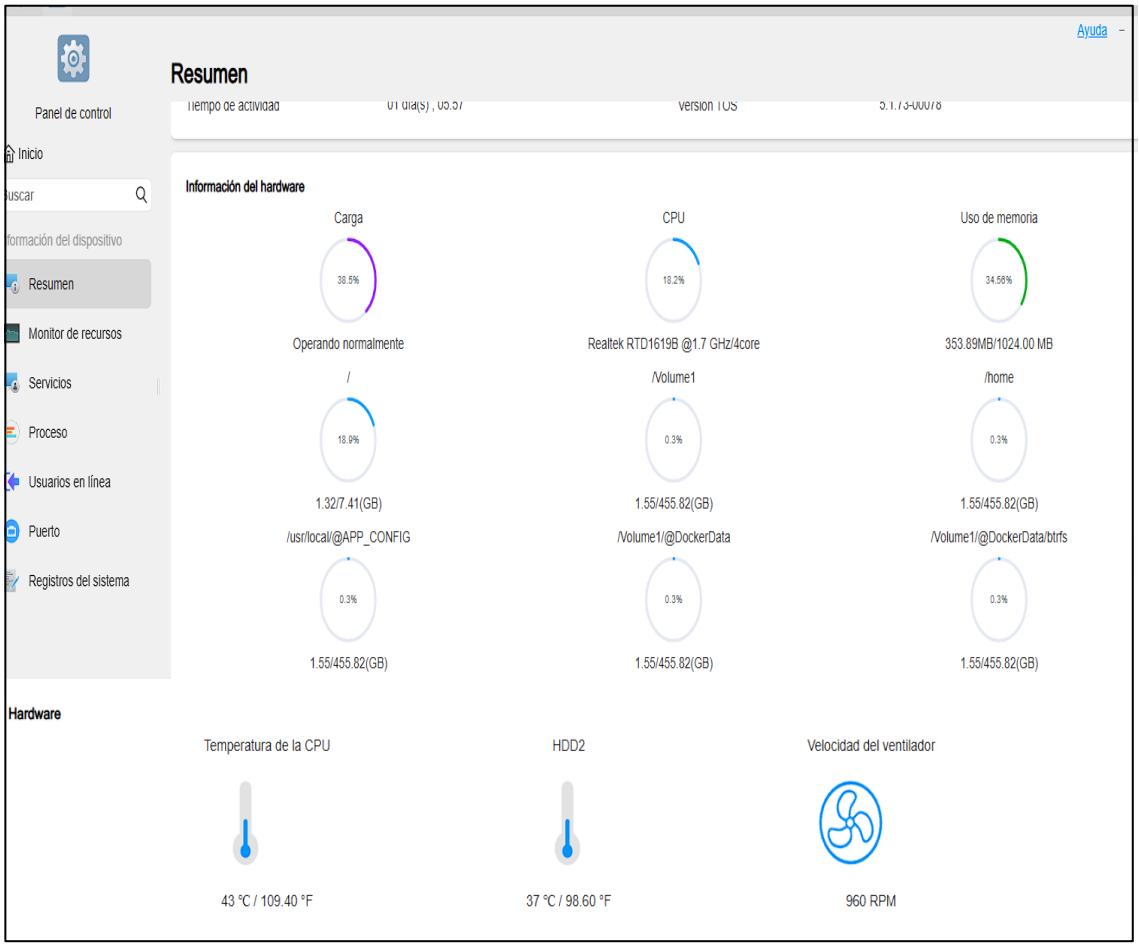


FIGURE 36 MONITOREO DE HARDWARE DEL DISPOSITIVO

MONITOREO DE RED

Muestra la pantalla del sistema NAS para monitorear en tiempo real el estado de la conexión de red. En esta sección, puede ver indicadores como la velocidad de transferencia, la actividad del puerto, el uso del ancho de banda y el estado de las interfaces de red. Estos datos son esenciales para garantizar una comunicación confiable entre el NAS y los dispositivos conectados y para ayudar a diagnosticar problemas de conectividad o rendimiento. También permite analizar el rendimiento general de la red y tomar medidas preventivas ante posibles fallos. De esta manera se garantiza un flujo de datos estable y un funcionamiento óptimo del sistema. Además, la monitorización continua permite detectar fácilmente fallos o interrupciones en la transmisión de datos en una fase temprana. Gracias a esta herramienta, los administradores pueden optimizar la configuración de la red y mantener un entorno más seguro y eficiente. También le permite predecir errores potenciales antes de que afecten el rendimiento general del sistema, lo que reduce el tiempo de inactividad. De esta forma se garantiza una mayor estabilidad operativa y una mejor experiencia para todos los usuarios conectados.

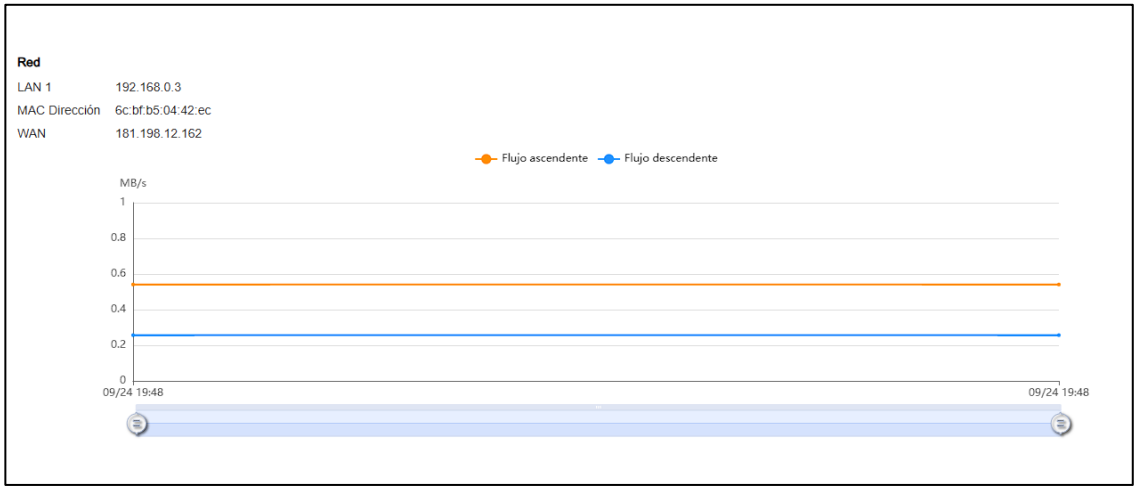


FIGURE 37 MONITOREO DE RED

LA NOTIFICACIÓN DE RESPALDO POR CORREO

Ilustra la manera en que el sistema NAS envía alertas automáticas a través de email al comenzar un proceso de copia de seguridad. Esta característica ayuda a que los administradores o usuarios encargados estén al tanto de la situación de las copias de seguridad, garantizando que se realicen de manera adecuada y continua. Asimismo, estas notificaciones pueden contener información como el tipo de respaldo, el lugar de destino, el avance y errores potenciales, lo que simplifica la supervisión y el manejo preventivo del sistema.

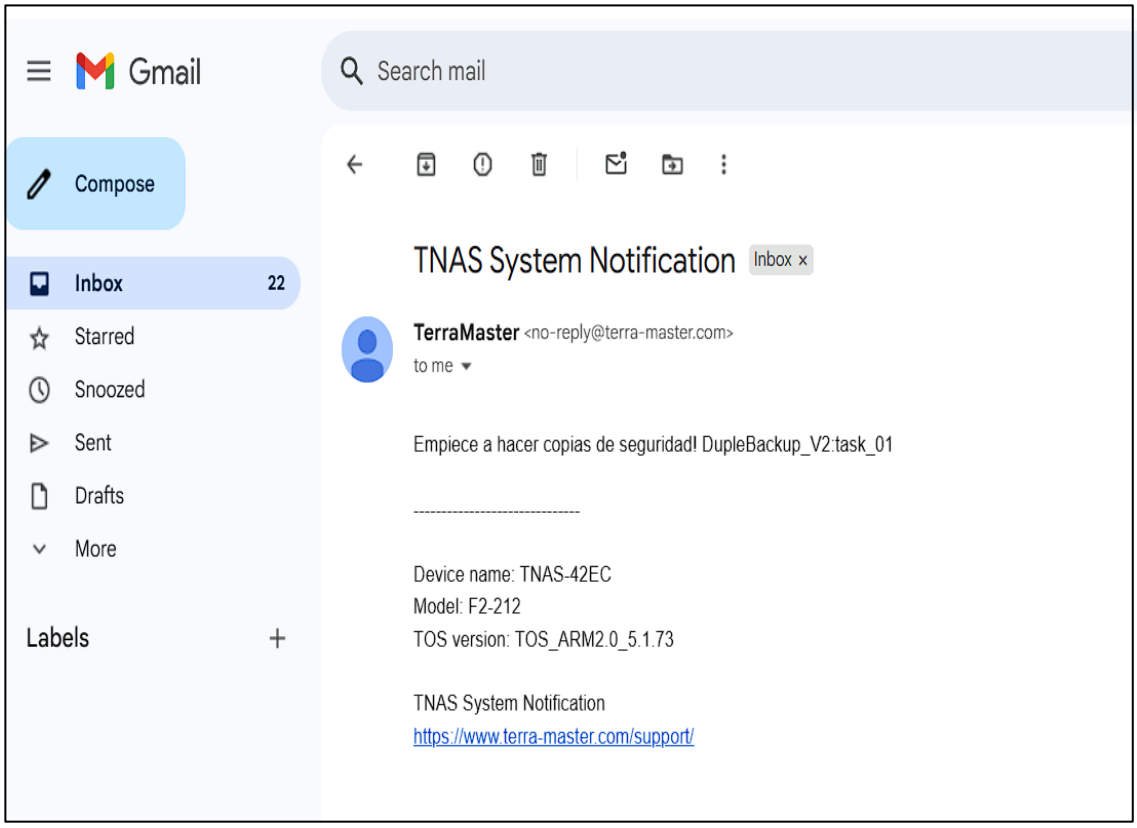


FIGURE 38 ALERTA POR BACKUP EN PROCESO VIA CORREO

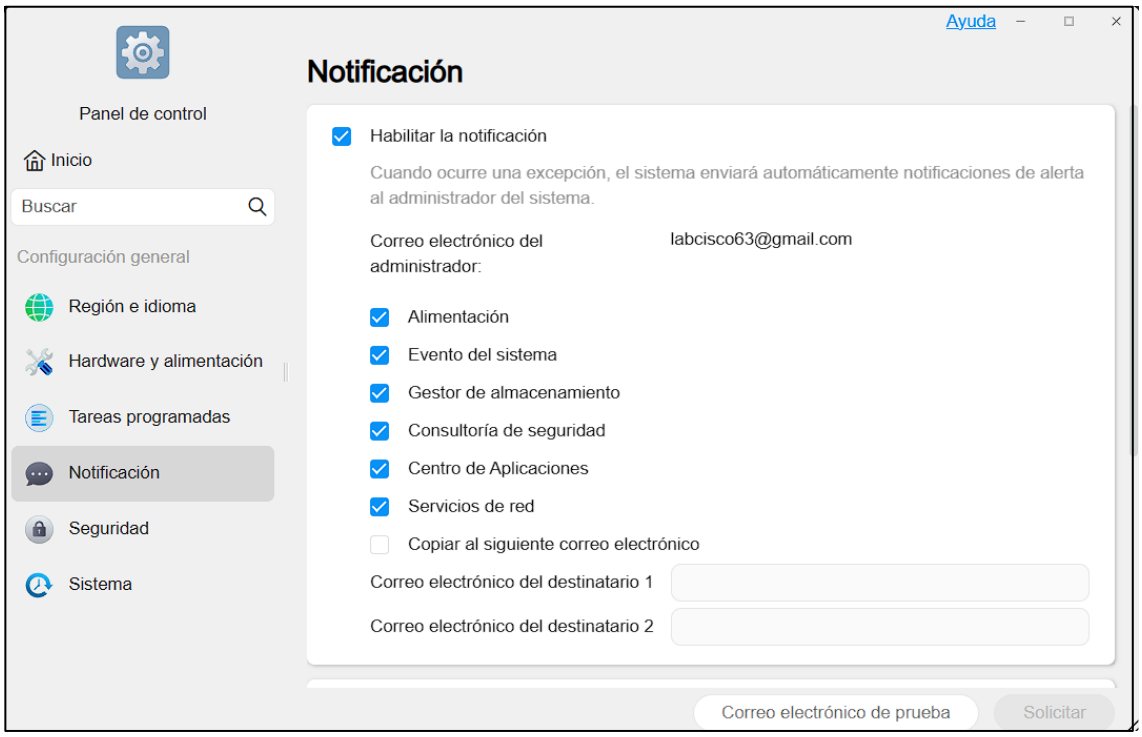


FIGURE 39 CONFIGURACIÓN DE ALERTAS VIA CORREO

ALERTA DE CONEXIÓN SSH AL NAS POR IPV6

La imagen muestra una alerta de seguridad generada por el sistema NAS indicando que la conexión SSH se realizó desde una dirección IPv6 perteneciente a la red ZeroTier. Este tipo de notificación permite a los administradores saber en tiempo real cuando alguien accede al dispositivo a través de un canal seguro, mostrando la hora exacta de inicio de sesión y la IP utilizada. Esta funcionalidad es esencial para mantener el control de acceso remoto y garantizar la integridad del sistema.

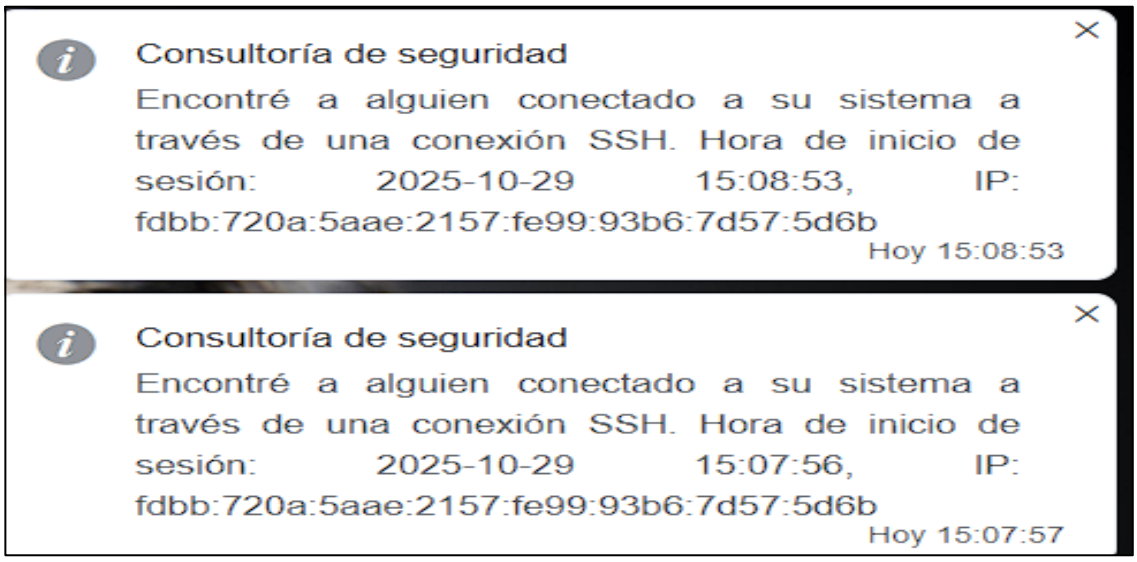


FIGURE 40 MENSAJE DE CONEXIÓN SSH AL NAS POR IPV6

CONCLUSIONES

- Se implementó mini NAS (Terramaster F2-212), con 2 unidades HDD en RAID 1, manteniendo la compatibilidad con la infraestructura existente. Se definió la topología de la red y se utilizaron políticas de acceso con autenticación mediante VPN (ZeroTier/OpenVpn). Se mejoró la gestión de respaldo en un laboratorio controlado utilizando un dispositivo NAS y se fortaleció la conectividad remota con medidas de seguridad de administración de archivos y prácticas de redes en evolución.
- La configuración del servidor mini NAS se completó e integró servicios importantes como dirección IP estática, carpetas compartidas y políticas de respaldo automático. Al crear usuarios con permisos especiales e implementar una VPN segura, se aseguró el acceso remoto controlado, reduciendo las vulnerabilidades.
- Este sistema se diseñó específicamente porque el 63 % de los estudiantes enfrentaban riesgos debido a un bolígrafo y más del 78 % necesitaban almacenamiento compartido. Utilizando VPN (Zerotier/OpenVPN), se realizaron pruebas de conexión remota con una latencia promedio de 26 ms y un pico de hasta 72 ms sin pérdida de paquetes. Las velocidades de transferencia alcanzaron 1,76 MB/s usando CloudSync y el sistema respondió exitosamente a más del 90% de los intentos con copias de seguridad automáticas y alertas de error.
- Desde el NAS, la latencia promedio hasta el enrutador local fue de alrededor de 0,805 ms, con un mínimo de 0,715 ms y sin pérdida de paquetes, estos valores representan un rendimiento óptimo de la red local para tareas de sincronización y copia de seguridad, aunque esto puede variar según las condiciones de la red, se espera que permanezcan dentro de rangos similares durante el funcionamiento normal. Se señala que al servicio SSH se accedió mediante IPv6 virtual, lo que permite una gestión remota eficiente y segura del sistema.
- El manual de usuario básico de instalación y formateo proporciona una guía accesible para los usuarios del laboratorio controlado, está elaborado para uso básico de la configuración inicial y el mantenimiento del sistema. Este facilita la implementación de un sistema NAS y promueve el uso eficiente de los recursos digitales. Además, fortalece las operaciones del laboratorio, permitiendo una gestión segura de la información.

RECOMENDACIONES

- Amplíar la capacidad del sistema integrando nuevos nodos NAS y configurando esquemas RAID , como RAID 5 o RAID 6, que ofrecen una mayor tolerancia a fallos, esto nos permitirá responder a la creciente demanda de almacenamiento y garantizar operaciones de laboratorio ininterrumpidas.
- Fortalecer la seguridad del acceso remoto implementando autenticación multifactor (2FA) y actualizaciones de credenciales, especialmente cuando se accede a través de VPN (ZeroTier/OpenVPN). Además revisar y actualizar las políticas de control de acceso para garantizar que los permisos otorgados a los usuarios sean consistentes con sus roles y niveles de responsabilidad.
- Se encarga aplicar servicios enlazados a ipv6, el uso de direcciones IPv6 tiene como objetivo habilitar servicios de almacenamiento distribuido, sincronización remota y administración de dispositivos en redes modernas, esta implementación proporcionaría mayor escalabilidad, mejor segmentación de la red y soporte para múltiples servicios simultáneos al optimizar la conectividad entre los nodos del sistema NAS y otros recursos de la red.
- Dar la posibilidad de capacitar a los docentes y estudiantes en el uso del sistema NAS y herramientas relacionadas, incluida la gestión de archivos, el uso de CloudSync para la sincronización en la nube y la administración de usuarios, esto causará el uso eficiente del sistema, reducirá errores operativos y fortalecerá la saber de protección de la información crítica en el entorno académico.
- Crear un mantenimiento anticipado y monitorear continuamente del sistema NAS mediante herramientas de software integradas al sistema operativo TOS, como panel de control, monitoreo de hardware y red, esto descubrirá fallas tempranas en el disco, congestión de la red o accesos no autorizados, garantizando la disponibilidad y estabilidad del sistema.

Referencias

[1] G. M. D. C.-. L. I.-. J. M. S. Peralta, «Jornadas de Investigacion,» EL IMPACTO DE LAS TIC EN GOBIERNO ABIERTO, 2024. [En línea]. Available: https://fce.unl.edu.ar/jornadasdeinvestigacion/trabajos/uploads/trabajos/105.pdf. [Último acceso: 11 11 2025].

[2] M. A. P. G. y. D. R. F. B. Juliet Díaz Lazo, «SCIELO,» SCIELO, 2011. [En línea]. Available: http://scielo.sld.cu/scielo.php?pid=S0258-59362011000100009&script=sci_arttext&tlng=pt. [Último acceso: 29 05 2025].

[3] J. D. Lazo, «MINISTERIO DE EDUCACION DE CUBA,» [En línea]. Available: https://www.redalyc.org/pdf/1932/193222352001.pdf. [Último acceso: 2025 05 2025].

[4] V. P. S. G. Santiago Fernando Vinueza Vinueza, «revistapublicando,» Universidad Central del Ecuador, [En línea]. Available: https://revistapublicando.org/revista/index.php/crv/article/view/530. [Último acceso: 29 05 2025].

[5] H. L. A. S. ,. A. A. Y. D. Carlos Augusto, «Editorial Universidad Manuela Beltrán,» 2018. [En línea]. Available: https://www.academia.edu/37422841/Tecnolog%C3%ADas_de_la_Nueva_Generaci%C3%B3n_para_el_Fortalecimiento_Empresarial_ISBN_978_958_5467_07_1. [Último acceso: 12 11 2025].

[6] V. A. ,. L. G. A. Monica Patricia, «Espacios,» 2012-2015. [En línea]. Available: https://www.revistaespacios.com/a18v39n47/a18v39n47p05.pdf.

[7] U. P. S. Elena, «ESTATUTO DE LA UNIVERSIDAD ESTATAL "PENÍNSULA DE SANTA ELENA",» 22 07 1998. [En línea]. Available: https://upse.edu.ec/images/2021/Mayo/ESTATUTO_REFORMADO_2021.pdf. [Último acceso: 12 11 2025].

[8] M. P. CRISTIAN, «UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE,» FACULTAD DE INGENIERÍA, 2020. [En línea]. Available: https://repositorio.uladech.edu.pe/bitstream/handle/20.500.13032/18484/IMPLEMENTACION_SERVIDOR_MORENO_PAICO_CRISTIAN.pdf?sequence=1. [Último acceso: 12 11 2025].

[9] J. D. B. R. C. B. W. Bach. Huarhua Diaz, «UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA,» 31 08 2023. [En línea]. Available: https://repositorio.upci.edu.pe/bitstream/handle/upci/863/tesis%20-%20joel%20huarhua-brett%20rodriguez.pdf?sequence=1&isAllowed=y. [Último acceso: 12 11 2025].

[10] C. A. C. MORALES, «UNIVERSIDAD POLITÉCNICA SALESIANA,» 11 2021. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/21288/1/UPS%20-%20TTS542.pdf. [Último acceso: 14 05 2025].

[11] cisco, «cisco,» red plataforma bibliote, [En línea]. Available: https://www.cisco.com/c/dam/global/es_mx/products/servicios/docs/LCS_Brochure_Enterprise_Spanish_062006.pdf. [Último acceso: 18 09 2025].

[12] J. R. H. A. J. D. M. D. A. R. t. Guido Paniagua, «Repositorio Institucional UNAN-LEON,» Repositorio Institucional UNAN-LEON, 06 2020. [En línea]. Available: http://riul.unanleon.edu.ni:8080/jspui/handle/123456789/7557. [Último acceso: 20 05 2025].

[13] DOMOTES, «DOMOTES,» DOMOTES, [En línea]. Available: https://www.domotes.com/post/como-brindar-acceso-seguro-con-conexiones-vpn-utilizando-nas-asustor. [Último acceso: 20 05 2025].

[14] M. A. R. L. A. B. M. P. T. W. J. Fonseca Lozano, «UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA,» 24 09 2004. [En línea]. Available: https://repository.unad.edu.co/bitstream/handle/10596/20167/mafonsecal.pdf?sequence=1&isAllowed=y. [Último acceso: 12 11 2025].

[15] PlanNacionalDeDesarrollo25-29, «planificacion,» [En línea]. Available: https://www.planificacion.gob.ec/wp-content/uploads/2025/08/PlanNacionalDeDesarrollo25-29_EcuadorNoSeDetiene.pdf. [Último acceso: 14 10 2025].

[16] S. K. Routray, «Tecnologías de la información y las comunicaciones para un mundo sostenible,» *Potenciales IEEE,* p. 10.1109/mpot.2024.3404114, 2023.

[17] S. N. R. Hasbie, «Adopción de tecnologías de la información y la comunicación (TIC) y comunidad: una revisión sistemática de la literatura,» pp. 10.6007/ijarbss/v13-i15/18799, 2023.

[18] T. S. Chiang, «Sistema de almacenamiento de datos,» *Sistema de almacenamiento de datos,* pp. https://scispace.com/papers/data-storage-system-rr6hm5dzfj .

[19] H. Ming, «Sistema de almacenamiento de datos y método de almacenamiento de datos,» *Sistema de almacenamiento de datos y método de almacenamiento de datos,* pp. https://scispace.com/papers/data-storage-system-and-data-storage-method-frrumatrao.

[20] W. Chang, «Sistema de almacenamiento NAS basado en el sistema de almacenamiento distribuido Ceph,» *Sistema de almacenamiento NAS basado en el sistema de almacenamiento distribuido Ceph,* pp. https://scispace.com/papers/nas-storage-system-based-on-distributed-storage-system-ceph-4u4xm902c3.

[21] C. Gallo, «Redes privadas virtuales,» *Redes privadas virtuales,* pp. https://scispace.com/papers/virtual-private-networks-2a9ngjf4bw.

[22] A. Shabbir, «Enfoque del ciclo de vida de PPDIOO para el diseño e implementación de redes,» *Enfoque del ciclo de vida de PPDIOO para el diseño e implementación de redes,* pp. https://www.linkedin.com/pulse/ppdioo-lifecycle-approach-network-design-adnan?utm_source=.

[23] microsoft, «¿Qué es el control de acceso?,» *¿Qué es el control de acceso?,* pp. https://www.microsoft.com/es-es/security/business/security-101/what-is-access-control, 26 08 2025.

[24] empowertalent, «Conexiones de Red: qué son,» *Conexiones de Red: qué son, tipos, funcionalidades y aplicaciones,* pp. https://empowertalent.com/conexiones-de-red/.

[25] getresponse, «getresponse,» getresponse, [En línea]. Available: https://www.getresponse.com/es/ayuda/cliente.html. [Último acceso: 02 11 2025].

[26] b2oceans, «¿Qué es: Monitoreo y alertas automatizadas?,» b2oceans, [En línea]. Available: https://www.b2oceans.com/es/glosario/que-es-la-monitorizacion-y-alertas-automatizadas/. [Último acceso: 05 11 2025].

[27] tecnovortex, «tecnovortex,» tecnovortex, [En línea]. Available: https://tecnovortex.com/western-digital-raptors-los-discos-rigidos-mas-impresionantes-de-la-historia/. [Último acceso: 18 09 2025].

[28] GroupTelecom, «GroupTelecom,» GroupTelecom, [En línea]. Available: https://www.gruptelecom.com/diferencias-entre-cable-cat-6-y-cat-7-de-ethernet/. [Último acceso: 14 05 2025].

[29] zerotier, «zerotier,» zerotier, [En línea]. Available: https://www.zerotier.com/. [Último acceso: 05 11 2025].

[30] xataka, «Servidores NAS: qué son, cómo funcionan y qué puedes hacer con uno,» *Servidores NAS: qué son, cómo funcionan y qué puedes hacer con uno,* pp. https://www.xataka.com/basics/servidores-nas-que-como-funcionan-que-puedes-hacer-uno.

[31] terra-master, «Duple Backup,» *Duple Backup,* pp. https://www.terra-master.com/es/duple-backup/.

[32] terramaster, «terramaster,» terramaster, [En línea]. Available: https://terramasterus.myshopify.com/es/pages/cloudsync?srsltid=AfmBOopww1eMGiwRd6bBi3Qzdjy9EhBqZTWGOfQMHTOmBHovS-ZJ7MKt. [Último acceso: 08 10 2025].

[33] GOOGLE, «Google Workspace,» GOOGLE, [En línea]. Available: https://workspace.google.com/intl/es-419/gmail/. [Último acceso: 08 10 2025].

[34] GOOGLE, «Google Workspace,» GOOGLE, [En línea]. Available: https://workspace.google.com/intl/es-419/products/drive/. [Último acceso: 08 10 2025].

[35] GOOGLE, «Google Workspace,» GOOGLE, 14 10 2025. [En línea]. Available: https://developers.google.com/apps-script/overview?hl=es-419. [Último acceso: 12 11 2025].

[36] Hostaliawhitepapers, «Hostaliawhitepapers,» [En línea]. Available: https://pressroom.hostalia.com/contents/ui/theme/images/WP-Hostalia-protocolo-SSH.pdf. [Último acceso: 08 10 2025].

[37] lenovo, «lenovo,» [En línea]. Available: https://www.lenovo.com/es/es/glossary/putty/?orgRef=https%253A%252F%252Fwww.google.com%252F&srsltid=AfmBOorYxOVoQUlkUKpg85FdZAd-3UIMMW7gS37r1YSd9En-OmsQwJhh. [Último acceso: 08 10 2025].

[38] primeinstitute, «primeinstitute,» primeinstitute, [En línea]. Available: https://www.primeinstitute.com/preguntas/descubre-por-que-openvpn-es-la-vpn-mas-confiable-del-mundo-24250. [Último acceso: 05 11 2025].

[39] S. T. T. Tsao, «Uso de un dispositivo NAS para construir un servidor de vídeo distribuido no convencional,» *Uso de un dispositivo NAS para construir un servidor de vídeo distribuido no convencional,* pp. https://scispace.com/papers/using-nas-appliance-to-build-a-non-conventional-distributed-39aup0yn9l, 22 octubre 2002.

[40] Y. Y. Dan, «Equipos NAS y sistemas y métodos de procesamiento distribuido,» *Equipos NAS y sistemas y métodos de procesamiento distribuido,* pp. https://scispace.com/papers/nas-equipment-and-distributed-processing-system-and-method-40m9nyhxwa, 03 agosto 2017.

[41] M. Bennion, «Acceso distribuido al almacenamiento remoto de datos,» *Acceso distribuido al almacenamiento remoto de datos,* pp. https://scispace.com/papers/distributed-remote-data-storage-access-32swr0s9wa, 15 mayo 2014.

[42] w. ran, «Sistema de almacenamiento remoto y método que utiliza un dispositivo de almacenamiento conectado a red (NAS),» *Sistema de almacenamiento remoto y método que utiliza un dispositivo de almacenamiento conectado a red (NAS),* pp. https://scispace.com/papers/remote-storage-system-and-method-using-network-attached-1vpnepuzn5, 12 agosto 2013.

[43] B. Jean-Pierre, «Archivado de servidores NAS en la nube,» *Archivado de servidores NAS en la nube,* pp. https://scispace.com/papers/archiving-nas-servers-to-the-cloud-2eebgao9c7, 31 julio 2019.

[44] A. Muc, «Proporcionar la capacidad de trabajar de forma remota en el servidor local de la empresa a través de VPN,» *Proporcionar la capacidad de trabajar de forma remota en el servidor local de la empresa a través de VPN,* pp. https://scispace.com/papers/providing-the-ability-of-working-remotely-on-local-company-1eccu0oq8k, 31 08 2020.

[45] J. S. Iwanski, «Acceso seguro a aplicaciones detrás del firewall,» *Acceso seguro a aplicaciones detrás del firewall,* pp. https://scispace.com/papers/secure-access-to-applications-behind-firewall-2o9uhnpoq2.

[46] satoricyber, «Políticas de control de acceso: definiciones y tipos,» *Políticas de control de acceso: definiciones y tipos,* pp. https://satoricyber.com/access-control/access-control-policies-definitions-types/.

[47] ibm, «¿Qué es una red de área amplia (WAN)?,» *¿Qué es una red de área amplia (WAN)?,* pp. https://www.ibm.com/es-es/think/topics/wide-area-network#:~:text=Las%20redes%20de%20%C3%A1rea%20amplia,de%20un%20proveedor%20de%20servicios..

[48] P. G. O. M. MUNAR MUÑOZ MARTHA LILIANA, «UNIVERSIDAD COOPERATIVA DE COLOMBIA,» [En línea]. Available: https://repository.ucc.edu.co/server/api/core/bitstreams/9f6dc324-2372-48c5-acf5-c75e477136b8/content. [Último acceso: 12 11 2025].

[49] M. R. J. D. CRISTHIAN PAÚL LAGLA GALLARDO, «dspace,» RED PLATAFORMA BIBLIOTECA, [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/16686/1/UPS-ST003882.pdf. [Último acceso: 05 11 2025].

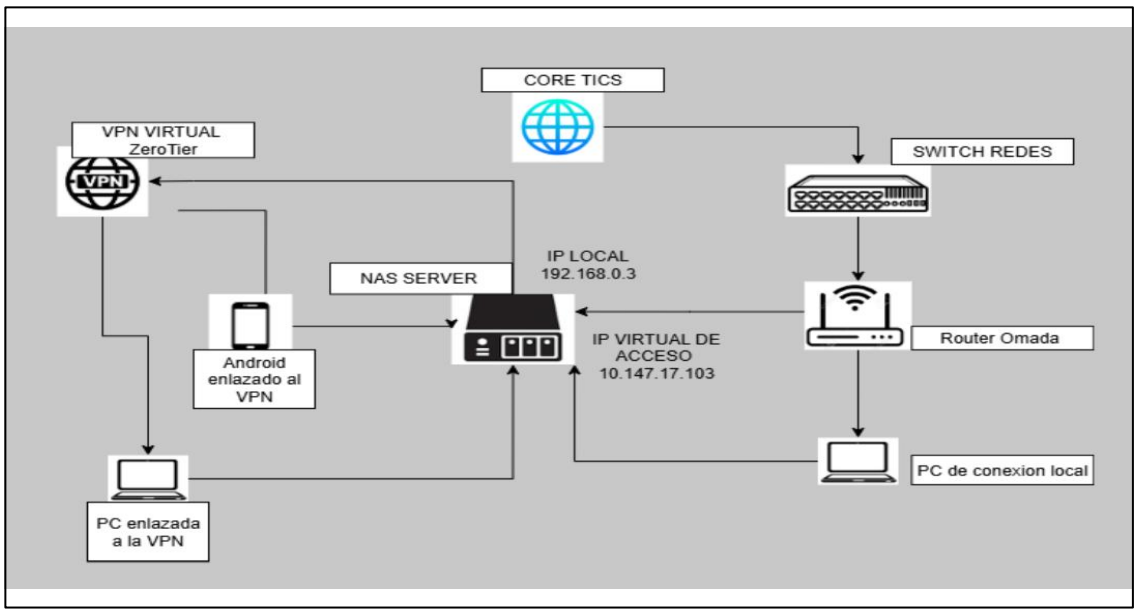
ANEXOS

ANEXOS 1 ENCUESTA

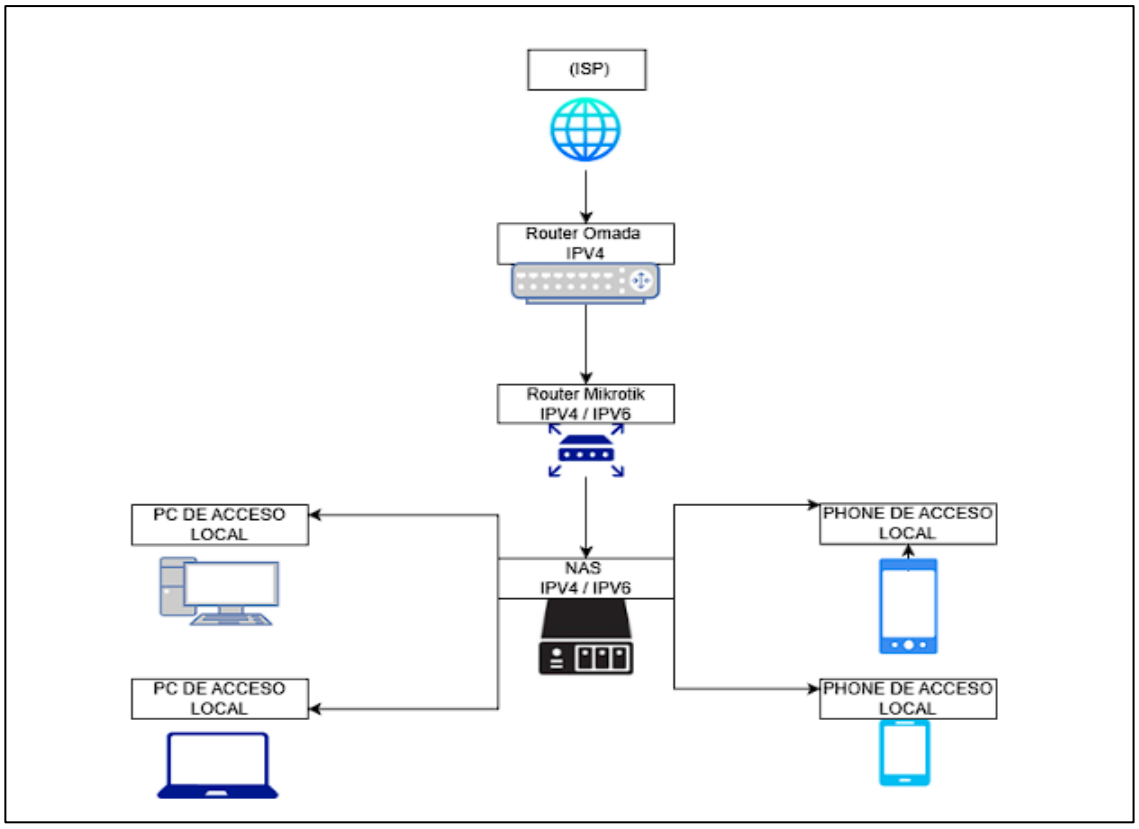
El objetivo de esta encuesta permitirá fundamentar técnicamente la necesidad de una estrategia de red más eficiente y centrada en el almacenamiento centralizado y seguro. **1. ¿Hay algúna Plataforma que no sea común donde se pueda guardar y consultar con los archivos?**
a). Sí b). No c). Probablemente
2. ¿ Cree usted que es seguro el almacenamiento que utilizan normalmente ?
a). Sí b). No c).Probablemente
3. ¿Ha Tenido un pendrive para el compartimiento de archivos con el temor de algún virus?
a). Si b). No c). Probablemente
4. ¿Crees que sería mejor si existiera un tipo de almacenamiento el cual todos puedan acceder a instaladores, horarios y manuales?
a). Si sería más organizado b). Tal vez c). No lo veo necesario
5. ¿Ha tenido que repetir tareas o configuraciones porque no encontró archivos de instaladores o documentos anteriores?

a). Si b). No c). Alguna vez me pasó
6. ¿Desearias poder ingresar archivos locales del laboratorio externamente de la Universidad ?
a). Si, lo considero muy útil b). Tal vez pero no lo usaría mucho c). No estoy interesado
7. ¿ Puedes compartir tus archivos con otras personas sin necesidad de enviárselos directamente.?
a). Si b). No c). Solo a veces
8. ¿Qué beneficio apreciaría más en el sistema de almacenamiento compartido?
a) Acceder a mis archivos desde cualquier lugar b) Que trabajemos con la misma versión del archivo c) No tener que usar USB ni discos externos

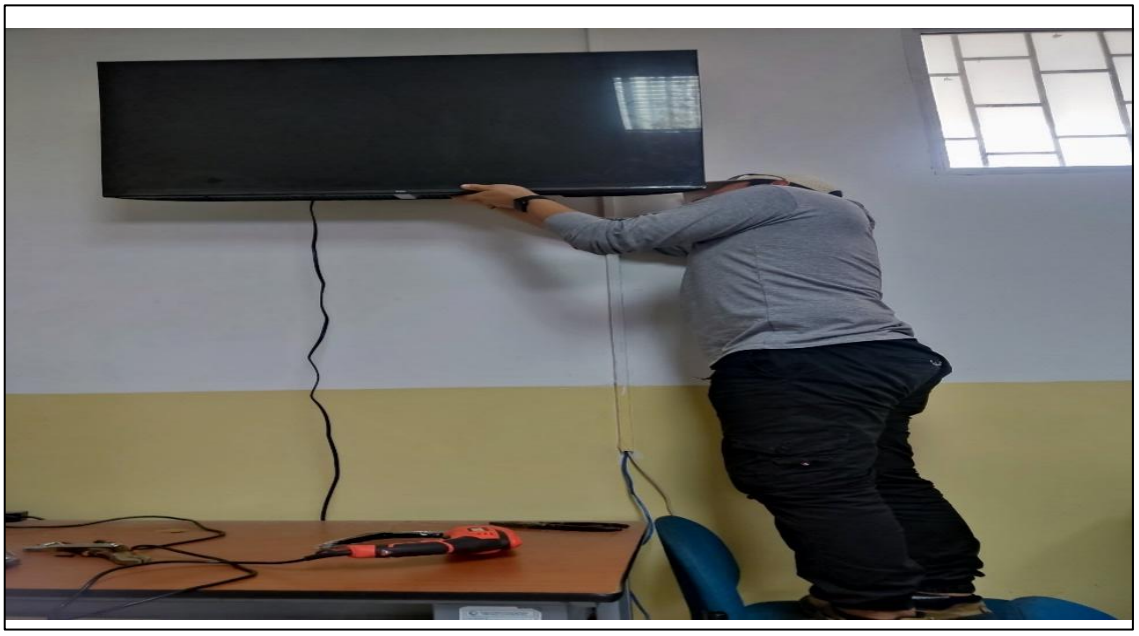
ANEXOS 2 INFRAESTRUCTURA DE RED



ANEXOS 3 TOPOLOGÍA DE RED HIBRIDA EN ESTRELLA

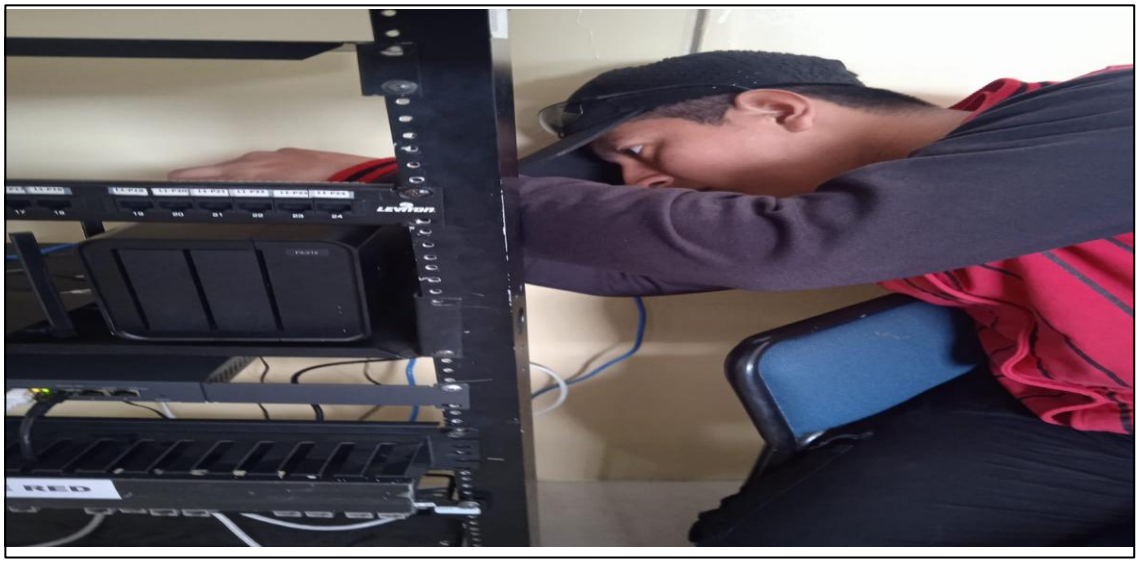


ANEXOS 4 INSTALACIÓN DE PANTALLA EN LAB REDES

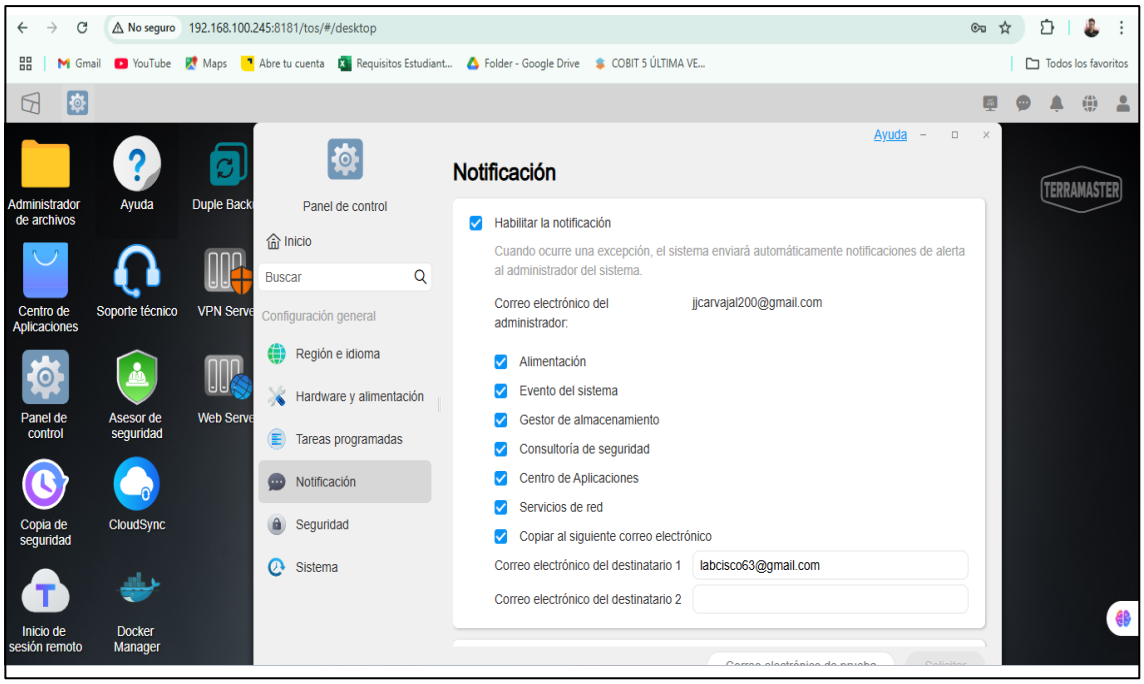


ANEXOS 5 INSTALACIÓN DE SEGUNDO MONITOR EN EL RACK

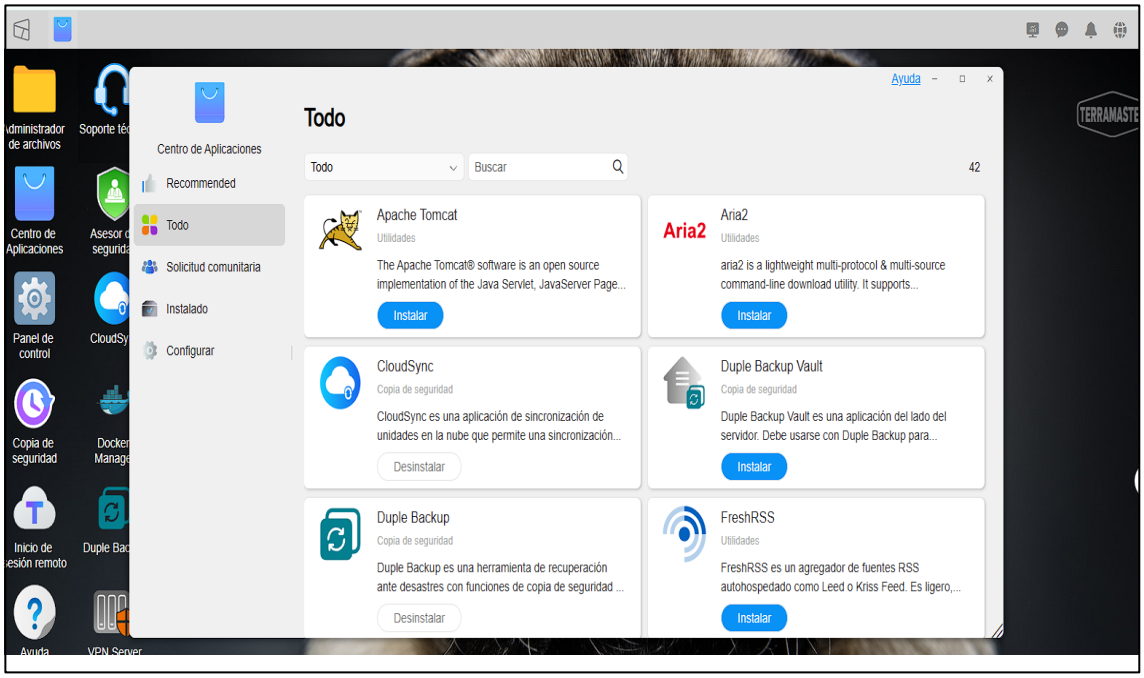
ANEXOS 6 INSTALACIÓN NAS



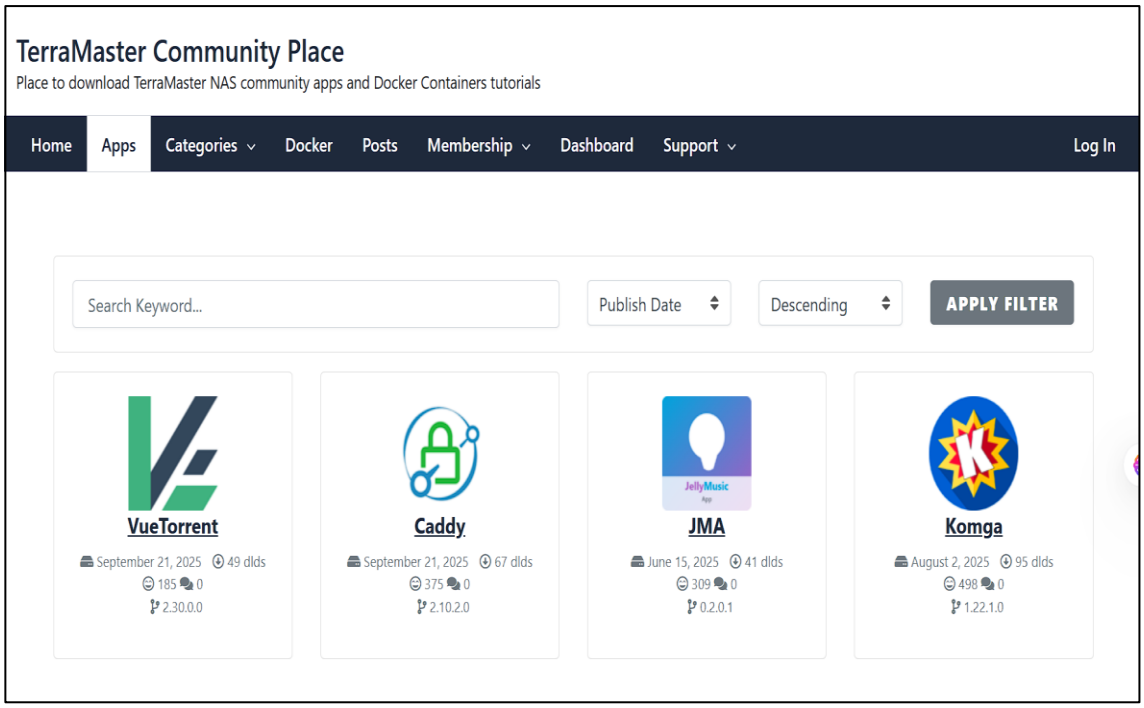
ANEXOS 7 SINCRONIZACIÓN DE CORREO PARA ALERTAS



ANEXOS 8 TIENDA DE SOFTWARE ADICIONALES



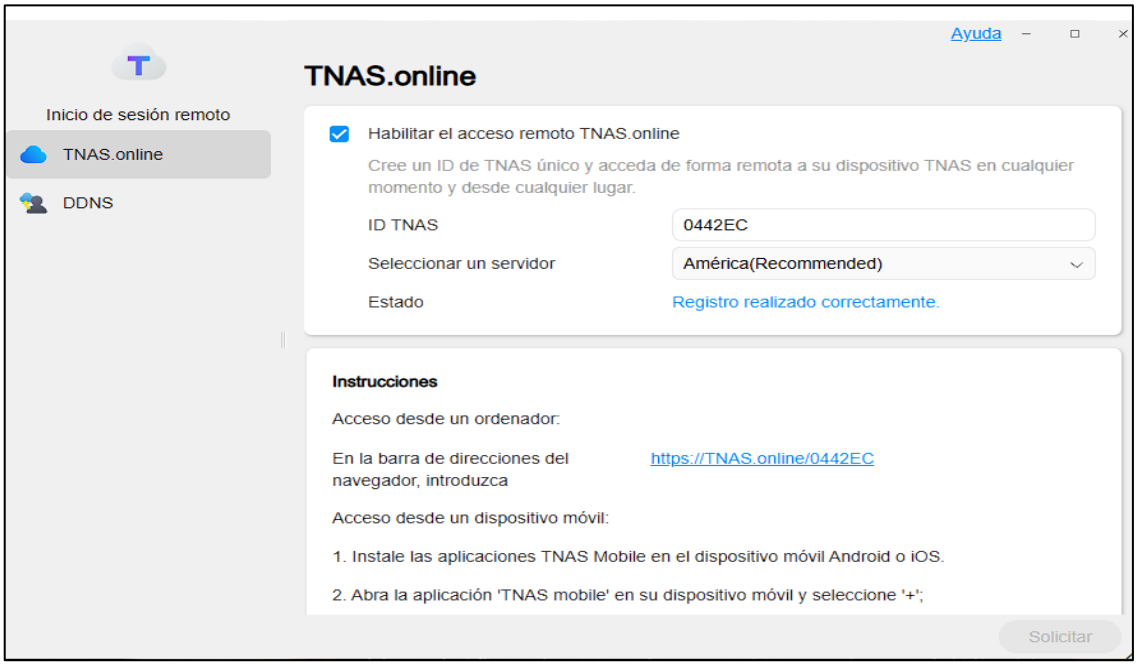
ANEXOS 9 SOFTWARE ADICIONALES



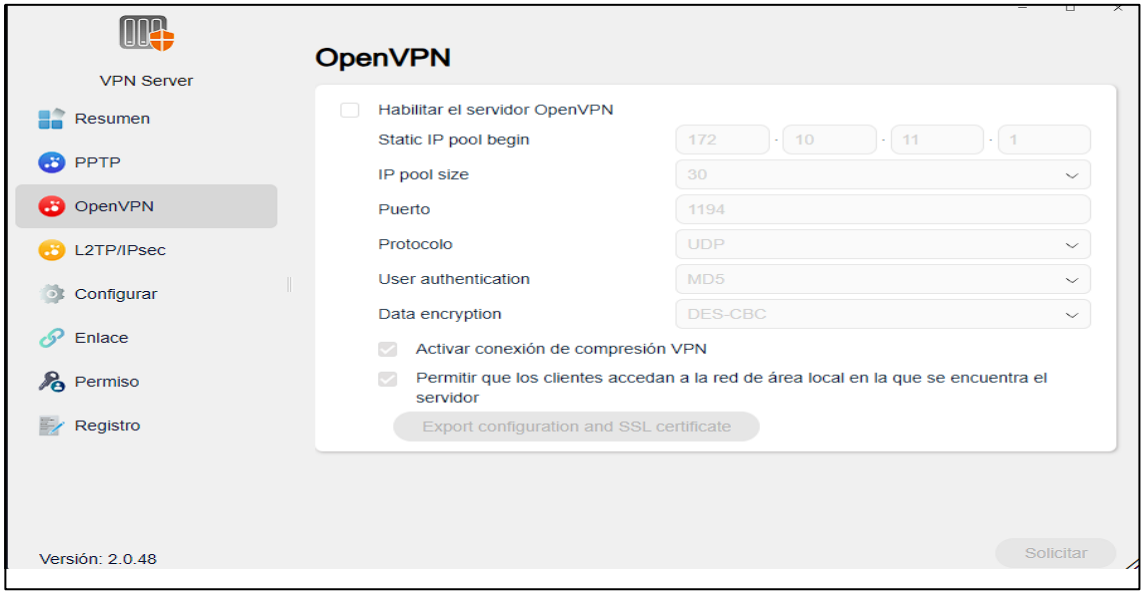
LINK

https://tmnascommunity.eu/apps/

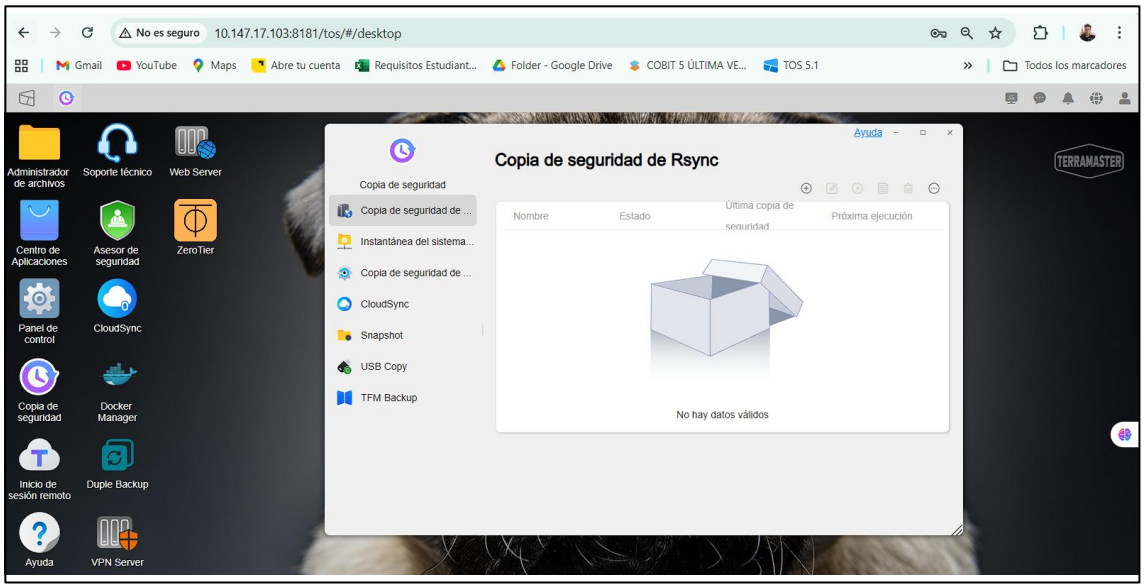
ANEXOS 10 CONEXIÓN REMOTA VIA URL (SIN VPN) MENOS SEGURA



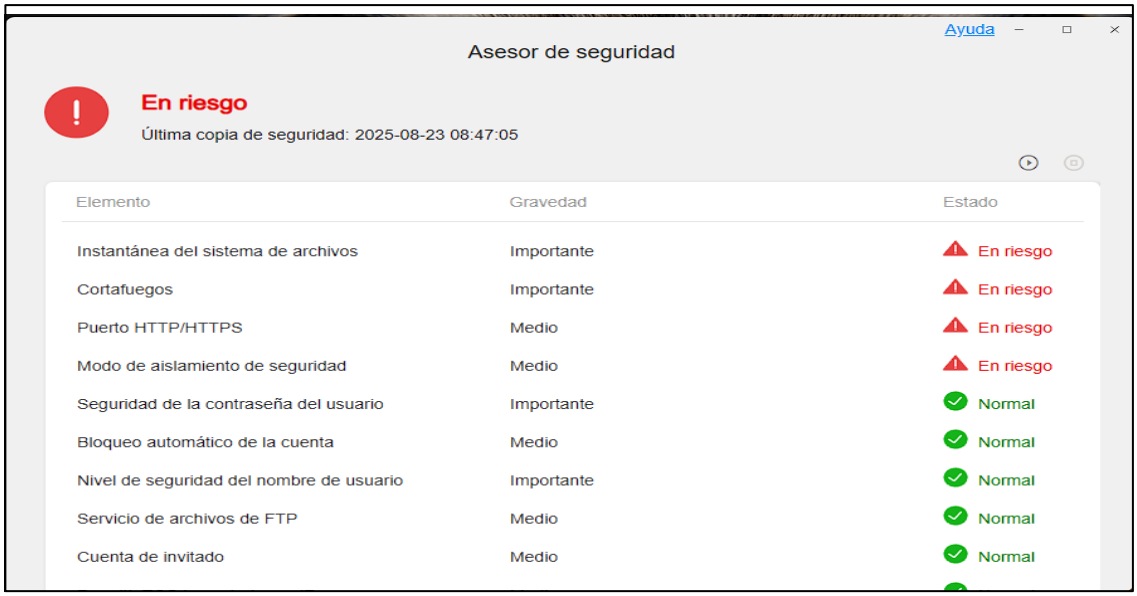
ANEXOS 11 VPN SERVER (SE NECESITA HABILITAR PUERTO 1194 Y USO DE IP PÚBLICA O DOMINIO PARA SU CONEXIÓN)



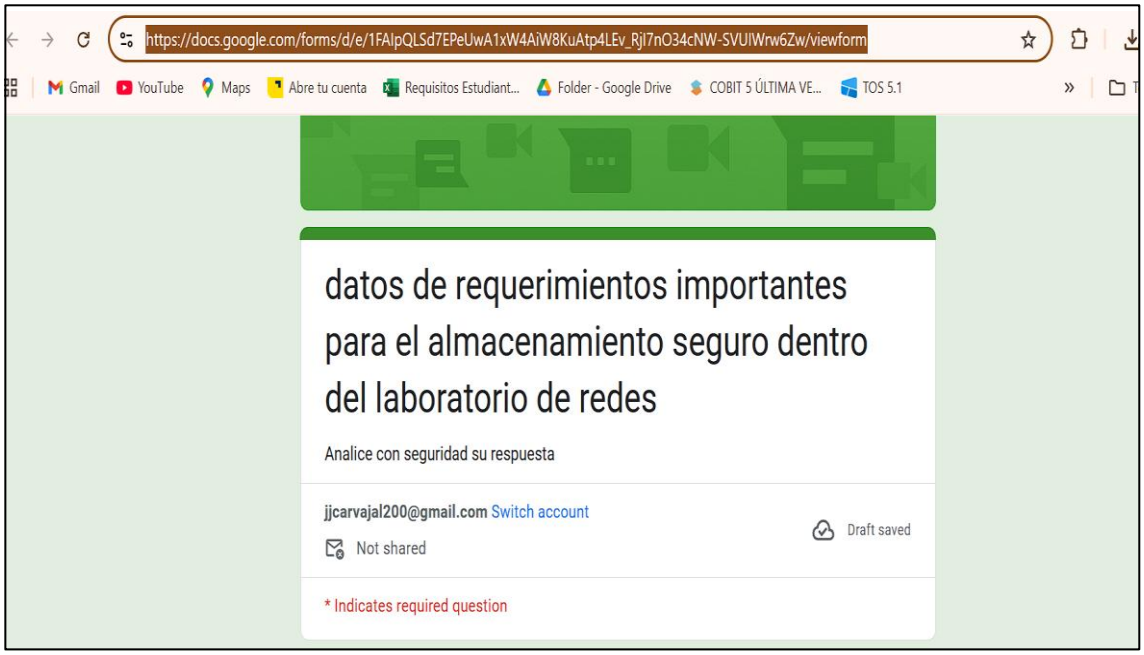
ANEXOS 12 SOFTWARE PREDETERMINADO PARA COPIAS DE SEGURIDAD DEL SISTEMA



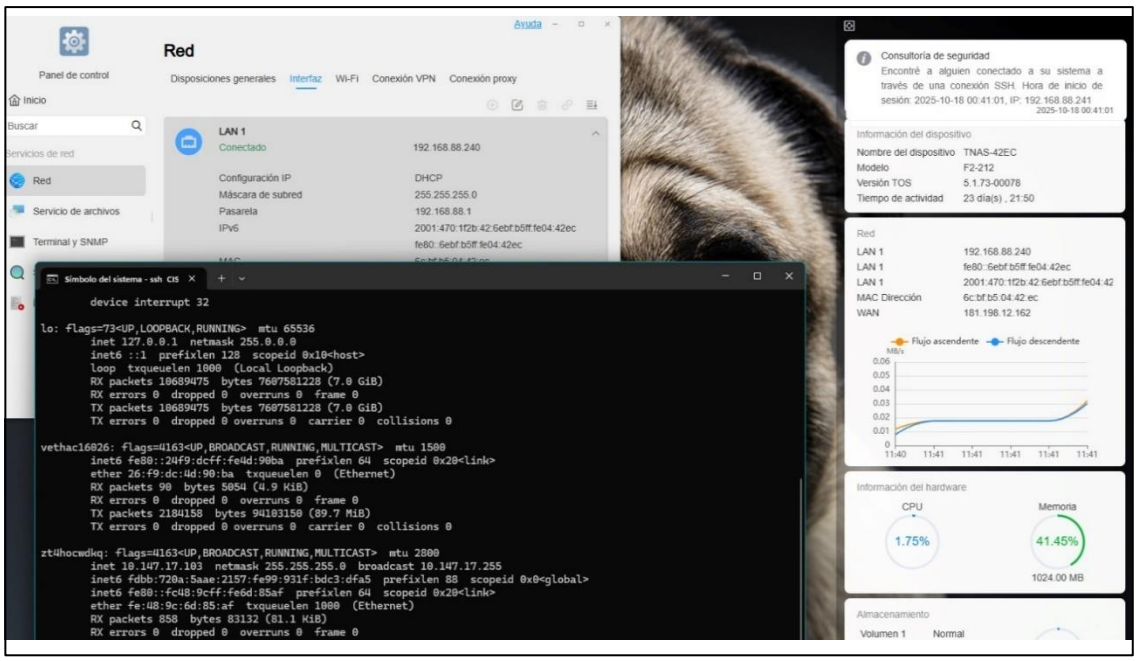
ANEXOS 13 ASESOR DE SEGURIDAD DE MONITOREO DE GRAVEDAD



ANEXOS 14 ENCUESTA HECHA EN GOOGLE FORM



ANEXOS 15 RECIBIMIENTO DE IPV6 MEDIANTE ROUTER MIKROTIK



MANUAL DE FUNCIONAMIENTO

MINI NAS (TERRAMASTER F2-212)

AUTOR

CARVAJAL NUÑEZ JAMES JOSUE

TUTOR

ING. DANIEL QUIRUMBAY

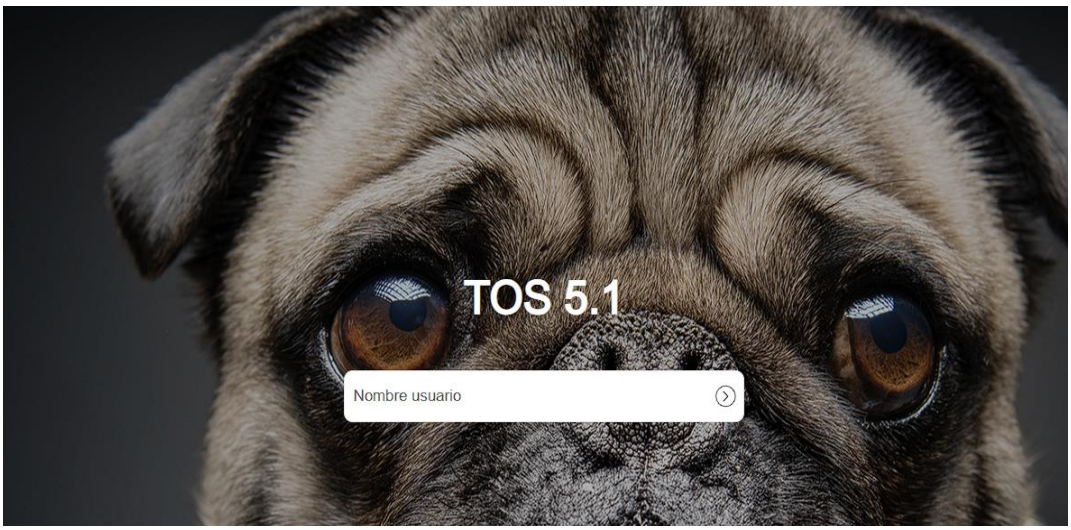
AÑO 2025-2

Credenciales para el acceso vía gmail.
CORREO **Usuario : labcisco63@gmail.com**
Contraseña: labCisco_01

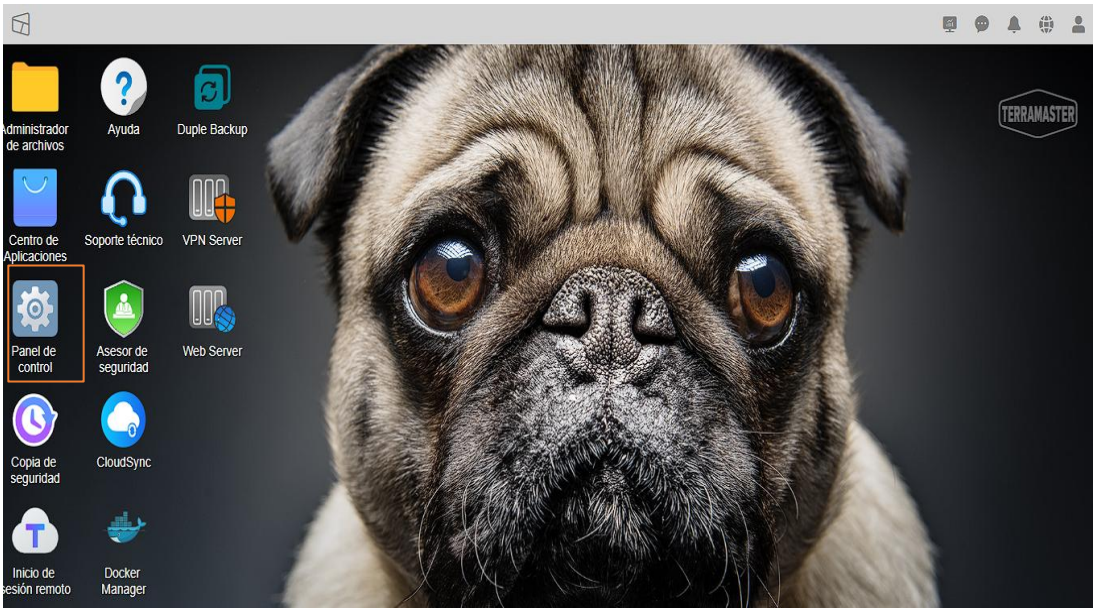
Recomendaciones :

El proceso de Formateo del dispositivo Deberá hacerse de forma local, no remotamente y tener una buena conexión a internet.

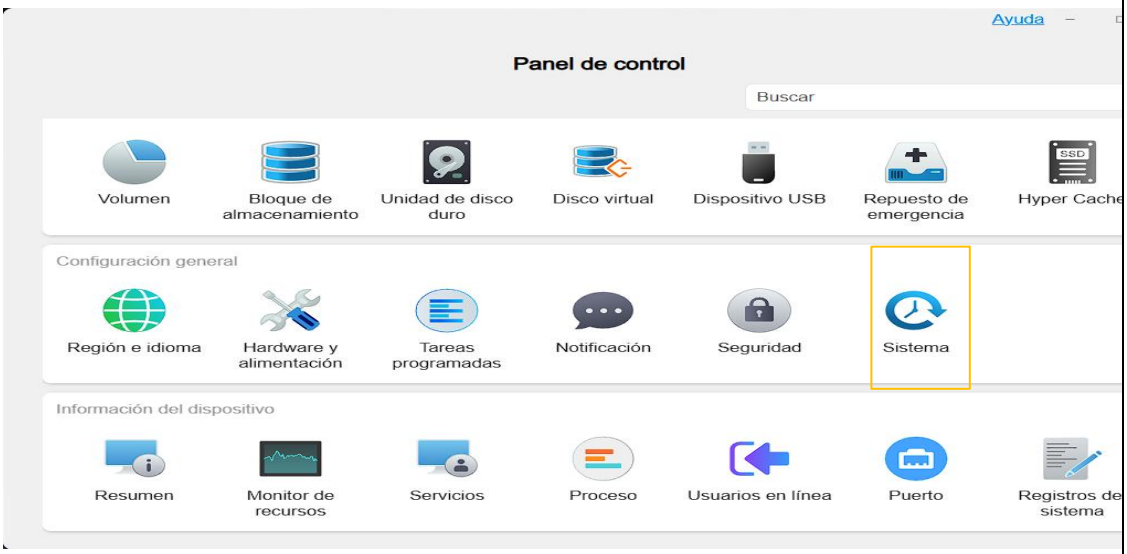
Formateo el Sistema NAS.

Iniciamos sesión con las credenciales que se les asignado Oficialmente como administrador:
Usuario : CISCO
Contraseña : labCisco_01


PASO 1 :
Ingresamos al panel de control



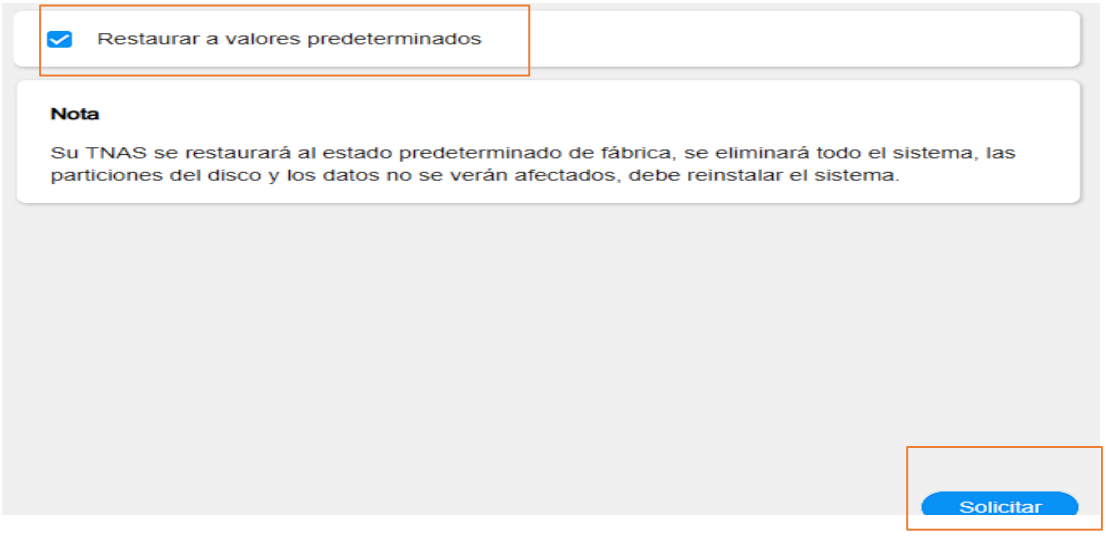
Nos dirigimos al panel de control , y seleccionamos (SISTEMA).



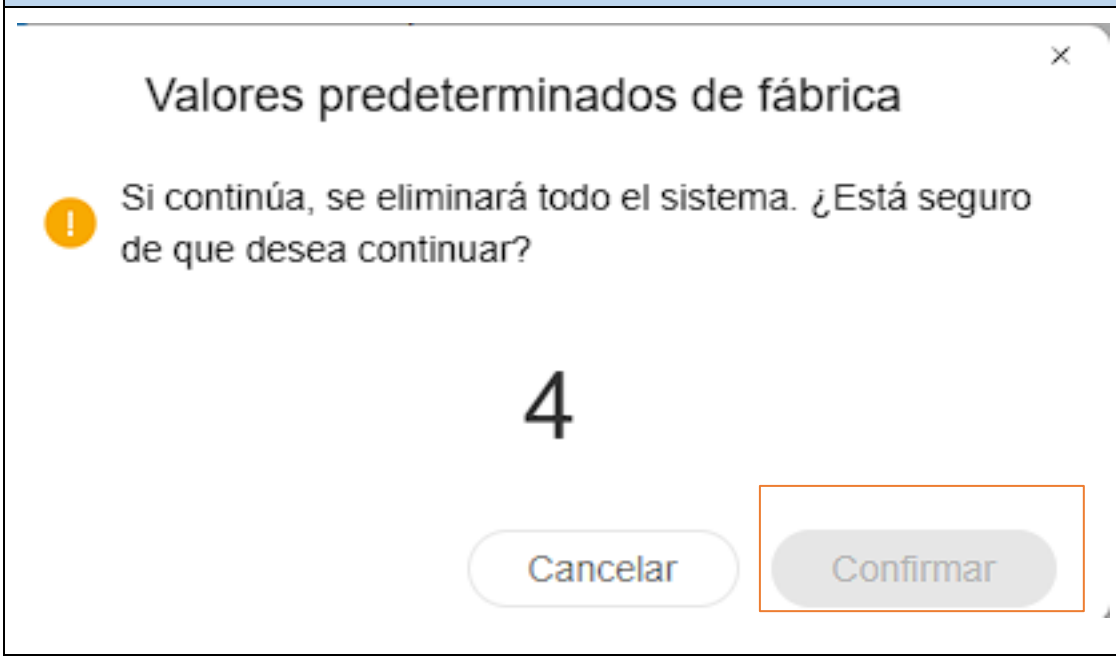
PASO 2

Paso 3 : en la pestaña de valores predeterminados de fábrica seleccionamos el check list : Restaurar a valores predeterminados

PASO 4 : Al tener marcado el check list , seleccionamos en el botón solicitar para que comience la restauración.

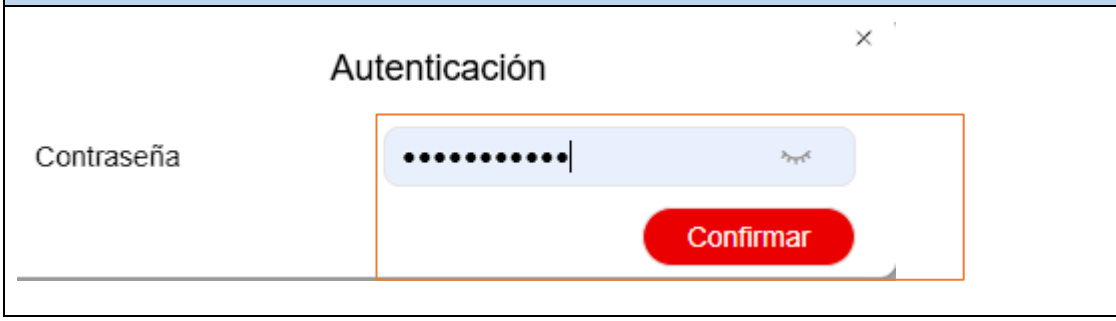


PASO 5 : Confirmamos luego de los 5 segundos

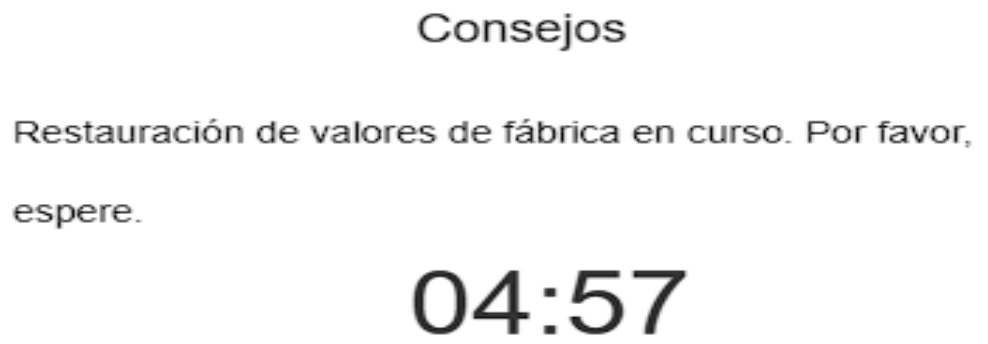


PASO 6 : Para el proceso nos pedirá la Contraseña el cual es : **labCisco_01**

y selecionamos confirmar.



PASO 7 :Próximo , saldrá un mensaje de espera después de 5 minutos , empezará desde 0 toda la configuración.

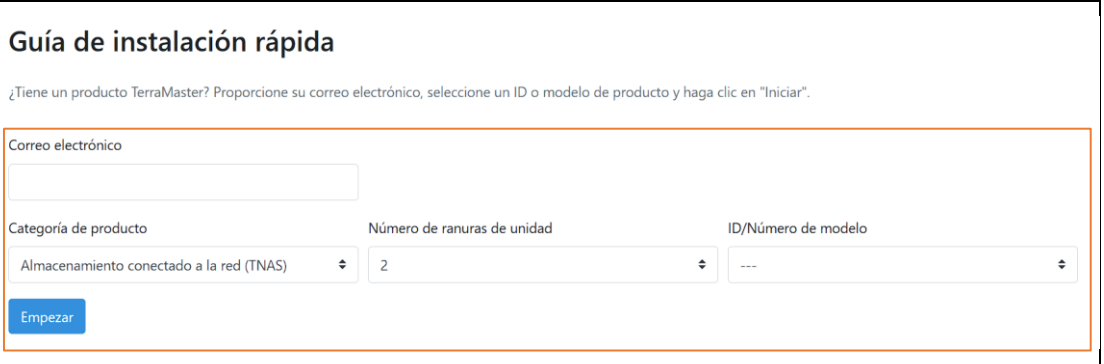


GUIA DE INSTALACIÓN BASICA (APLICA DURANTE LA INCIALIZACIÓN MEDIANTE INSTALACIÓN LIMPIA O TRAS PROCESO DE FORMATEO DEL DISPOSITIVO).

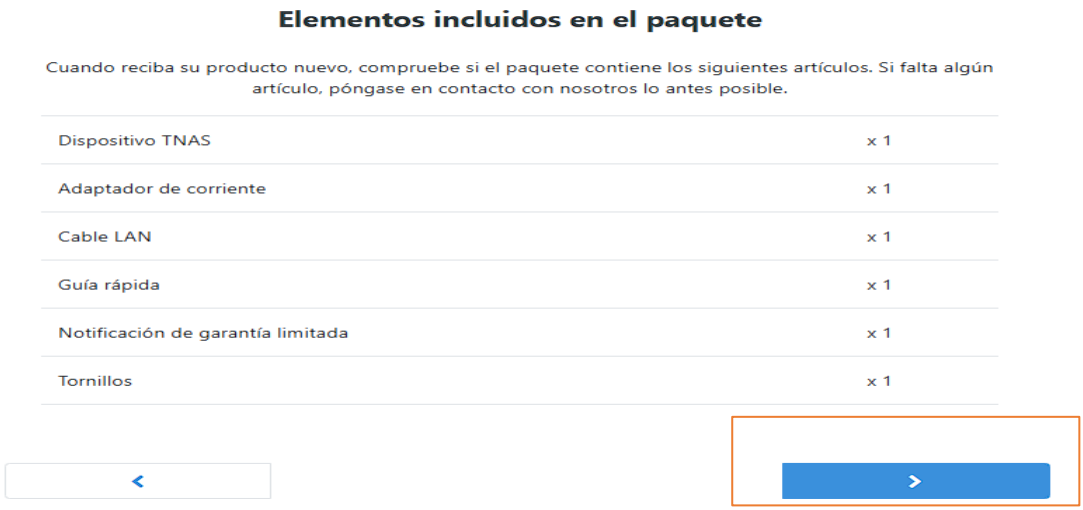
PASO 1:

Link de soporte oficial : https://support.terra-master.com/quickguide/

Agregamos un correo , la categoria seria (TNAS) , el dispositivo tiene 2 bahías, y el Modelo es el F2-212 , una vez cubierto esto , seleccionamos Iniciar.



PASO 2 : Seleccionamos la flecha para avanzar

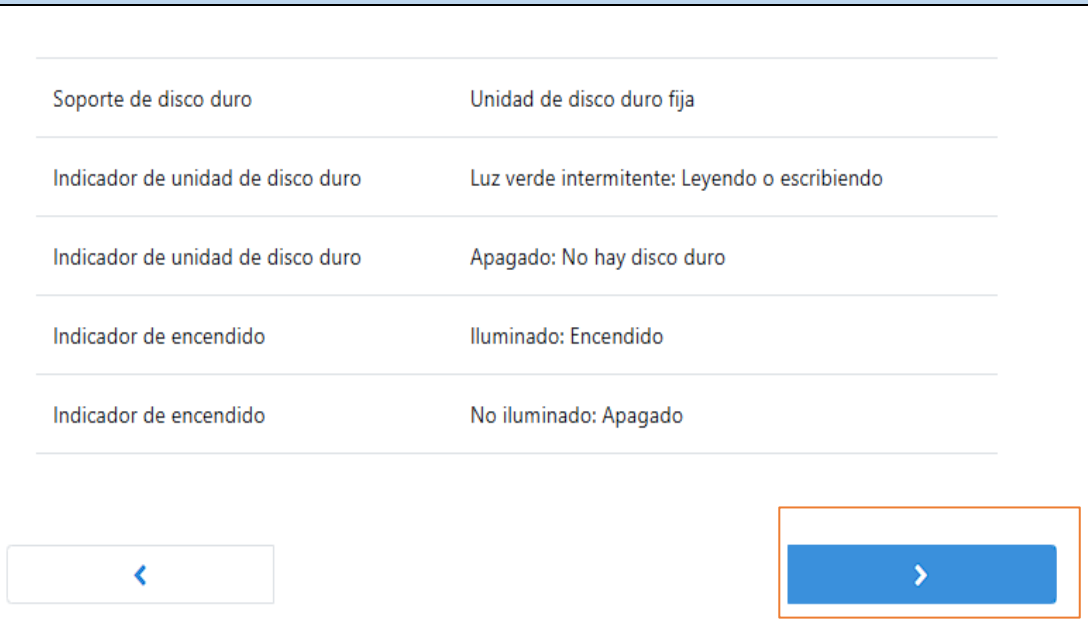


Elementos incluidos en el paquete

Cuando reciba su producto nuevo, compruebe si el paquete contiene los siguientes artículos. Si falta algún artículo, póngase en contacto con nosotros lo antes posible.

Dispositivo TNAS	x 1
Adaptador de corriente	x 1
Cable LAN	x 1
Guía rápida	x 1
Notificación de garantía limitada	x 1
Tornillos	x 1

PASO 3 : Seguimos avanzando con la flecha



Soporte de disco duro	Unidad de disco duro fija
Indicador de unidad de disco duro	Luz verde intermitente: Leyendo o escribiendo
Indicador de unidad de disco duro	Apagado: No hay disco duro
Indicador de encendido	Iluminado: Encendido
Indicador de encendido	No iluminado: Apagado

PASO 4 : continuamos avanzando

Toma de corriente	DC 12V
Puerto LAN x1	Puerto de red 1000 Mbps/100 Mbps
Puerto USB x2	Host USB 3.0 * 1 + host USB 2.0 * 1
Botón de encendido	Pulse brevemente para encender

Nota

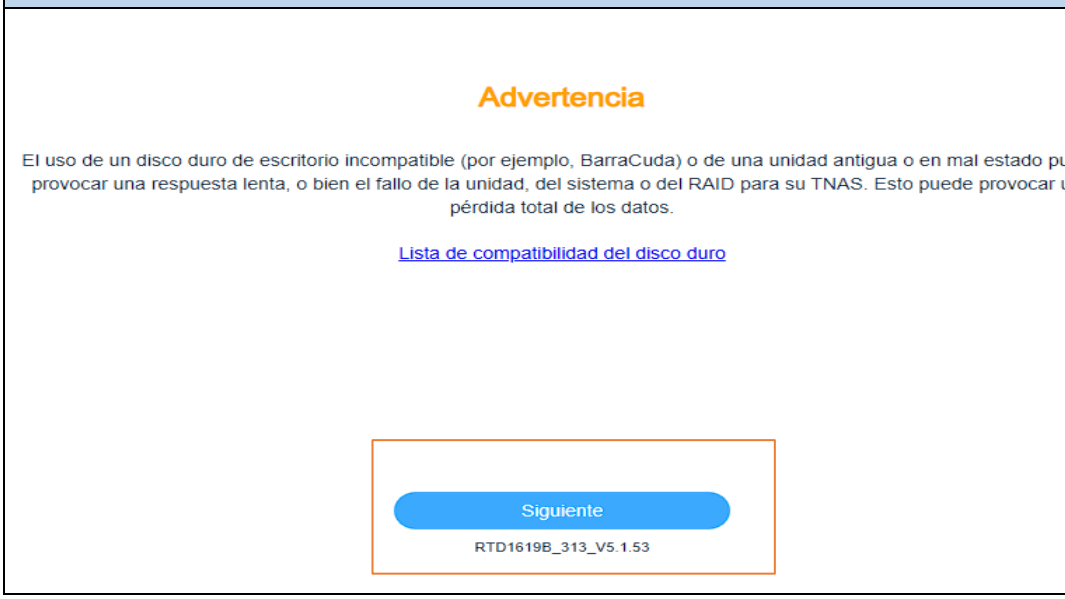
Advertencia: No utilice adaptadores de corriente no oficiales. Si lo hace, corre el riesgo de dañar su dispositivo.

PASO 5 : Indicaciones sobre la instalación del disco duro como anteriormente y seguimos avanzando

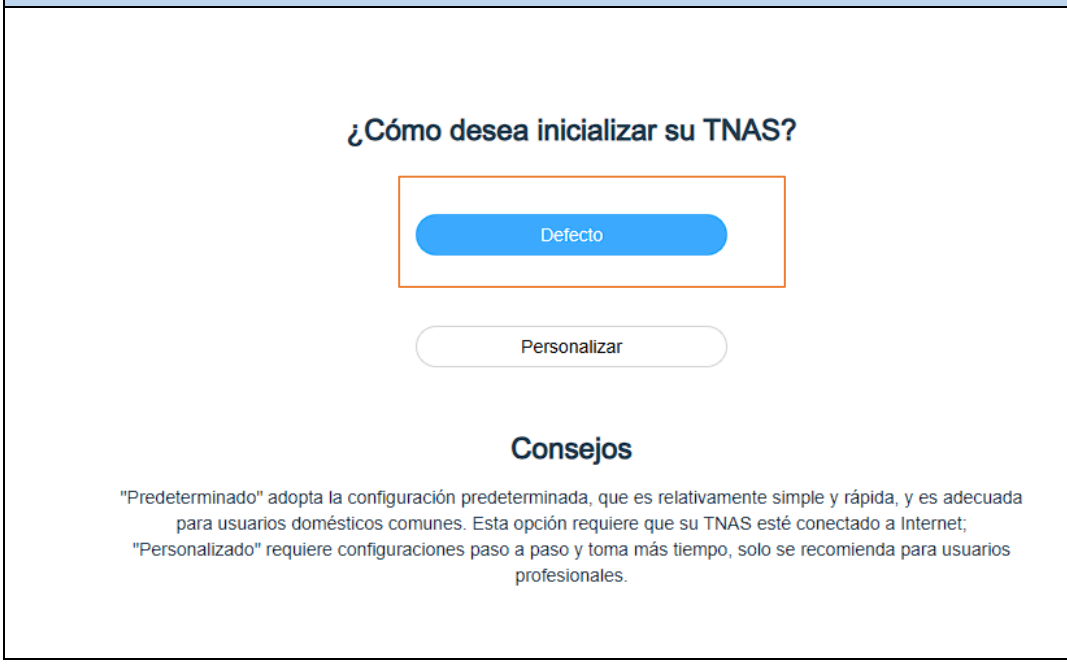
Sujete el disco duro a la bandeja, como se indica.

PASO 6 : Finalmente llegamos a la parte de Iniciar , se nos muestra la IP con la que accederemos al servidor.

PASO 7 : Nos saldrá una breve advertencia la cual podremos ver la lista de Compatibilidad de los discos duros , seleccionamos siguiente para avanzar .

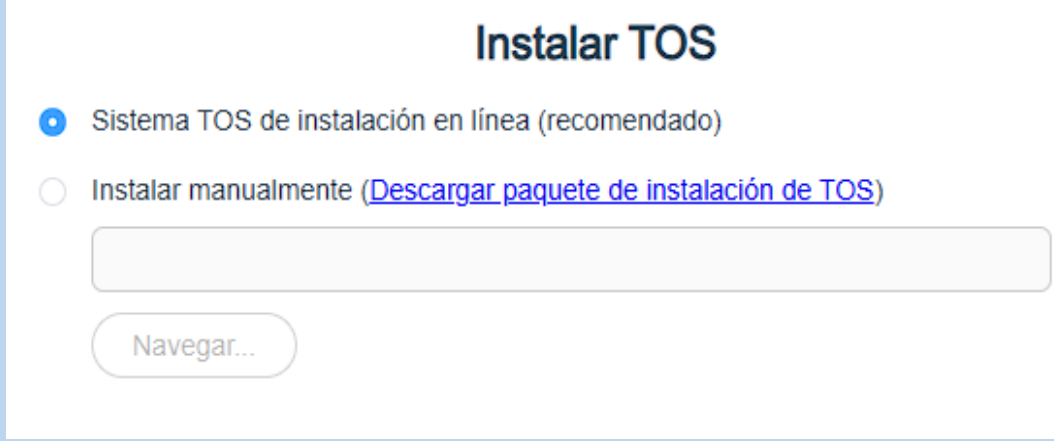


PASO 8 : En esta seccion , podriamos escoger personalidad, para sus repectivas modificaciones , pero escogeremos por defecto.

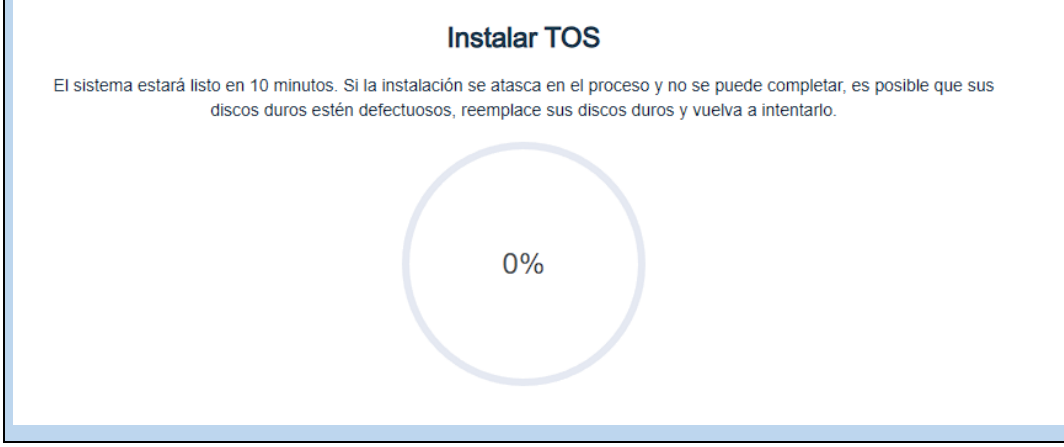


PASO 9 : Comprobación de ambos discos duros y se avanza correctamente

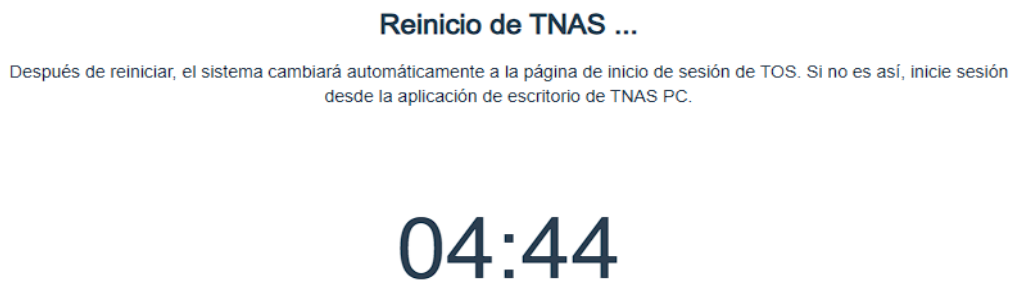
PASO 10 : Seleccionamos instalación en línea



PASO 11 : Proceso de carga de instalación del sistema TOS

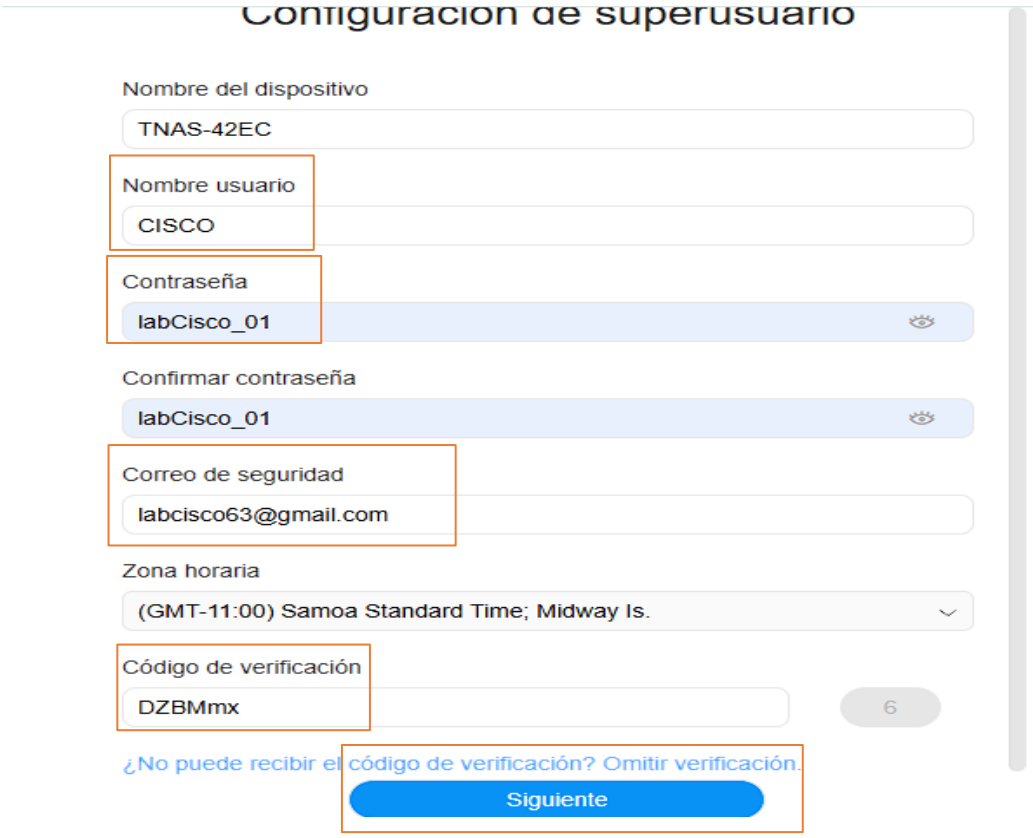


PASO 12 : Tras haberse completado la instalación , esperamos el reinicio del dispositivo

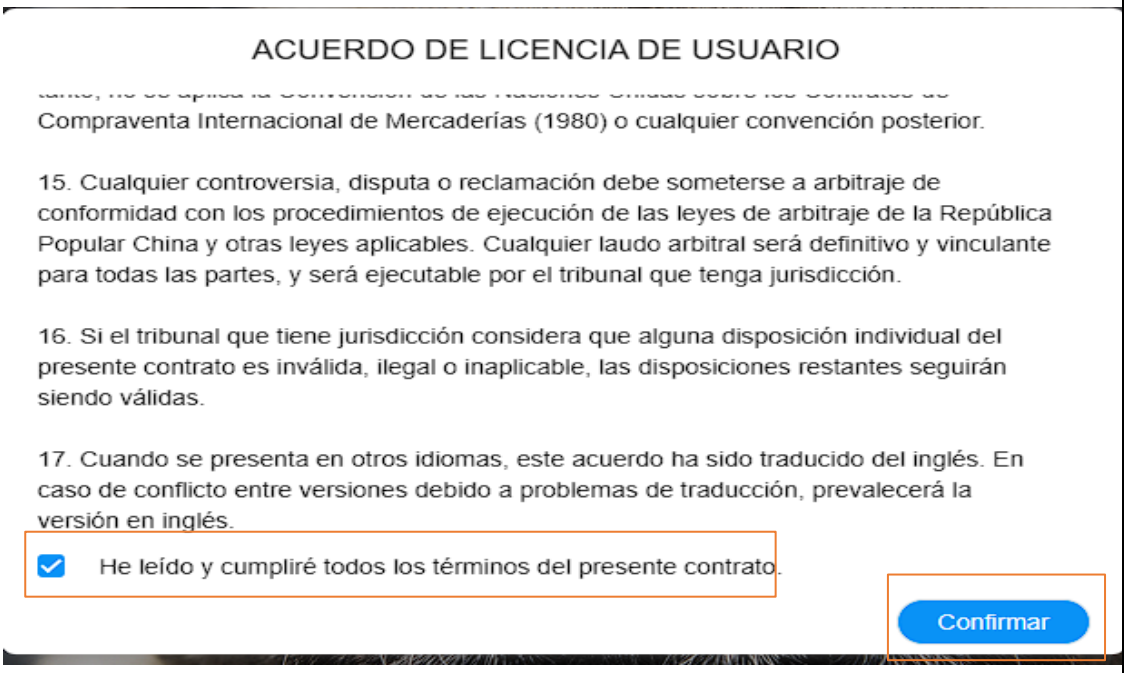


PASO 13 : Configuracion de Super usuario con las siguientes credenciales

Usuario : **CISCO** , Contraseña : **labCisco_01** , correo **:** **labcisco63@gmail.com**, llegará código de verificación al correo y ese código será último paso de esta pestaña

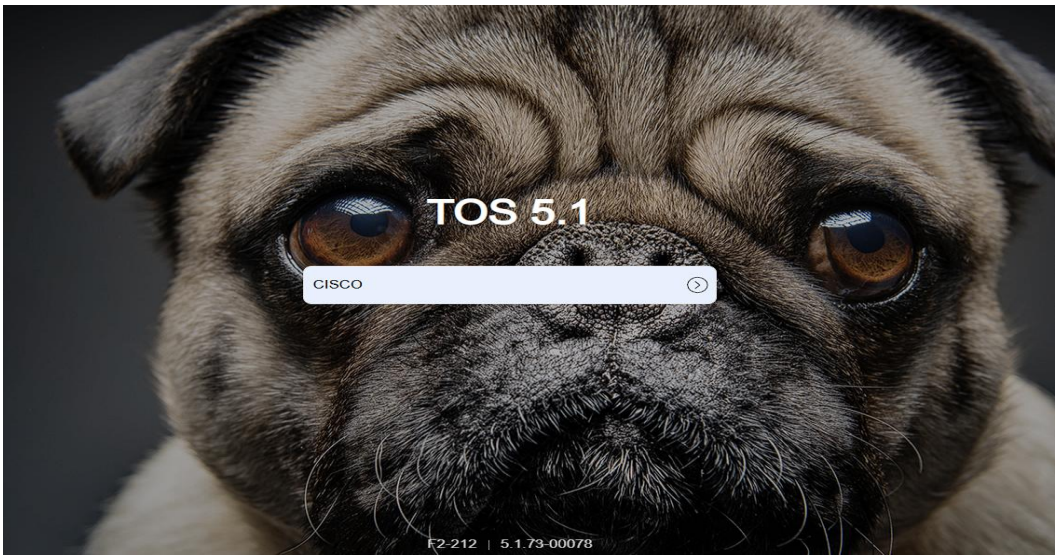


PASO 14 : Marcamos el check list al estar de acuerdo con la licencia de usuario y Confirmamos

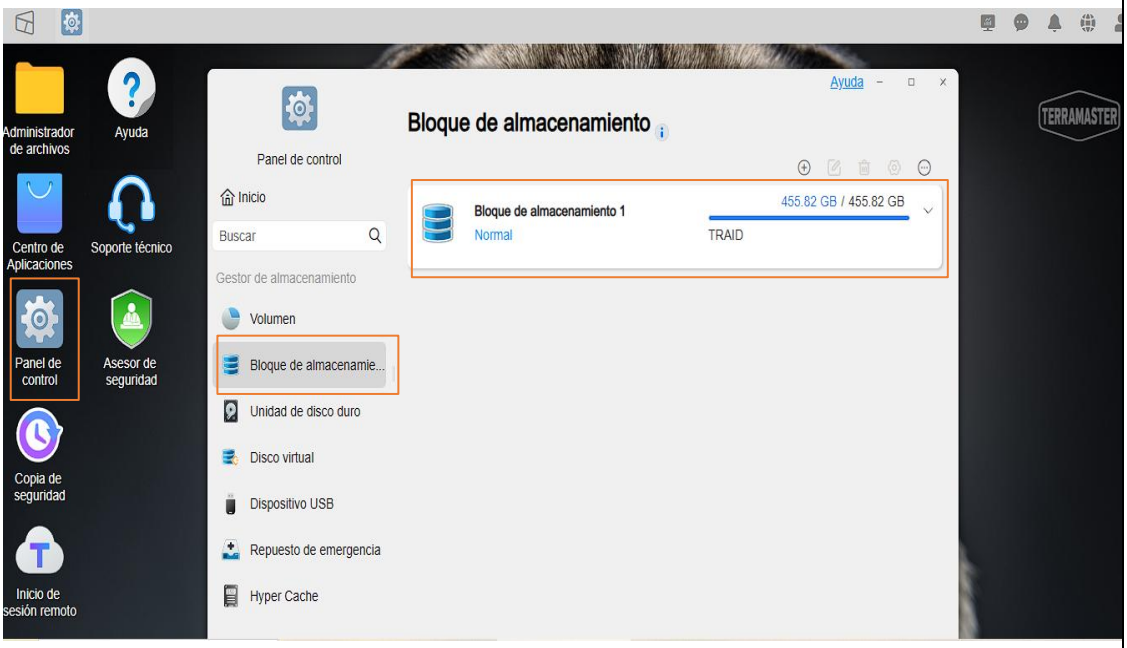


PASO 15 : Ya ingresando al servidor con la IP designado anteriormente , se procede a ingresar con las credenciales.

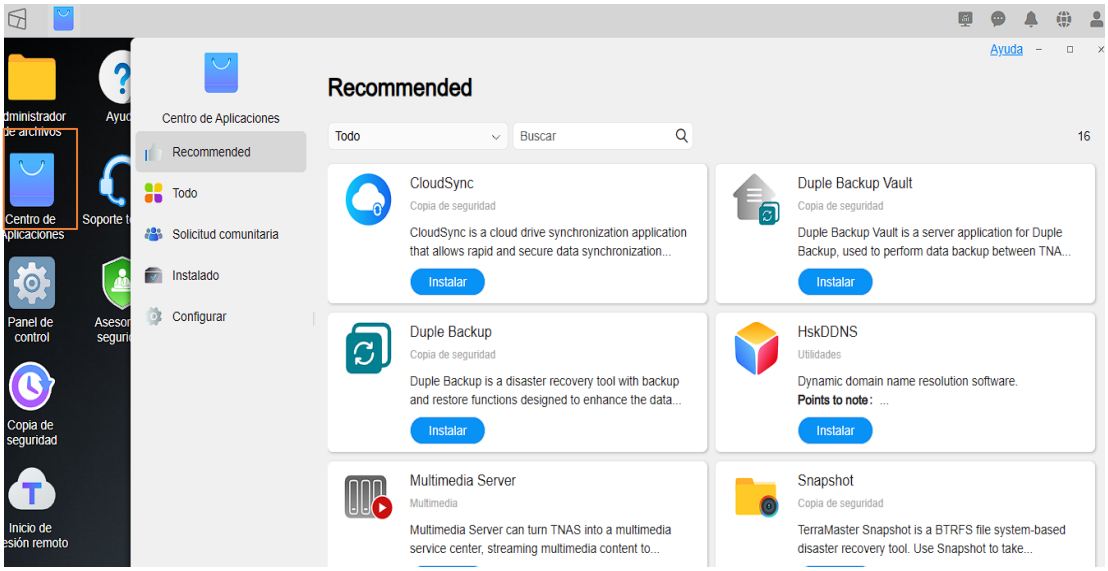
USUARIO : CISCO **CONTRASEÑA** : labCisco_01



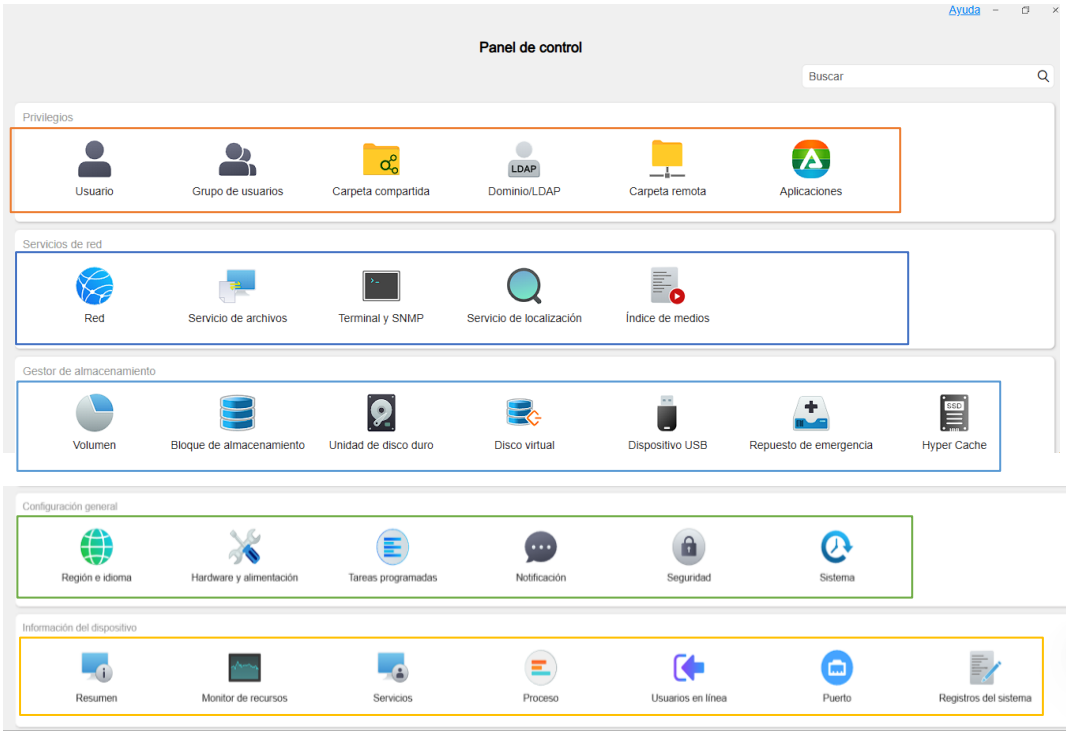
PASO 16 : nos dirigimos al panel de control y verificamos que el arreglo RAID se haya hecho automaticamente en el dispositivo



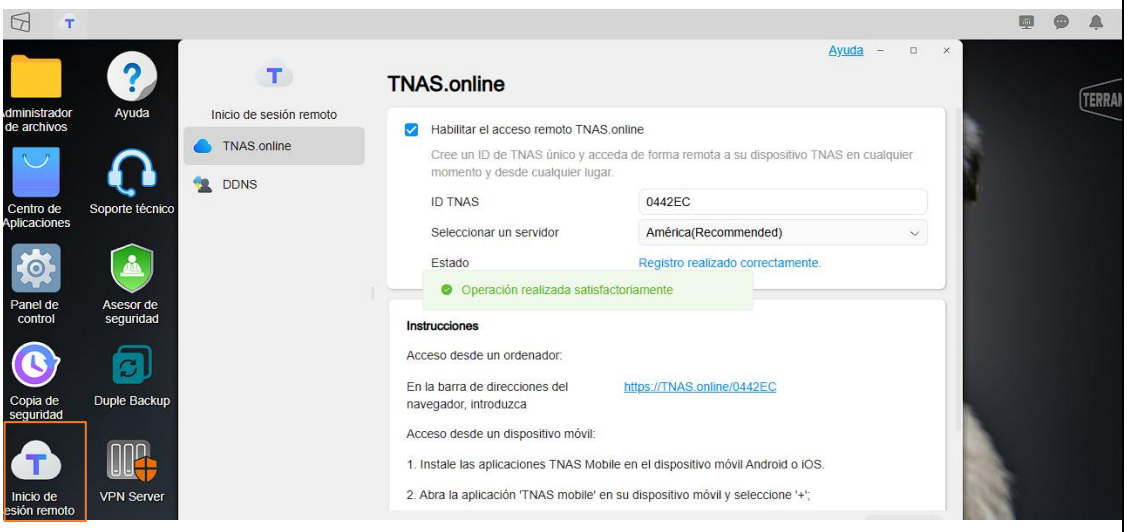
PASO 17 : En app center obtendremos acceso a variedades de software que nos podran servir en diferentes tipos de tarea, dependiendo lo que necesitemos



PASO 18 : En nuestro Panel de control podemos crear usuarios para los accesos necesarios al NAS en caso se requiera , los servicios de red , la gestión de almacenamiento, configuracion general e informacion de dispositivo.



PASO 19 : En inicio de sesión remoto obtendremos como acceder remotamente al NAS desde cualquier lugar con una url.



Acceso al correo del dispositivo vía gmail.

Correo : labcisco63@gmail.com

Contraseña : labCisco_01