PASO 9 - SOLUCIONANDO NECESIDADES ESPECÍFICAS CON GNU/LINUX

Camilo Andrés Enciso Muñoz
E-mail: camiloenciso93@outlook.com

RESUMEN. *Este trabajo se enfoca en la instalación, configuración y prueba de una red privada virtual (VPN) implementada en NethServer, un sistema operativo basado en GNU/Linux que se destaca por su capacidad para gestionar servicios de infraestructura IT en redes de gran escala. La actividad principal consistió en establecer un túnel seguro de comunicación entre una estación de trabajo GNU/Linux y un servidor NethServer, garantizando una conexión remota confiable y protegida para acceder a aplicaciones y recursos en entornos corporativos. A lo largo del proceso, se configuraron adecuadamente las zonas DMZ, redes internas y roles específicos del servidor para asegurar la correcta segmentación de la infraestructura y un flujo de tráfico controlado. La implementación de la VPN incluyó la personalización de parámetros de seguridad, tales como la configuración de protocolos de cifrado y autenticación, así como la validación del acceso mediante pruebas funcionales desde estaciones de trabajo. Los resultados obtenidos muestran que NethServer se presenta como una solución eficaz y sólida para la administración de la infraestructura IT, permitiendo un control robusto de la red y una gestión integral de servicios como VPN, Proxy, Cortafuegos, y servidores de DHCP, DNS y Controlador de Dominio. Finalmente, se discuten las mejoras posibles y los desafíos enfrentados durante la implementación, proporcionando recomendaciones para optimizar futuras configuraciones.*

PALABRAS CLAVE: Redes privadas virtuales, NethServer, administración de servidores, GNU/Linux, seguridad de redes, acceso remoto, configuración de redes, infraestructura de TI, segmentación de red, servicios de red.

INTRODUCCIÓN

En un contexto en el que las organizaciones enfrentan una creciente necesidad de contar con infraestructuras IT sólidas y seguras, se hace imprescindible implementar sistemas que aseguren no solo la conectividad, sino también la protección frente a diversas amenazas, tanto internas como externas. Los servicios como servidores DHCP, DNS, controladores de dominio, proxies, cortafuegos, servidores de archivos, impresoras y redes privadas virtuales (VPN) son elementos clave para garantizar el control adecuado de los recursos y la seguridad en las redes corporativas. Estos servicios permiten gestionar la distribución de direcciones IP, la resolución de nombres de dominio, el filtrado de tráfico, el acceso a datos compartidos y la comunicación remota de forma segura, entre otras funcionalidades esenciales.

Este trabajo se centra en la implementación y configuración de estos servicios utilizando NethServer, una distribución basada en GNU/Linux, especialmente diseñada para la administración de infraestructura IT en entornos corporativos y de gran escala. NethServer proporciona una plataforma modular que facilita la implementación de una amplia variedad de servicios críticos para la gestión de redes, permitiendo a las organizaciones contar con soluciones eficaces para administrar sus recursos de manera centralizada.

A lo largo de este proyecto, se abordarán aspectos clave de la infraestructura de red corporativa, comenzando por la gestión de direcciones IP a través del servicio DHCP, la resolución de nombres con DNS, la creación de entornos seguros mediante cortafuegos y proxies, hasta el establecimiento de redes privadas virtuales (VPN) para comunicaciones remotas seguras. Cada uno de estos componentes desempeña un papel fundamental en la arquitectura de redes modernas, permitiendo a las organizaciones gestionar de forma eficaz el acceso a los recursos, asegurar la integridad y confidencialidad de la información, y mantener un control estricto sobre el tráfico de la red.

El objetivo principal de este proyecto es proporcionar una guía detallada sobre cómo implementar estos servicios de manera eficiente en un entorno de red utilizando NethServer, destacando las mejores prácticas y configuraciones necesarias para asegurar una infraestructura IT que sea estable, segura y eficiente. En este sentido, se hará especial énfasis en cómo las estaciones de trabajo basadas en GNU/Linux interactúan con los servicios proporcionados, garantizando que los usuarios tengan un acceso controlado y seguro a los recursos de la organización.

1 INSTALACIÓN DE NETHSERVER.

1.1 REQUISITOS

Antes de iniciar con la instalación de NethServer, es fundamental asegurar que el equipo cumpla con ciertos requisitos técnicos tanto de hardware como de software

para garantizar un funcionamiento adecuado y eficiente del sistema operativo. A continuación, se detallan los requisitos principales para una instalación exitosa:

REQUISITOS DE HARDWARE

- **MEMORIA RAM**: El sistema requiere un mínimo de 1 GB de RAM para poder ejecutar NethServer de manera estable. Sin embargo, para un rendimiento óptimo, especialmente si se planea utilizar múltiples servicios, se recomienda 2 GB o más.
- **ESPACIO EN DISCO**: Se necesitan al menos 20 GB de espacio libre en disco. Este espacio es necesario para almacenar el sistema operativo NethServer, así como los servicios adicionales que se instalarán, como bases de datos, servidores web y otros servicios de red.
- **PROCESADOR**: NethServer está basado en CentOS, el cual es compatible con procesadores de arquitectura de 64 bits. Por lo tanto, se requiere un procesador de 64 bits para instalar correctamente el sistema operativo.
- **CONEXIÓN A INTERNET**: Es imprescindible contar con una conexión activa a Internet, ya que durante la instalación pueden ser necesarias descargas adicionales de paquetes, así como actualizaciones de seguridad.
- **MEDIO DE INSTALACIÓN**: Se necesita un medio físico o virtual para realizar la instalación. Esto puede ser una unidad flash USB, un CD/DVD o un entorno de máquina virtual como VirtualBox o VMware.

SOPORTE DE HARDWARE

Es esencial verificar que el hardware sea compatible con CentOS, ya que NethServer utiliza esta distribución como base. Se recomienda consultar la documentación oficial de CentOS 7 o superior para confirmar la compatibilidad con el hardware de la máquina.

1.2 ENLACE DE DESCARGA NETHSERVER

La imagen ISO de NethServer está disponible para descarga desde su página web oficial. Para descargar la versión más reciente, sigue el siguiente enlace: https://www.nethserver.org/

Es recomendable seleccionar la versión más actual de NethServer para asegurar que se cuente con las últimas características y actualizaciones de seguridad. En este ejemplo, se utilizará la versión

Una vez descargada la imagen ISO de NethServer, el siguiente paso es proceder con la instalación, ya sea en un entorno físico o virtual. A continuación, se describe el proceso de instalación paso a paso:

Fig 1. Crear la máquina virtual

Fuente: Autoría propia

El primer paso es crear una nueva máquina virtual en el software de virtualización de tu elección, como VirtualBox o VMware. Durante este proceso, es crucial asignar la cantidad adecuada de recursos, como la memoria RAM y el espacio en disco, en función de los requisitos del sistema operativo. En este caso, se asignarán al menos 1 GB de RAM y 20 GB de espacio en disco.

Fig 2. Selección del Boot

Fuente: Autoría propia

Una vez creada la máquina virtual, es necesario seleccionar el dispositivo de arranque para iniciar la instalación. En la figura 2 se muestra la ventana de configuración del "Boot", donde se debe elegir el medio de instalación (USB o DVD). Este paso es esencial para arrancar el sistema desde el medio de instalación de NethServer.

Fig 3. Selección ítem zona horaria

Fuente: Autoría propia

A continuación, el sistema solicitará la configuración de la zona horaria. En la figura 3 se muestra cómo seleccionar la zona horaria adecuada para el servidor. En este caso, se seleccionará "Bogotá, Colombia", para que la hora del sistema coincida con la ubicación geográfica del servidor**.**

Fig 4. Configuración zona horaria

Fuente: Autoría propia

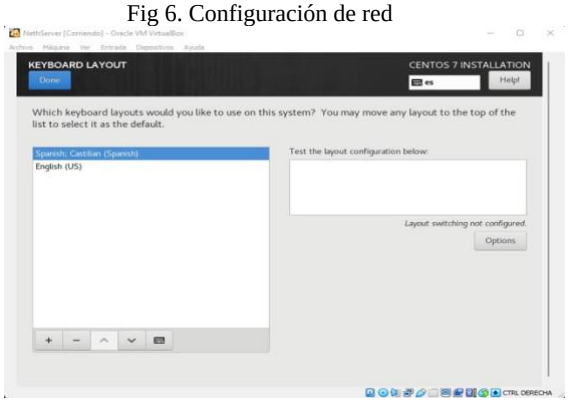
Se configura la fecha y hora del servidor, que es un paso crucial para evitar errores en los registros de eventos y en la sincronización de procesos automatizados.

Fig 5. Configuración del teclado

Fuente: Autoría propia

Este paso permite configurar el idioma y la distribución del teclado. En la figura 5, se elige la opción para configurar el teclado, seleccionando la distribución en español para facilitar la interacción con el sistema operativo.

Fig 6. Configuración de red



Fuente: Autoría propia

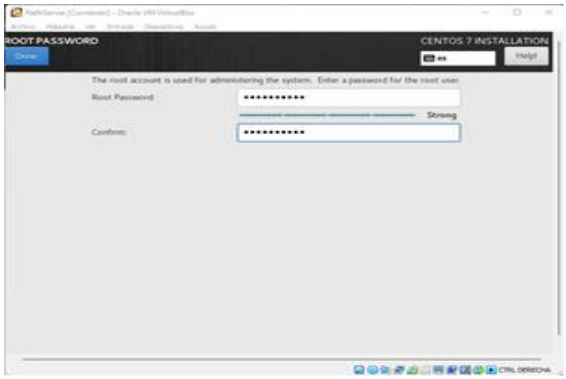
Una vez configurado el idioma, el siguiente paso es configurar las interfaces de red. En la figura 6 se observa cómo asignar configuraciones como direcciones IP estáticas o dinámicas. Es importante asegurarse de que el servidor esté correctamente conectado a la red para garantizar su administración remota y su comunicación con otros dispositivos de la red.

Fig 7. Selección de usuario root

Fuente: Autoría propia

El siguiente paso es configurar el usuario root. En la figura 7 se muestra cómo asignar la contraseña para el usuario root, que es esencial para acceder a la administración del servidor. Es fundamental seleccionar una contraseña robusta y segura para proteger el acceso a la configuración del sistema.

Fig 8. Asignación de clave



Fuente: Autoría propia

El sistema solicitará que se ingrese y confirme la contraseña para el usuario root. Se recomienda una contraseña que contenga una combinación de letras mayúsculas y minúsculas, números y caracteres especiales, para asegurar la protección del sistema.

Fig. 9 Proceso final de configuración e instalación

Fuente: Autoría propia

Al finalizar la instalación, es importante verificar que la dirección IP del servidor esté correctamente configurada. En la figura 10, se muestra cómo utilizar el comando ipconfig o ip a para confirmar la IP asignada al servidor, asegurándose de que esté accesible desde la red.

Fig. 10 Verificación de IP

Fuente: Autoría propia

Este proceso, una vez completado, deja a NethServer listo para ser configurado y utilizado en el entorno de red corporativo o institucional.

2 TEMATICAS

2.1 TEMÁTICA 5: VPN

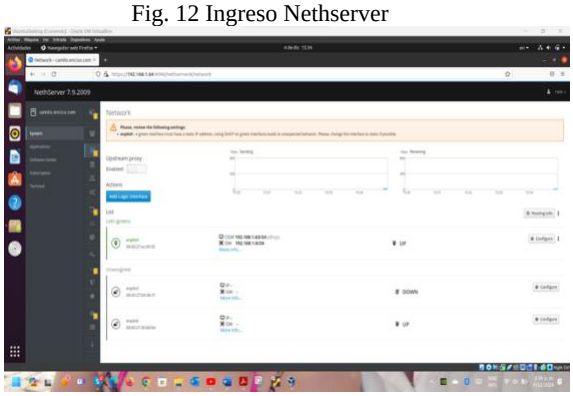
El objetivo de esta temática es establecer una conexión segura y privada entre un servidor NethServer y una estación de trabajo basada en GNU/Linux mediante una VPN. El propósito final es habilitar el acceso remoto exitoso a una aplicación o contenido alojado en la estación de trabajo a través de esta conexión VPN. A continuación, se detalla el proceso paso a paso para configurar y verificar la conexión VPN.

Fig. 11 Ingresar credenciales

Fuente: Autoría propia.

Para comenzar, se ingresan las credenciales de usuario root (nombre de usuario y contraseña) previamente configuradas durante la instalación inicial de NethServer. Este acceso proporciona los privilegios necesarios para administrar la configuración del servidor.

Fig. 12 Ingreso Nethserver



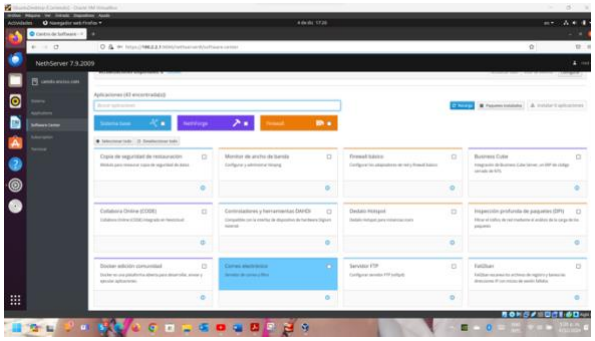
Fuente: Autoría propia.

Dentro de la interfaz de administración de NethServer, es esencial configurar correctamente las zonas de red para garantizar la correcta seguridad y flujo de tráfico. Las zonas definidas por NethServer incluyen:

- **ZONA VERDE (LAN)**: Red interna o local, que incluye los dispositivos dentro de la infraestructura del servidor.
- **ZONA ROJA (WAN)**: Red externa, generalmente conectada a Internet, que maneja el tráfico de la red pública.
- **ZONA NARANJA (DMZ)**: Zona desmilitarizada, diseñada para los servicios que necesitan ser expuestos a la red pública de forma controlada y segura, como un servidor web.

El siguiente paso es instalar el servicio OpenVPN en NethServer. Esto se puede realizar desde el "Software Center" en la interfaz web de administración de NethServer. Para ello, buscamos OpenVPN en el centro de software y seleccionamos la opción de Instalar.

Fig. 13 Descarga de OpenVPN

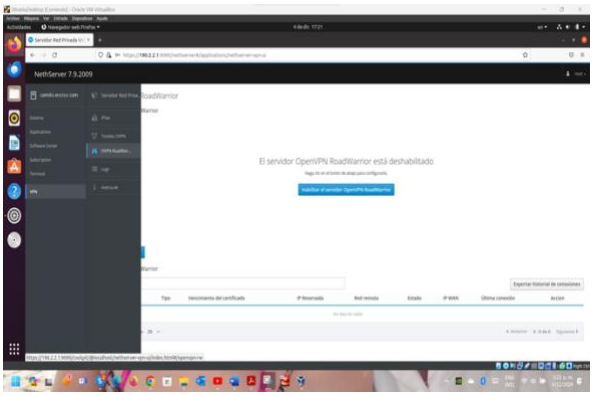


Fuente: Autoría propia.

Con OpenVPN instalado, es necesario configurarlo para establecer la VPN. Para ello, seleccionamos la opción **OVPN RoadWarrior**, diseñada para conexiones de clientes VPN. Se abrirá un formulario donde debemos ingresar los siguientes parámetros clave:

- **MODO DE AUTENTICACIÓN**: Seleccionar **Certificado** para mayor seguridad.
- **MODO**: Seleccionar **Enrutado**, ya que la VPN se configurará para enrutar el tráfico a través del servidor.
- **RED**: Definir la red interna que el cliente VPN podrá acceder. Ejemplo: **10.2.2.0**.
- **MÁSCARA DE RED**: Establecer como **255.255.255.0**.
- **IP/HOST PÚBLICO**: Ingresar la dirección IP pública de la interfaz **WAN** de NethServer (por ejemplo, **192.168.1.64**).

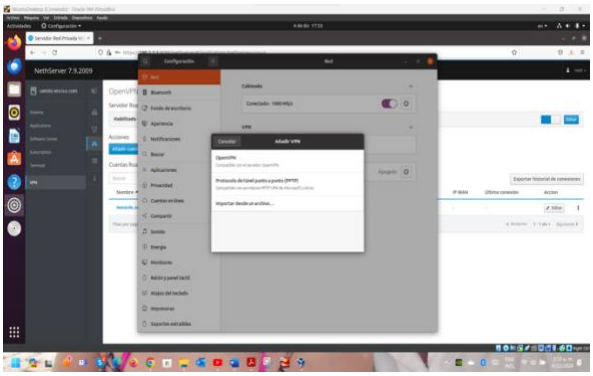
Fig. 14 Configuración OpenVPN



Fuente: Autoría propia

Se selecciona la opción **Solo VPN** y se asigna un nombre de usuario que el cliente utilizará para la conexión. Una vez configurado, aplicamos los cambios para guardar la configuración.

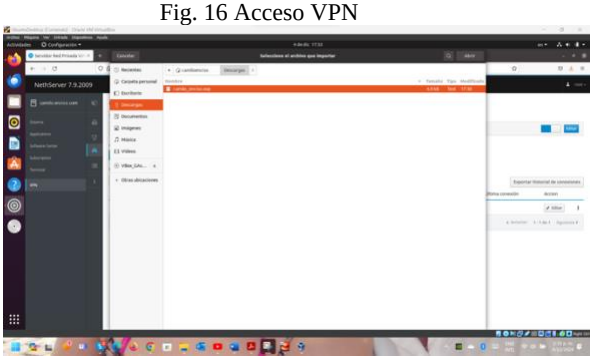
Fig.15 Instalación solo VPN



Fuente: Autoría propia

Una vez completada la configuración en NethServer, es necesario generar un archivo de configuración ovpn que será utilizado por el cliente para establecer la conexión VPN.

Fig. 16 Acceso VPN



Fuente: Autoría propia

Este archivo contiene todos los parámetros necesarios (como la IP del servidor y los certificados de autenticación)

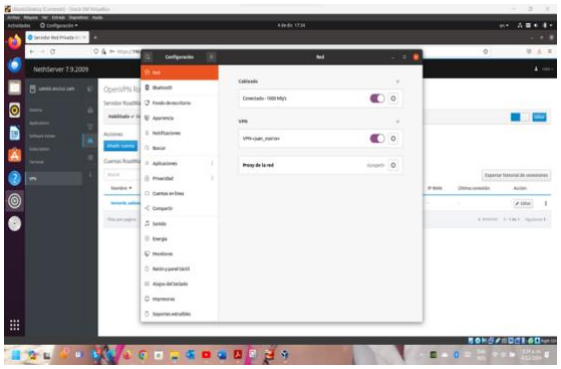
que permitirán al cliente conectarse de manera segura a la red interna.

Fig. 17 Acceso VPN

Fuente: Autoría propia

En la estación de trabajo GNU/Linux (por ejemplo, Ubuntu), se debe importar el archivo .ovpn generado en el paso anterior. Esto se puede hacer a través de la herramienta de redes del sistema operativo, asegurándose de que la VPN esté activada antes de intentar realizar una conexión.

Fig. 18 Acceso VPN

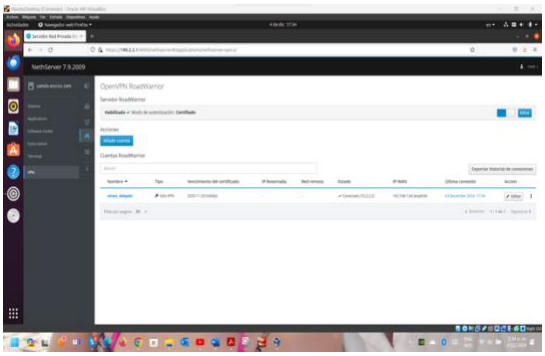


Fuente: Autoría propia

Una vez que la VPN esté configurada y activa en la estación de trabajo, se debe verificar desde el panel de administración de NethServer que la conexión del cliente se haya establecido correctamente. Para ello, se pueden consultar los registros del sistema o usar herramientas de monitoreo de red de NethServer.

- Verifique que la **IP del cliente** aparezca en los registros de conexión.
- Asegúrese de que la conexión esté activa y que el tráfico esté siendo correctamente enrutado a través de la VPN.

Figura 18 Evidencia de la conexión en Nethserver



Fuente: Autoría propia

Finalmente, para confirmar que la configuración de la VPN es exitosa, intente acceder a una aplicación o contenido alojado en la estación de trabajo desde la red remota. Si la conexión es exitosa, el acceso a los recursos internos será transparente y seguro a través del túnel VPN.

2.2 TEMÁTICAS COMPLETAS

Tabla 1 - Tematicas.

Estudiantes	Links:
CAMILO ANDRES ENCISO MUNOZ	https://docs.google.com/document/d/1bPd7GFQuyl6ZEVgCBG9Huk4VmIja3pkA/edit

Fuente: Autoría Propia

VIDEOS SUSTENTACIÓN

Tabla 2 video sustentación.

Estudiantes	Links:
CAMILO ANDRES ENCISO MUNOZ	https://drive.google.com/drive/folders/11jL81BuKqqUeZAqEKEC18sZZR8xNycQ-

CONCLUSIONES

El proyecto desarrollado ha sido exitoso en la implementación de diversos servicios de infraestructura IT utilizando NethServer, un sistema operativo basado en GNU/Linux. A través de este proceso, se configuraron y optimizaron una serie de servicios esenciales para administrar y asegurar una red eficiente en el entorno organizacional. Los servicios implementados incluyen DHCP Server, DNS Server, Controlador de Dominio, Proxy, Cortafuegos, File Server, Print Server y VPN, cubriendo un amplio espectro de configuraciones que garantizan el correcto funcionamiento y la seguridad de la red corporativa.

1. Configuración de Servicios de Red

Uno de los principales logros fue la implementación y configuración adecuada del DHCP Server, DNS Server y Controlador de Dominio, lo cual permitió la correcta integración y registro de las estaciones de trabajo GNU/Linux en la infraestructura de NethServer. A través de estos servicios, se optimizó la asignación dinámica de direcciones IP, garantizando que las estaciones de trabajo pudieran conectarse de manera eficiente y segura a la red. Además, la creación de cuentas de usuario con acceso controlado, mediante el uso de credenciales (usuario y contraseña), proporcionó un mecanismo eficaz para administrar y restringir el acceso a la red, mejorando así el control sobre los dispositivos conectados.

2. Control de Acceso a Internet mediante Proxy

La implementación del Proxy en el puerto 3128 permitió gestionar y filtrar el tráfico de salida hacia la red externa (Internet). Este paso fue crucial para controlar el acceso de las estaciones de trabajo GNU/Linux a sitios web externos, especialmente aquellos no relacionados con las actividades laborales. Además de contribuir a una navegación más segura, el proxy mejoró el rendimiento de la red, ya que bloqueó el acceso a sitios web no deseados, optimizando el uso de recursos y garantizando una mayor productividad en la organización.

3. Seguridad Mejorada con Cortafuegos

El Cortafuegos (Firewall) fue configurado con reglas y políticas específicas que restringen el acceso a sitios web no esenciales, como redes sociales y sitios de entretenimiento. Estas políticas no solo protegieron la infraestructura interna de accesos indeseados, sino que también ayudaron a minimizar las distracciones de los usuarios. La configuración del cortafuegos permitió un control de tráfico más granular, asegurando que solo el tráfico necesario para las actividades empresariales pudiera acceder a la red, lo que contribuyó a mejorar la seguridad y la productividad de la organización.

4. Gestión Centralizada de Recursos con File Server y Print Server

La implementación del File Server y el Print Server permitió centralizar la gestión de archivos e impresión dentro de la red. Los usuarios de las estaciones GNU/Linux pudieron acceder de manera eficiente a carpetas compartidas y impresoras configuradas en el servidor. Esto no solo mejoró la administración de recursos, sino que también facilitó la colaboración entre usuarios, ya que los archivos podían ser accedidos y compartidos de forma centralizada a través del Controlador de Dominio LDAP, lo que fortaleció la seguridad y el control de acceso a los datos sensibles de la organización.

5. Conexión Remota Segura a través de VPN

Uno de los logros más destacados de este proyecto fue la implementación de la VPN (Virtual Private Network), que permitió establecer un túnel privado de comunicación entre la estación de trabajo GNU/Linux y el servidor NethServer. Este servicio proporcionó una forma segura y eficiente de acceder de manera remota a recursos y aplicaciones dentro de la red interna. La implementación de la VPN no solo mejoró la conectividad externa, sino que también garantizó que los datos y la comunicación entre la estación de trabajo y el servidor se mantuvieran protegidos contra accesos no autorizados, ofreciendo una solución robusta y segura para la conexión remota.

6. Reflexión sobre el Uso de NethServer y Tecnologías de Código Abierto

Este proyecto permitió consolidar y aplicar los conocimientos adquiridos en la gestión de servidores y servicios de infraestructura IT, demostrando cómo una configuración adecuada y la administración eficaz de estos servicios puede mejorar significativamente la seguridad, la conectividad y la eficiencia de la red dentro de una organización. La implementación exitosa de NethServer y sus servicios asociados resalta la importancia de utilizar tecnologías de código abierto, no solo por sus beneficios económicos, sino también por la flexibilidad y escalabilidad que ofrecen para gestionar y optimizar los recursos tecnológicos de una institución.

Este proyecto también subraya la relevancia de contar con una infraestructura de red bien configurada, que no solo sea segura, sino también eficiente, escalable y flexible para adaptarse a las necesidades cambiantes de la organización. Con la correcta implementación y gestión de estos servicios, NethServer ha demostrado ser una plataforma sólida y confiable para satisfacer los requerimientos tecnológicos de las empresas modernas.

REFERENCIAS

[1] Barker, I. (2016). *Virtual Private Networks (VPNs): Conexiones seguras para redes corporativas*. Packt Publishing.

[2] Cano, A., & Ortiz, M. (2012). *Seguridad informática y redes: Un enfoque práctico*. Ediciones UCM.

[3] Hernández, R., Fernández, C., & Baptista, P. (2010). Metodología de la investigación (5.ª ed.). McGraw-Hill.

[4] López, J., & Rodríguez, V. (2017). *Tecnologías de la información y comunicaciones en la empresa: Gestión e infraestructura* (3.ª ed.). Editorial Pirámide.

[5] Mayer, R., & Sánchez, J. (2018). Redes y comunicaciones en entornos corporativos. Editorial Alfaomega.

[6] NethServer Community. (2020). NethServer manual. NethServer Community. https://docs.nethserver.org

[7] Olivares, P. (2013). *Administración de redes* (2.ª ed.). Editorial Prentice Hall.

[8] Radwan, A. (2019). *Guía práctica para la implementación de servidores con GNU/Linux*. Editorial Raso.

[9] Stallings, W. (2015). Seguridad en redes de computadoras (7.ª ed.). Pearson.

[10] Zúñiga, L. (2014). Redes de computadores y telecomunicaciones. Pearson Educación.