

FACULTAD DE CIENCIAS
EXACTAS Y NATURALES

Universidad Nacional de La Pampa

Tecnicatura en Informática de Gestión

Plan para la realización del Trabajo Final Integrador

Despliegue de Servidor Doméstico Multiusuario

Franco Joel Luque Haim

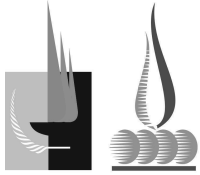
francofjlh@gmail.com

Tutor

Leandro Castro

castro.leandro@exactas.unlpam.edu.ar

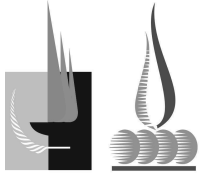
2026



Resumen

A partir de este trabajo se busca visibilizar y reafirmar la presencia de los contenedores, dentro del *cloud computing*, como una de las tecnologías más versátiles y veloces de implementar a la hora de montar nuestros propios laboratorios de prueba destinados al uso de prácticas y/o *servidores domésticos*, así también como la construcción de entornos en producción para empresas de diferentes escalas. El *cloud computing* se presenta como una solución tecnológica que busca desplazar a los servidores físicos y utilizar servidores virtuales mediante la nube y servicios dedicados al almacenamiento de información y aplicaciones.

En el presente trabajo se pretende abordar la problemática referida a la falta de soberanía sobre nuestra información y los elevados precios de algunas plataformas Cloud que ofrecen servicios de almacenamiento. Hoy en día es muy sencillo llenar los 15 Gb de almacenamiento gratuito que ofrece Google asociados a una cuenta, y si bien existen soluciones como crear cuentas a medida que se requiere de más espacio, no terminan de ser opciones ideales, muchos menos si dejamos de lado el ámbito personal y nos enfocamos en alguna pequeña o mediana empresa, pues resulta poco conveniente y/o práctico que una organización haga uso de múltiples cuentas solamente para paliar la falta de espacio de almacenamiento en la nube.



Introducción

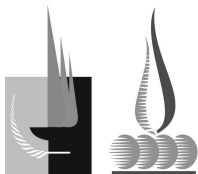
El tema que elegí para desarrollar como Trabajo Final Integrador es el Diseño de una Nube Privada que cumpla con las principales exigencias que suele tener un usuario final al hacer uso de un sistema de Información. Lo que busco es diseñar y desplegar un pequeño servidor en una computadora de escritorio que se encuentre disponible, independientemente del lugar y momento en el que se intente acceder, siempre y cuando se cuente con una conexión a internet.

La idea principal es implementar un servidor de archivos que le facilite al usuario final un espacio de almacenamiento que dependa exclusivamente de la capacidad y cantidad de discos instalados sobre la estación de trabajo, cosa que no sucede al hacer uso de servicios como Google Drive, OneDrive o Dropbox, donde el espacio a utilizar depende del plan que se tenga contratado. De esta forma, otra ventaja que tienen los usuarios es que poseen el control y la potestad total sobre la información que deciden o no almacenar en el servidor, sin depender de servicios de terceros o de limitaciones en almacenamiento.

La construcción de este servidor, será un banco de pruebas que permitirá hacer un uso personal, logrando escalar a un punto de resultar de relevancia para pequeñas y medianas empresas que requieran una manera de centralizar su información e incrementar su productividad a través del trabajo remoto.

Un punto importante a considerar también es la viabilidad del proyecto en cuanto a tiempos de producción y a conocimientos personales para llevarlo a cabo. A partir de esto, se puede estimar que con los conocimientos adquiridos a lo largo de la carrera se puede lograr un primer acercamiento a lo que exige la propuesta, pero se requiere de investigación sobre las tecnologías concretas a utilizar, más en un punto en el que se requiera de nuevas funcionalidades.

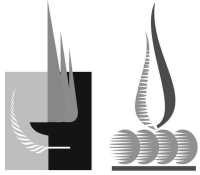
Una vez expuesto lo anterior, ¿qué relevancia tiene el tema elegido en el contexto de la Tecnicatura en Informática de Gestión? El desarrollo de este proyecto otorga muchos conocimientos sobre cómo funcionan muchos de los servicios en la nube hoy en día y a la vez se explora el funcionamiento de muchas herramientas útiles para el trabajo diario en



FACULTAD DE CIENCIAS
EXACTAS Y NATURALES

Universidad Nacional de La Pampa

Sistemas de Información. Si exploramos el perfil del egresado y lo relacionamos con el desarrollo del proyecto, vemos que el mismo exige conocimientos sobre el uso e implementación de recursos y tecnologías de acceso abierto, punto que se relaciona intrínsecamente con el desarrollo del presente proyecto.

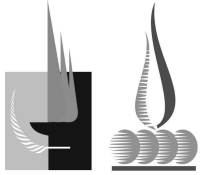


Objetivos

Como objetivo general de mi trabajo, propongo diseñar una infraestructura de nube privada haciendo uso de contenedores y máquinas virtuales.

Y, en cuanto a los objetivos específicos:

1. Diferenciar Máquinas Virtuales de Contenedores, definiendo en qué casos es pertinente utilizar cada una de estas tecnologías.
2. Definir reglas para establecer una seguridad básica en la infraestructura de nube privada.
3. Implementar acceso remoto junto con herramientas de gestión y compartición de archivos.

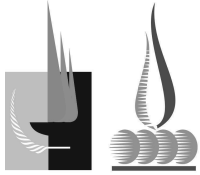


Marco teórico

En el presente apartado se presentarán los conceptos teóricos y tecnológicos fundamentales que sustentan el diseño e implementación de una nube privada en un *servidor doméstico*, haciendo uso de virtualización, contenedores y software de código abierto. Se abordarán definiciones, enfoques y tecnologías que permiten comprender el funcionamiento y la pertinencia de la solución planteada.

Tradicionalmente, cuando se piensa en servicios de almacenamiento en la nube, la primera opción como solución es la utilización de aplicaciones como *Google Drive*, *OneDrive* o *DropBox*. Sin embargo, al decantarnos por una de estas soluciones, estaremos confiando nuestros archivos e información a servicios y servidores de terceros, generando una dependencia de los mismos. Pero el avance en la *virtualización* y la *contenerización* ha permitido la implementación de servicios de características similares en redes propias, incluso con hardware pensado para uso personal fuera de entornos de servidores. Esta alternativa promueve la *soberanía digital*, la *independencia tecnológica* y la *privacidad de la información*.

Es entonces que surge la idea de diseñar una *nube privada* que se adapte a las necesidades particulares de cada usuario y que posee como limitante la cantidad/calidad de hardware del que se disponga. ¿Qué se entiende por el concepto de nube privada? Según la documentación oficial de Google Cloud (2025), “una nube privada es un modelo de implementación de computación en la nube en el que todos los recursos de la nube están destinados a un solo cliente o a una organización”. Esta definición se corresponde con el servicio que ofrece Google Cloud, cuyos servidores, se encuentran disponibles en sus propios centros de datos a los que accedemos de manera remota. Aun así, este concepto de Nube puede ser aplicado a casos en los que los recursos se encuentren accesibles de manera física por usuarios finales, por ejemplo en una PC de escritorio conectada a una pequeña red local de un hogar. A diferencia de las nubes públicas, en las que los recursos son compartidos entre múltiples clientes, en una nube privada el control, la seguridad y la personalización están completamente en manos del propietario del sistema.

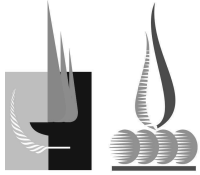


Entonces una nube privada en este contexto representa una infraestructura de computación que está dedicada exclusivamente a un único usuario o grupo de usuarios dentro de una organización o red local. La idea central de una Nube propiamente dicha, es encontrarse siempre accesible desde cualquier sitio, en cualquier momento y es este tipo de solución la que permite ofrecer servicios como almacenamiento, sincronización de archivos, calendarios, mensajería, y colaboración en línea, todo dentro de un entorno gestionado por el propio usuario, maximizando la privacidad y reduciendo la dependencia de servicios externos.

Ahora bien, para lograr este objetivo se deben de utilizar tecnologías existentes en la actualidad que son de mucha relevancia para gestionar de una mejor manera los recursos de hardware de los que disponemos.

Lo primero sobre lo que se debe de hablar es la *virtualización*, tecnología que permite crear varios entornos simulados o recursos específicos desde un solo sistema de hardware físico (RedHat, 2024). Esto se logra a través de software llamado *hipervisor*, que administra los recursos del sistema y los distribuye entre las *máquinas virtuales* (instancias simuladas de un sistema operativo completo). Las mismas permiten alojar servicios o sistemas con distintos propósitos, manteniéndolos aislados para aumentar la seguridad, la estabilidad y la facilidad de mantenimiento. En contextos hogareños o de bajo presupuesto, herramientas como *Proxmox VE* ofrecen una solución fiable de virtualización híbrida, es decir que permite gestionar tanto máquinas virtuales como *contenedores* desde una interfaz centralizada. Su uso otorga la posibilidad de crear entornos de prueba y despliegue funcionales para las diferentes aplicaciones que se estarán utilizando. Cabe aclarar que Proxmox VE es un hipervisor de tipo 1 denominado “*bare-metal*” (expresión en inglés atribuida a un dispositivo sin sistema operativo), es decir que se ejecuta directamente sobre el hardware, a diferencia de los hipervisores más conocidos de tipo 2 que lo hacen sobre un sistema operativo anfitrión, siendo *Virtualbox* el exponente más popular de los mismos.

Es a partir de hipervisores como Proxmox VE que se hace uso de **máquinas virtuales** y **contenedores**, herramientas claves para el desarrollo de la computación en la nube. Ambas tecnologías se apoyan en la virtualización, pero la aplican de distintas maneras. Mientras



que las máquinas virtuales hacen uso de su propio núcleo o *kernel* para funcionar, los contenedores comparten el mismo *kernel* instalado sobre el equipo anfitrión.

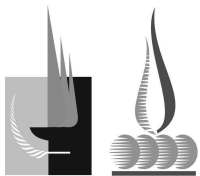
Un concepto clave que se debe introducir en este punto es el de *contenerización*, proceso que permite empaquetar una aplicación y todas sus dependencias en un contenedor ligero que podrá ejecutarse en cualquier entorno compatible. A diferencia de las máquinas virtuales, los contenedores comparten el mismo *kernel* del sistema operativo anfitrión, lo que los hace más eficientes en términos de rendimiento y uso de recursos.

Aunque muchas aplicaciones ya cuentan con versiones contenerizadas para ser utilizadas a través de Proxmox VE, muchas otras aún no permiten esto de *manera nativa*¹ para el hipervisor. Por lo tanto, se introduce el uso de *Docker* y *Docker Compose*, tecnologías que han revolucionado la forma en la que se implementan servicios al permitir el empaquetado de aplicaciones junto con sus dependencias. Esto garantiza que los entornos sean portables, ligeros y reproducibles. Su uso permite el orquestado de los servicios que se utilizan en muchos servidores (almacenamiento, herramientas de comunicación y servicios multimedia).

Docker es la herramienta más utilizada para contenerización y para hacer uso de ella se necesita de un sistema operativo con un *kernel* que los contenedores puedan utilizar, y es en este punto en el que entran en juego software de sistema como *Ubuntu Server*, una distribución de *GNU/Linux* ampliamente utilizada en servidores y reconocida por su estabilidad, compatibilidad con software moderno y facilidad de administración.

Una vez lograda la base sobre la cual se instalarán los servicios, se debe de elegir el software necesario. Para el almacenamiento en la nube, existe el caso de *Nextcloud*, una plataforma de código abierto que permite la creación de un espacio colaborativo completo que incluye almacenamiento, edición colaborativa de documentos, calendarios, gestión de tareas, videollamadas (a través de *Nextcloud Talk*) y más extensiones que pueden ser anexadas a medida que se las requiera. En este proyecto, Nextcloud actúa como el núcleo

¹ Si bien estas aplicaciones requieren ser descargadas para utilizarlas, Proxmox tiene de manera nativa un listado con las mismas pre descargadas.



de la nube privada, funcionando como interfaz principal de usuario y punto de integración de los servicios colaborativos.

Todas estas tecnologías pertenecen a lo que se denomina *software open source* (o software de código abierto), aquel cuyo código fuente está disponible públicamente para que cualquier persona pueda estudiarlo, modificarlo y redistribuir con pocas o ninguna restricción. Según una definición de IBM², “*el software de código abierto es software desarrollado y mantenido mediante colaboración abierta. Está disponible para que cualquiera lo use, lo examine, lo modifique y lo redistribuya como quiera, generalmente sin coste alguno*”.

Finalmente, un último punto a abordar es el correspondiente al acceso remoto de toda esta infraestructura a desplegar, puesto que el objetivo es lograr el acceso a la información almacenada desde fuera de la red local sobre la que se encontraría funcionando. Y, en este punto es en donde entra en juego Tailscale, una solución de red superpuesta (*overlay network*) que permite crear una red privada virtual (VPN) en malla³ (*mesh*), basada en el protocolo *WireGuard*⁴.

A diferencia de las VPN tradicionales de configuración "estrella" (donde todo el tráfico se centraliza en un único servidor *gateway*), Tailscale conecta los dispositivos de manera directa (punto a punto) entre sí, sin importar dónde estén configurados o detrás de qué firewalls se encuentren. El tráfico de datos real nunca pasa por los servidores de Tailscale; viaja cifrado directamente entre los nodos añadidos a la *tailnet*⁵.

Esta *tailnet* sienta las bases de su seguridad sobre 2 pilares fundamentales denominados *Planos de Control* (para la coordinación) y *Planos de Datos* (para el procesamiento y transporte real de los paquetes de información).

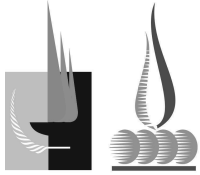
El Plano de Control se encarga de la gestión, la lógica y la configuración de la red. Su función principal no es mover archivos, sino intercambiar la información necesaria para

² IBM (s.f.). Recuperado de <https://www.ibm.com/es-es/topics/open-source>.

³ Los nodos se comunican directamente en lugar de triangular a través de un servidor central.

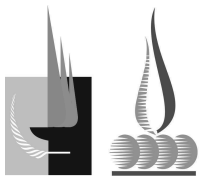
⁴ Protocolo de comunicación y un software libre de código abierto.

⁵ Una *tailnet* no es más que el nombre popularizado por Tailscale que se le atribuye a esta topología en malla.



que los nodos puedan encontrarse entre sí. El plano de control nunca ve el tráfico de datos, por lo tanto no sabe si se está transmitiendo un video, una base de datos o un comando SSH. Solo actúa como la "agenda telefónica" inteligente de la tailnet y entre sus funciones principales se encuentran la Autenticación de Identidad, el intercambio de claves criptográficas y el Descubrimiento de Rutas.

Por otro lado, el Plano de Datos es el encargado del procesamiento y transporte real de los paquetes de información. Entre sus funciones principales se destacan el cifrado, descifrado y transporte de los paquetes de información a través de la conexión punto a punto previamente establecida por el Plano de Coordinación.



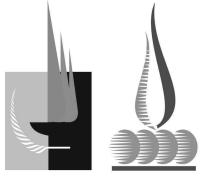
Metodología de Investigación

La metodología a desarrollar para llevar a cabo el trabajo es mixta, ya que el objetivo es demostrar que depender de empresas de terceros para gestionar nuestra información es perder la soberanía sobre la misma. La intención de este trabajo es visibilizar esto y, para ello, requiere comprender el fenómeno en sí a través de experiencias o perspectivas diferentes desde el punto de vista de los usuarios finales de servicios como lo es el almacenamiento en nubes de terceros. Es por esto que la investigación se volcará sobre lo cualitativo en un principio, pero también es de interés saber si los usuarios finales estarían dispuestos a implementar sus propias nubes domésticas, sabiendo que esto requiere de cierto nivel de manejo y control sobre las tecnologías a utilizar.

A raíz de esto, esta investigación será enmarcada dentro de un enfoque metodológico mixto, combinando estrategias cualitativas y cuantitativas para obtener una visión integral sobre el diseño e implementación de una infraestructura de nube privada, utilizando contenedores y máquinas virtuales. Esta combinación metodológica permite no solo comprender el contexto técnico y las decisiones de diseño, sino también evaluar objetivamente el rendimiento de las tecnologías involucradas.

Los métodos cualitativos permiten explorar en profundidad las características, procesos y decisiones técnicas vinculadas a la infraestructura en estudio. En este sentido, se pretenden utilizar las siguientes herramientas:

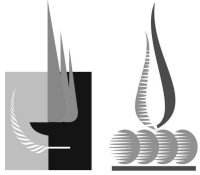
- *Análisis documental*: Se analizarán fuentes secundarias, incluyendo documentación técnica oficial (manuales de Docker, Proxmox, etc.), artículos académicos, *blogs* especializados y reportes de experiencias similares. Este análisis permitirá fundamentar las decisiones de diseño técnico y comprender el *estado del arte*.
- *Observación*: A lo largo del proceso de implementación, se registrarán detalladamente las observaciones realizadas, en relación con el funcionamiento del sistema, los problemas surgidos, las decisiones adoptadas y los resultados obtenidos. Esta observación se convertirá en una fuente reflexiva clave para la evaluación cualitativa del proyecto.



- *Estudio de caso*: El proyecto se documentará como un estudio de caso, permitiendo analizar el diseño, desarrollo, configuración y puesta en marcha de la infraestructura. Este método será útil para generar conocimiento aplicable en contextos similares.

En cuanto al enfoque cuantitativo, se orienta a recolectar y analizar datos numéricos que permitan evaluar objetivamente el comportamiento técnico de la infraestructura implementada. Los métodos a considerar son:

- *Pruebas de rendimiento (benchmarking)*: Se aplicarán herramientas de análisis de desempeño (como htop, sysbench, iperf, entre otras) para medir y comparar el uso de recursos (CPU, RAM, red, disco) en distintos entornos: máquinas virtuales y contenedores. Estos datos permitirán determinar la eficiencia relativa de cada tecnología.
- *Recolección de métricas del sistema*: Durante las pruebas de funcionamiento, se utilizarán herramientas de monitoreo para capturar métricas objetivas relacionadas con la estabilidad, tiempos de respuesta y consumo de recursos de la infraestructura.
- *Análisis estadístico y tablas comparativas*: Los datos obtenidos serán organizados en tablas y gráficos, permitiendo contrastar numéricamente el comportamiento de los distintos componentes del sistema bajo diversas condiciones de operación.



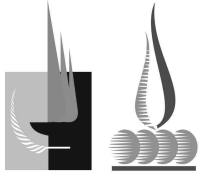
Resultados esperados

A partir de los objetivos planteados en el presente proyecto, se espera obtener los siguientes resultados:

1. La elaboración de una guía técnica comparativa entre máquinas virtuales y contenedores, que permita establecer criterios prácticos para decidir cuál de estas tecnologías utilizar en diferentes escenarios de implementación dentro de un entorno de servidores hogareños.
2. El desarrollo de un protocolo básico de seguridad informática, aplicable a infraestructuras de nube privada. Dicho protocolo incluirá reglas para el control de acceso, autenticación de usuarios, configuración de firewall y segmentación de servicios.
3. La implementación funcional de un servidor doméstico (*home lab*) que integre acceso remoto seguro y herramientas colaborativas basadas en software libre, como por ejemplo Nextcloud. Esta implementación estará orientada a su evaluación en entornos reales o simulados.
4. Experiencias de usuarios que permitan evaluar la facilidad de uso, la percepción de seguridad y la utilidad práctica de las soluciones implementadas, independientemente del nivel de conocimiento técnico que los usuarios posean.

Estos resultados se encuentran estrechamente vinculados con la metodología de investigación mixta adoptada para este trabajo, la cual combina enfoques cuantitativos y cualitativos. En primer lugar, el enfoque cuantitativo permitirá realizar mediciones objetivas sobre el rendimiento de las tecnologías empleadas (por ejemplo, uso de recursos, tiempos de respuesta, disponibilidad), así como aplicar pruebas de seguridad en la infraestructura diseñada. En segundo lugar, el enfoque cualitativo permitirá recoger y analizar testimonios, opiniones y valoraciones de los usuarios, brindando una comprensión más profunda de los factores subjetivos que intervienen en el uso de servidores domésticos con tecnologías *open source*.

La integración de ambos enfoques metodológicos ofrece una visión más completa del

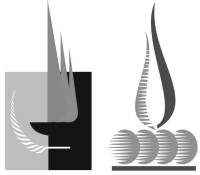


FACULTAD DE CIENCIAS
EXACTAS Y NATURALES

Universidad Nacional de La Pampa

fenómeno estudiado, ya que no solo se consideran los aspectos técnicos y medibles, sino también las percepciones, dificultades y aprendizajes de quienes interactúan con estas soluciones tecnológicas.

En este sentido, se espera que los resultados obtenidos sean significativos para la temática abordada, en tanto contribuyan a fomentar la apropiación tecnológica en contextos domésticos, promover la autonomía digital mediante el uso de software libre y fortalecer la capacidad de los usuarios para implementar infraestructuras de red seguras y funcionales sin depender de servicios externos.

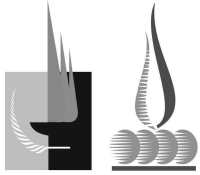


Resultados Obtenidos

Los resultados obtenidos son expuestos en la documentación del proceso de despliegue de Nextcloud junto con la configuración de su acceso remoto a través de la aplicación *Tailscale* (Ver anexo 1 al presente trabajo).

Los puntos que se consiguieron resolver fueron la definición y aplicación de tecnologías de virtualización, junto con la creación de una documentación que aborda el despliegue de un servidor privado para transferencia de archivos, al cual se le implementó acceso remoto haciendo uso de Tailscale.

Por otro lado, lo que no se logró fue la construcción de una documentación sólida sobre el desarrollo de un protocolo básico de seguridad informática, puesto que todo lo referido a seguridad en la comunicación entre dispositivos es delegado al propio servicio de Tailscale a través de sus Planos de Control (para la coordinación) y Planos de Datos (para el tráfico).



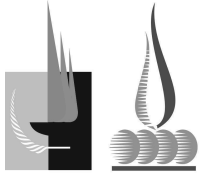
Conclusiones

El desarrollo de este trabajo y la construcción de la documentación anexada al mismo, permitieron validar la diferenciación que existe entre máquinas virtuales y contenedores (enfocado en contenedores de tipo LXC) destacando la eficiencia de estos últimos para servicios como lo es Tailscale. Y aunque para fines prácticos se utilizó un CT (contenedor) para desplegar Nextcloud, debe de quedar constancia que lo recomendado es hacer uso de máquinas virtuales de Proxmox (o directamente sobre un dispositivo físico aislado de otros servicios) para aprovechar la robustez y aislamiento de las mismas, garantizando así una capa extra de seguridad.

Por otro lado, la implementación de Tailscale demuestra ser una solución más robusta y segura que el reenvío de puertos (*port forwarding*) convencional. Al no requerir la apertura de puertos en el *router* hacia la Internet pública, se elimina una de las principales superficies de ataque para actores malintencionados, cumpliendo así con el objetivo de establecer una seguridad básica en la infraestructura. La creación de una red privada distribuida y cifrada (*tailnet*) garantiza que el tráfico entre los dispositivos y Nextcloud viaje de forma segura, incluso sobre redes públicas. Esto refuerza el objetivo de alcanzar la *soberanía digital*, ya que el usuario mantiene el control total del acceso a su información sin depender de la infraestructura de seguridad de terceros.

En cuanto al uso de una PC de escritorio convencional, prueba que no es necesaria una inversión en hardware de nivel empresarial o servicios de computación en la nube costosos para obtener un rendimiento funcional. A pesar de tener años de antigüedad, el hardware doméstico demostró ser capaz de gestionar servicios como Nextcloud y Tailscale simultáneamente bajo cargas de trabajo típicas de un entorno personal o de pequeña empresa.

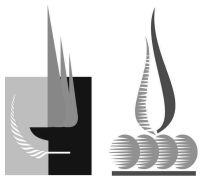
Finalmente, la elección de herramientas como Proxmox VE, Ubuntu Server, Nextcloud y Tailscale *elimina la dependencia de licencias propietarias y ecosistemas cerrados*. Al desplegar Nextcloud, el usuario recupera el control sobre su información, superando las limitaciones de almacenamiento (como los 15GB gratuitos de Google) y las



FACULTAD DE CIENCIAS
EXACTAS Y NATURALES

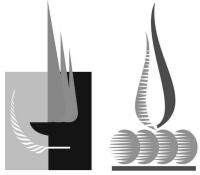
Universidad Nacional de La Pampa

preocupaciones de privacidad asociadas a las plataformas de terceros. En este sentido, el software de código abierto permite, además, configurar un entorno a medida donde cada servicio (como el nodo de Tailscale en un contenedor LXC) utiliza solo los recursos estrictamente necesarios (ej. 512MB de RAM), algo difícil de replicar en servicios de nube comercial sin incurrir en costos crecientes, puesto que muchas opciones de Computación en la Nube (*cloud computing*) tienden a incrementar sus tarifas de uso en base a la cantidad de recursos de hardware solicitados.



Recursos bibliográficos consultados

- Serrano Perelló, J. (2016). *Análisis de soluciones cloud para almacenamiento de archivos y trabajo colaborativo*. Universidad Politécnica de Valencia.
- Santamaría, F., Ballesteros, J. y González, J. (2015). *Plataforma cloud computing como infraestructura tecnológica para laboratorios virtuales, remotos y adaptativos*. Revista Científica.
- Docker (2025). *Docker Documentation*. Recuperado el 8 de junio de 2025 de <https://docs.docker.com/>.
- Oracle (2025). *VirtualBox documentation*. Recuperado el 2 de junio de 2025 de <https://www.virtualbox.org/manual/>.
- Amazon Web Services (2024). *¿Qué es un hipervisor?*. Recuperado el 4 de junio de 2025 de <https://aws.amazon.com/es/what-is/hypervisor/>.
- Red Hat (2019). *What is Open Source?*. Recuperado el 4 de junio de 2025 de <https://www.redhat.com/en/topics/open-source/what-is-open-source>.
- Nextcloud (2025). *Nextcloud Admin documentation*. Recuperado el 8 de junio de 2025 de https://docs.nextcloud.com/server/latest/admin_manual/.
- Proxmox (2025). *Proxmox VE documentation*. Recuperado el 9 de junio de 2025 de <https://pve.proxmox.com/pve-docs/>.
- Canonical (2025). *Ubuntu Server documentation*. Recuperado el 9 de junio de 2025 de <https://documentation.ubuntu.com/server/>.
- Google. (2025). *Google Cloud documentation*. Recuperado el 4 de junio de 2025 de <https://cloud.google.com/discover/what-is-a-private-cloud?>.
- Ausmun Cloud (2025). *Virtualización cloud: qué es, cómo funciona y por qué deberías usarla*. Recuperado el 4 de junio de 2025 de <https://ausum.cloud/vitualizacion-cloud-que-es-y-como-funciona/>.
- Red Hat (2024). *¿Qué es la virtualización?*. Recuperado el 4 de junio de 2025 de <https://www.redhat.com/es/topics/virtualization/what-is-virtualization>.
-



IBM (s.f.) *¿Qué es la virtualización?*. Recuperado el 5 de junio de 2025 de <https://www.ibm.com/mx-es/topics/virtualization>.

Jason Perlow (13 de junio de 2024). *LXC vs. Docker: Which One Should You Use?* [Blog]. Docker.

https://www-docker-com.translate.goog/blog/lxc-vs-docker/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc.

Avery Pennarun (20 de marzo de 2020). *How Tailscale works* [Blog]. Tailscale. <https://tailscale.com/blog/how-tailscale-works>.

Tailscale (2026). *Tailscale documentation*. Recuperado el 3 de mayo de 2026 de <https://tailscale.com/docs>.