

MANUAL DE

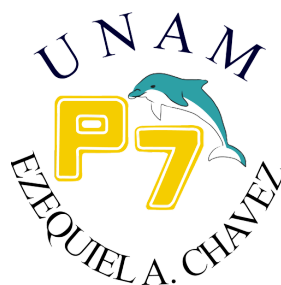


nextcloud

INSTALACIÓN Y FUNCIONAMIENTO

GALINDO REYES DANIEL ADRIAN

EDITOR



INTRODUCCIÓN

Nextcloud es una plataforma de almacenamiento en la nube de código abierto que permite a los usuarios almacenar archivos y datos en una nube privada, ya sea en un servidor local o accesible desde múltiples dispositivos a través de internet, ofrece una alternativa segura y flexible a los servicios comerciales de almacenamiento en la nube, proporcionando funcionalidades avanzadas de sincronización y colaboración en tiempo real.

Algo que cabe resaltar de Nextcloud es la capacidad de compartir archivos y carpetas con otros usuarios, realizar copias de seguridad de los datos, sincronizar calendarios y contactos, y utilizar aplicaciones adicionales para mejorar la productividad, como herramientas de chat y edición de documentos en línea. Además, al ser de código abierto, permite a los usuarios adaptar la plataforma según sus necesidades, integrándose de manera efectiva en infraestructuras ya existentes o en soluciones personalizadas para el manejo de datos.

Dentro de este manual se tiene como objetivo guiar en el proceso de instalación de Nextcloud en una distribución de Ubuntu utilizando Apache como servidor web. A través de esta guía, se pretende no solo realizar una instalación básica de Nextcloud, sino también familiarizarnos con los apartados y características principales que ofrece esta herramienta de almacenamiento en la nube.

La instalación en Ubuntu permite aprovechar un entorno de servidor robusto y ampliamente utilizado, mientras que Apache, como servidor web, asegura una configuración estable y compatible con la mayoría de los módulos y funcionalidades de Nextcloud. Además, exploraremos configuraciones adicionales y revisaremos algunos de los componentes clave de Nextcloud, permitiendo al usuario aprovechar al máximo esta plataforma de almacenamiento.

ÍNDICE

1

Requisitos previos para Nextcloud

2

Descarga e Instalación de PHP

3

Instalación y Configuración de MariaDB

4

Configuración de Apache

5

Instalación y descarga de Nextcloud

6

Sobre seguridad y rendimiento

7

Manual de usos Nextcloud

- **Requisitos
previos
para
Nextcloud**

RREQUISITOS PREVIOS

Para instalar Nextcloud, asegúrate de cumplir con los siguientes requisitos mínimos:

- **CPU:** Procesador de al menos 2 núcleos.
- **RAM:** Mínimo 1 GB, recomendados 2 GB o más para múltiples usuarios.
- **Espacio en Disco:** Mínimo 8 GB, con espacio adicional según el volumen de archivos de usuario.
- **Sistema Operativo:** Distribución de Linux (se recomienda Ubuntu 20.04 LTS o superior)
- **Apache instalado en:** el sistema operativo Ubuntu o servidor web instalado con posterioridad, así como conocimientos mínimos sobre el mismo.
- **Conexión a Internet:** Necesaria para la descarga de paquetes y actualizaciones.
- **Conocimiento de:** la IP pública del servidor o equipo, o en su defecto, un dominio o subdominio apuntando al servidor. Alternativamente, Nextcloud puede configurarse para uso local, pero en este caso no permitirá tráfico desde internet.

NOTA:

La configuración e instalación detallada de Ubuntu la podemos encontrar en el *Manual de Ubuntu: Instalación y funcionamiento (Galindo Reyes, 2024)*.

ACTUALIZACIÓN DE PAQUETES DEL SISTEMA

Para comenzar con la instalación de Nextcloud, verificaremos que las dependencias y paquetes dentro del sistema estén actualizados. Esto lo realizaremos de la siguiente forma en Ubuntu.

1. Abrimos la terminal y escribiremos los comandos para actualizar los paquetes del sistema. Como primer comando, utilizaremos **update**. Este comando actualiza la lista de paquetes disponibles en los repositorios configurados.

2. A continuación, ejecutaremos el segundo comando **upgrade**, el cual instalará las versiones más recientes de los paquetes ya instalados en el sistema y como extra se recomienda instalar **unzip**. (Ver figura 1.2.)

```
sudo apt update  
sudo apt upgrade  
sudo apt install unzip
```

3. Podemos colocar ambos comandos en la misma línea de la terminal y agregar la bandera **-y** para aprobar los cambios automáticamente en caso de ser necesarios. Al utilizar la palabra *sudo*, será necesario ingresar la contraseña del sistema para confirmar la operación. (Ver figura 1.1)

```
sudo apt update && sudo apt upgrade -y
```

```
ubuntu@ip-172-31-82-65:~$ sudo apt update && sudo apt upgrade -y
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Figura 1.1. Comandos update y upgrade:

```
ubuntu@ip-172-31-82-65:~$ sudo apt install unzip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
unzip is already the newest version (6.0-28ubuntu4.1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Figura 1.2. Instalación de Unzip

- **Descarga e
Instalación
de PHP**

DESCARGA E INSTALACIÓN DE PHP:

PHP es esencial y necesario para la instalación de Nextcloud, ya que permite ejecutar el código del sistema, procesar las solicitudes de los usuarios y gestionar la conexión con la base de datos, facilitando así el acceso y manejo seguro de archivos y configuraciones.

Para instalarlo en nuestro sistema Ubuntu, abriremos una terminal e instalaremos las siguientes extensiones de PHP. Todas ellas tienen una funcionalidad, pero no todas son estrictamente necesarias, es decir, en casos particulares se podría omitir o ignorar algunas extensiones; sin embargo, para una instalación adecuada, se recomienda la instalación de todas las extensiones. A continuación, se explicará cada una de ellas:

php-cli: Permite ejecutar scripts PHP desde la línea de comandos, útil para tareas de mantenimiento de Nextcloud.

php-fpm: Un manejador de procesos para PHP que mejora el rendimiento y maneja mejor las solicitudes de usuarios en un servidor web como Apache.

php-json: Necesario para procesar datos en formato JSON, común en la comunicación de aplicaciones modernas.

php-intl: Ofrece soporte de internacionalización, necesario para que Nextcloud funcione correctamente en múltiples idiomas.

php-imagick: Extensión para manipular imágenes, necesaria para visualizar y redimensionar imágenes en Nextcloud.

php-pdo: Habilita el acceso a bases de datos a través de una interfaz unificada, indispensable

php-mysql: Extensión específica para conectar Nextcloud a bases de datos MySQL o MariaDB, que son las más utilizadas.

php-zip: Permite el manejo de archivos comprimidos, lo cual es útil para la descarga y subida de archivos comprimidos en Nextcloud.

php-gd: Librería de gráficos para el procesamiento de imágenes, utilizada para la generación de miniaturas y visualización de imágenes.

php-mbstring: Maneja cadenas de texto en múltiples caracteres, necesario para garantizar la compatibilidad de texto en diferentes idiomas

php-curl: Permite realizar solicitudes HTTP, usado por Nextcloud para conectarse a otros servicios web.

php-xml: Habilita el manejo de datos en formato XML, esencial para diversas funcionalidades de Nextcloud.

php-pear: Sistema de distribución de paquetes y clases en PHP, aunque opcional, puede ser útil para dependencias adicionales.

php-bcmath: Extensión matemática para operaciones de precisión arbitraria, que puede ser necesaria para cálculos específicos en Nextcloud.

Estas instalaciones se pueden realizar de forma separada, es decir modulo por modulo o en conjunto.

Instalación separada:

```
sudo apt install -y php-cli  
sudo apt install -y php-fpm  
sudo apt install -y php-json  
sudo apt install -y php-intl  
sudo apt install -y php-imagick  
sudo apt install -y php-pdo  
sudo apt install -y php-mysql  
sudo apt install -y php-zip  
sudo apt install -y php-gd  
sudo apt install -y php-mbstring  
sudo apt install -y php-curl  
sudo apt install -y php-xml  
sudo apt install -y php-pear  
sudo apt install -y php-bcmath
```

Instalación en conjunto:

```
sudo apt install -y php-cli php-fpm php-json php-intl php-imagick php-  
pdo php-mysql php-zip php-gd php-mbstring php-curl php-xml php-pear  
php-bcmath
```

NOTA:

La configuración e instalacion detallada de PHP la podemos encontrar en el *Manual de Apache: Instalación y fortalecimiento (Galindo Reyes, 2024, p. 7)*. Para más información, consulte el apartado "Instalación y descarga de apache".

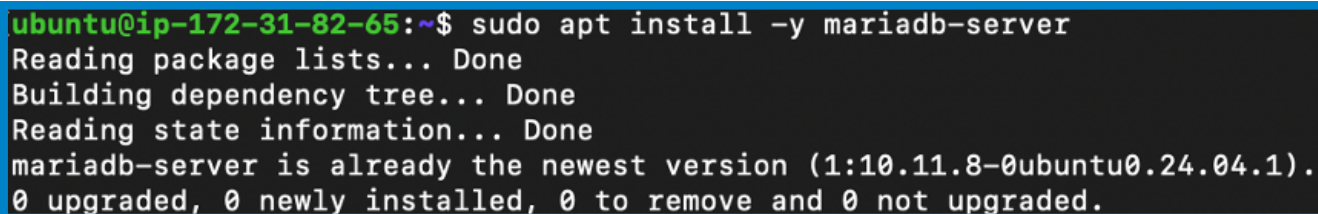
- **Instalación y Configuración de MariaDB**

INSTALACIÓN Y CONFIGURACIÓN DE MARIADB

Una vez instalado PHP, continuaremos con la instalación de MariaDB. Nextcloud requiere una base de datos para almacenar información, como datos de usuarios, configuraciones, permisos y detalles sobre los archivos y documentos almacenados. Esta base de datos permite a Nextcloud organizar y acceder a la información de manera eficiente. En este manual, realizaremos la instalación de MariaDB, aunque Nextcloud también es compatible con otras bases de datos como MySQL, PostgreSQL o SQLite.

La instalación de MariaDB es bastante sencilla; basta con ejecutar el siguiente comando en la terminal:

```
sudo apt install -y mariadb-server
```

A terminal window with a black background and green text. The prompt is 'ubuntu@ip-172-31-82-65:~\$'. The command 'sudo apt install -y mariadb-server' has been executed. The output shows the package lists being read, the dependency tree being built, and state information being read, all successfully. It then states that mariadb-server is already the newest version (1:10.11.8-0ubuntu0.24.04.1) and that 0 packages were upgraded, 0 newly installed, 0 to be removed, and 0 not upgraded.

```
ubuntu@ip-172-31-82-65:~$ sudo apt install -y mariadb-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
mariadb-server is already the newest version (1:10.11.8-0ubuntu0.24.04.1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Figura 1.3. Instalación de MariaDB

Una vez instalada la base de datos, es necesario configurar algunos aspectos de seguridad en MariaDB, ya que, por defecto, algunas configuraciones no son muy seguras y se recomienda modificarlas con el uso de una herramienta que la misma MariaDB nos proporciona.

Accederemos a la herramienta con el comando:

```
sudo mysql_secure_installation
```

Este comando iniciará una serie de preguntas que permitirán mejorar la seguridad de MariaDB, como establecer una contraseña para el usuario root, eliminar usuarios anónimos, desactivar el acceso remoto para el usuario root y eliminar la base de datos de prueba. Se recomienda responder "sí" a todas las opciones para fortalecer la seguridad de la instalación de MariaDB y colocar una contraseña fuerte para el usuario root, es necesario guardar y recordar estas claves de acceso para futuras modificaciones o cambios.

```
Switch to unix_socket authentication [Y/n] y
Enabled successfully!
Reloading privilege tables..
... Success!
```

Figura 1.4. Habilitar la autenticación por unix_socket

```
Change the root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!
```

Figura 1.5. Cambiar contraseña de root

```
By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!
```

Figura 1.6. Remover usuarios anónimos

```
Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
... Success!
```

Figura 1.7. Conexiones del usuario root

```
By default, MariaDB comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!
```

Figura 1.8. Remover Bases de Datos de Prueba

```
Reloading the privilege tables will ensure that all changes made so far will take effect immediately.

Reload privilege tables now? [Y/n] y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB installation should now be secure.
```

Figura 1.9. Recargar las tablas de privilegios

Una vez actualizada la configuración de seguridad de la base de datos, será necesario crear un usuario específico para Nextcloud. Este usuario tendrá permisos limitados y estará destinado exclusivamente para gestionar la base de datos de Nextcloud. Para crear este usuario, accedemos a la base de datos con el siguiente comando:

```
sudo mysql -u root -p
```

```
ubuntu@ip-172-31-82-65:~$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 42
Server version: 10.11.8-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

Figura 1.10. Acceder a root en MariaDB

Este comando nos pedirá la contraseña que configuramos anteriormente en el apartado de seguridad de MariaDB. Una vez dentro de la consola de MariaDB, podremos proceder a crear la base de datos y el usuario específicos para Nextcloud.

Ahora, dentro de la sesión de MariaDB, crearemos una base de datos llamada nextcloud. Esto se hace con el siguiente comando:

```
CREATE DATABASE nextcloud;
```

```
MariaDB [(none)]> CREATE DATABASE nextcloud;
Query OK, 1 row affected (0.000 sec)
```

Figura 1.11. Creación de base de datos para Nextcloud

También será necesario crear un usuario con los permisos adecuados para acceder a esta base de datos. Nombramos a este usuario Nextcloud, y la contraseña puede ser cualquiera, pero es importante guardarla, ya que se necesitará más adelante. A este usuario le otorgaremos todos los permisos necesarios para acceder, modificar y eliminar información en la base de datos. Esto se realiza con los siguientes comandos:

```
CREATE USER 'nextcloud'@'localhost' IDENTIFIED BY '<Contraseña>';
GRANT ALL PRIVILEGES ON nextcloud.* TO 'nextcloud'@'localhost';
```

```
[MariaDB [(none)]]> CREATE USER 'nextcloud'@'localhost' IDENTIFIED BY '12345';  
Query OK, 0 rows affected (0.001 sec)  
  
[MariaDB [(none)]]> GRANT ALL PRIVILEGES ON nextcloud.* TO 'nextcloud'@'localhost';  
Query OK, 0 rows affected (0.002 sec)
```

Figura 1.12. Creación de usuario para Nextcloud con contraseña < 12345 >

Para aplicar los cambios se deberá colocar el siguiente comando:

```
FLUSH PRIVILEGES;
```

```
[MariaDB [(none)]]> FLUSH PRIVILEGES;  
Query OK, 0 rows affected (0.000 sec)
```

Figura 1.13. Recargar las tablas de privilegios

Con estos comandos, el usuario Nextcloud tendrá acceso completo a la base de datos Nextcloud, permitiéndole gestionar los datos que Nextcloud almacene.

Para salir de la base de datos colocaremos exit.

```
MariaDB [(none)]> exit  
Bye
```

Figura 1.14. Salir de MariaDB

- **Configuración de Apache**

CONFIGURACIÓN DE APACHE

Una vez instalada y creada la base de datos, procederemos a configurar algunas cosas dentro del proveedor de servicios web. En este manual se asumirá que se encuentra instalado Apache en el servidor. También será necesario un módulo específico de Apache para que PHP pueda utilizarlo de forma correcta, esto se realizará con el comando:

```
sudo apt install apache2 libapache2-mod-php -y
```

```
ubuntu@ip-172-31-82-65:~$ sudo apt install apache2 libapache2-mod-php -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.58-1ubuntu8.4).
libapache2-mod-php is already the newest version (2:8.3+93ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Figura 1.15. Instalar Apache2 con su modulo para PHP

Apache permite la creación de servidores virtuales o virtual hosts; en el caso de Nextcloud, nos permitirán almacenar información en otra carpeta que no sea directamente /var/www/html, que es la ruta por defecto que Apache toma para almacenar sitios web.

En este manual se tomará como referencia la creación de un virtual host dedicado a Nextcloud. Como primer paso, y para facilitar el proceso, se recomienda copiar el archivo de configuración de HTML original, ubicado en la carpeta /etc/apache2/sites-available y que, por lo general, lleva el nombre de 000-default.conf. Lo copiaremos, pegaremos y cambiaremos el nombre de esta copia a nextcloud.conf. Esto se puede realizar con el comando:

```
sudo cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/nextcloud.conf
```

También será necesario modificar algunas cosas dentro de este archivo, así como algunos privilegios para que Nextcloud y Apache lo puedan utilizar. Comenzaremos por cambiar la ruta de la carpeta en el archivo nextcloud.conf, como la ubicación de la carpeta donde estarán todos los archivos de Nextcloud y cambiar los nombres de los logs y errores que Apache genere. Abrimos el archivo con el comando :

```
sudo nano /etc/apache2/sites-available/nextcloud.conf
```

```

<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>

```

Figura 1.16. Archivo *nextcloud.conf* copiado de *000-default.conf*

Este comando nos abrirá una configuración básica a la que tendremos que agregar las líneas marcadas en el siguiente archivo:

```

<VirtualHost *:80>

# Configuración básica del servidor
ServerAdmin webmaster@localhost
ServerName <Ip publica o dominio>
DocumentRoot /var/www/nextcloud

# Logs
ErrorLog ${APACHE_LOG_DIR}/nextcloud_error.log
CustomLog ${APACHE_LOG_DIR}/nextcloud_access.log combined

# Otras configuraciones opcionales
<Directory /var/www/nextcloud>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
    SetEnv HOME /var/www/nextcloud
    SetEnv HTTP_HOME /var/www/nextcloud
    # Desactivar WebDAV para evitar conflictos con Nextcloud
    <IfModule mod_dav.c>
        Dav off
    </IfModule>
</Directory>
</VirtualHost>

```

```

<VirtualHost *:80>
# Configuración básica del servidor
ServerAdmin webmaster@localhost
ServerName <Ip publica o dominio>
DocumentRoot /var/www/nextcloud

# Logs
ErrorLog ${APACHE_LOG_DIR}/nextcloud_error.log
CustomLog ${APACHE_LOG_DIR}/nextcloud_access.log combined

# Otras configuraciones opcionales
<Directory /var/www/nextcloud>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
    SetEnv HOME /var/www/nextcloud
    SetEnv HTTP_HOME /var/www/nextcloud
# Desactivar WebDAV para evitar conflictos con Nextcloud
    <IfModule mod_dav.c>
        Dav off
    </IfModule>
</Directory>
</VirtualHost>

```

Figura 1.17. Archivo nextcloud.conf modificado

En este caso, también se desactiva el uso de DAV, dado que Nextcloud ya incluye una implementación de WebDAV optimizada para su sistema. Mantener el módulo DAV de Apache activo podría causar conflictos, ya que ambas implementaciones podrían interferir entre sí.

El nombre del servidor (ServerName) debe configurarse con la dirección IP pública o un dominio que apunte a dicha IP. En este caso, se asume que estas direcciones son conocidas o que se configurará en un entorno local. Si el servidor aloja varios servicios, será necesario crear subdominios y especificar estos subdominios en ServerName, salimos del editor de texto pulsando **Ctrl + O** y **Ctrl + X**.

Para completar la configuración de Apache, deshabilitaremos la página predeterminada de Apache y activaremos varios módulos, como los de reescritura de URLs, manejo de rutas no especificadas, interpretación de archivos y formatos, gestión de variables de entorno y adición de encabezados HTTP, y por ultimo reiniciar el servicio e apache para cargar los cambios realizados esto con los comandos:

```

sudo a2dissite 000-default.conf
sudo a2enmod rewrite dir mime env headers
sudo systemctl restart apache2

```

- **Instalación y
descarga de
Nextcloud**

INSTALACIÓN Y DESCARGA DE NEXTCLOUD

Ahora que tenemos todo el entorno correctamente configurado, es hora de descargar los archivos de Nextcloud. Esto lo realizaremos mediante un enlace que nos proporciona la página oficial de Nextcloud. Lo primero que debemos hacer es dirigirnos a la carpeta /var/www con el siguiente comando:

```
cd /var/www
```

```
ubuntu@ip-172-31-82-65:~$ cd /var/www
ubuntu@ip-172-31-82-65:/var/www$
```

Figura 1.18. Cambiando directoria a /var/www

Una vez dentro, ejecutaremos el siguiente comando para descargar los archivos de Nextcloud y los descomprimiremos con la función unzip, instalada anteriormente:

```
sudo wget https://download.nextcloud.com/server/releases/latest.zip
sudo unzip latest.zip
```

```
ubuntu@ip-172-31-82-65:/var/www$ sudo wget https://download.nextcloud.com/server/releases/latest.zip
--2024-11-08 15:03:01-- https://download.nextcloud.com/server/releases/latest.zip
resolving download.nextcloud.com (download.nextcloud.com)... 5.9.202.145, 2a01:4f8:210:21c8::145
connecting to download.nextcloud.com (download.nextcloud.com)[5.9.202.145]:443... connected.
HTTP request sent, awaiting response... 200 OK
length: 22411416 (214M) [application/zip]
saving to: 'latest.zip'

latest.zip
100%[=====] 213.73M 16.6MB/s in 87s
2024-11-08 15:04:28 (2.47 MB/s) - 'latest.zip' saved [22411416/22411416]
```

Figura 1.19: Descargando archivos de NextCloud

```
ubuntu@ip-172-31-82-65:/var/www$ sudo unzip latest.zip
```

Figura 1.20: Descomprimiendo archivos de NextCloud

Luego, asignaremos los permisos adecuados al directorio de Nextcloud:

```
sudo chmod 755 /var/www/nextcloud
sudo chown -R www-data:www-data /var/www/nextcloud
```

```
ubuntu@ip-172-31-82-65:/var/www$ sudo chmod 755 /var/www/nextcloud
ubuntu@ip-172-31-82-65:/var/www$ sudo chown -R www-data:www-data /var/www/nextcloud
```

Figura 1.21 Conceder permisos

También eliminaremos el archivo latest.zip dado que ya no será de más utilidad:

```
sudo rm latest.zip
```

```
ubuntu@ip-172-31-82-65:/var/www$ sudo rm latest.zip
```

Figura 1.22. Eliminar latest.zip

A continuación, activaremos el servidor virtual de Nextcloud y reiniciaremos Apache con los siguientes comandos:

```
sudo a2ensite nextcloud.conf
sudo systemctl restart apache2
```

```
ubuntu@ip-172-31-82-65:/var/www$ sudo a2ensite nextcloud.conf
Enabling site nextcloud.
To activate the new configuration, you need to run:
  systemctl reload apache2
ubuntu@ip-172-31-82-65:/var/www$ sudo systemctl restart apache2
ubuntu@ip-172-31-82-65:/var/www$
```

Figura 1.23. Activar servidor virtual de Nextcloud y reinicio de apache

Una vez realizada esta instalación, podremos acceder a nuestra instancia de Nextcloud usando la dirección IP asignada al servidor virtual. Es importante recalcar que, si el tráfico proviene de internet, será necesario abrir los puertos 80 y 443 en UFW (cortafuegos de Ubuntu):

```
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
```

Después de configurar los puertos y descargar los paquetes necesarios, procederemos con la configuración de Nextcloud.

CONFIGURACIÓN DE NEXTCLOUD

Al ingresar a la dirección configurada en nuestro servidor virtual, tendremos acceso a la creación de un usuario administrador y podremos seleccionar la ubicación donde se almacenarán los datos de nuestra nube privada. En esta primera pantalla, también será necesario ingresar las credenciales para la base de datos: nombre de la base de datos, usuario y contraseña. Estos deben coincidir con los valores configurados anteriormente en MariaDB. El nombre de la base de datos debe ser Nextcloud, al igual que el usuario (Nextcloud), y la contraseña debe coincidir con la especificada al crear el usuario Nextcloud, al pulsar instalar podrá tardar algunos momentos hasta mostrar o cambiar de pagina, esto es normal, espera hasta ver una página distinta, como la mostrada en la figura 1.26.

Iniciar sesión

UNAM

Contraseña

Almacenamiento y base de datos ▾

Carpeta de datos

/var/www/nextcloud/data

Configurar la base de datos

Solo MySQL/MariaDB está disponible. Instalar y activar módulos PHP adicionales para elegir otros formatos de base de datos.

Para más detalles revisar la documentación. ↗

Cuenta de la base de datos

nextcloud

Contraseña de la base de datos

12345

Nombre de la base de datos

nextcloud

Host de la base de datos

localhost

Por favor especifique el numero del puerto junto al nombre del host (p.e., localhost:5432).

Instalar

¿Necesita ayuda? Vea la documentación ↗

Nextcloud – un lugar seguro para todos tus datos

Figura 1.24. Creación de usuario administrador de Nextcloud

Nextcloud se instalará correctamente y mostrará algunas extensiones que pueden ser de utilidad, las cuales facilitan el uso de distintos servicios de Nextcloud. Sin embargo, por ahora omitiremos la instalación de estas aplicaciones pulsando el botón "Saltar" que se encuentra en la parte inferior de la página. De este modo, solo instalaremos las aplicaciones que realmente necesitemos en nuestro servicio y evitaremos ocupar espacio innecesario en el almacenamiento, también en la figura 1.27 se muestra un menú que cerraremos por el momento, pulsando en la cruz de la esquina superior derecha.

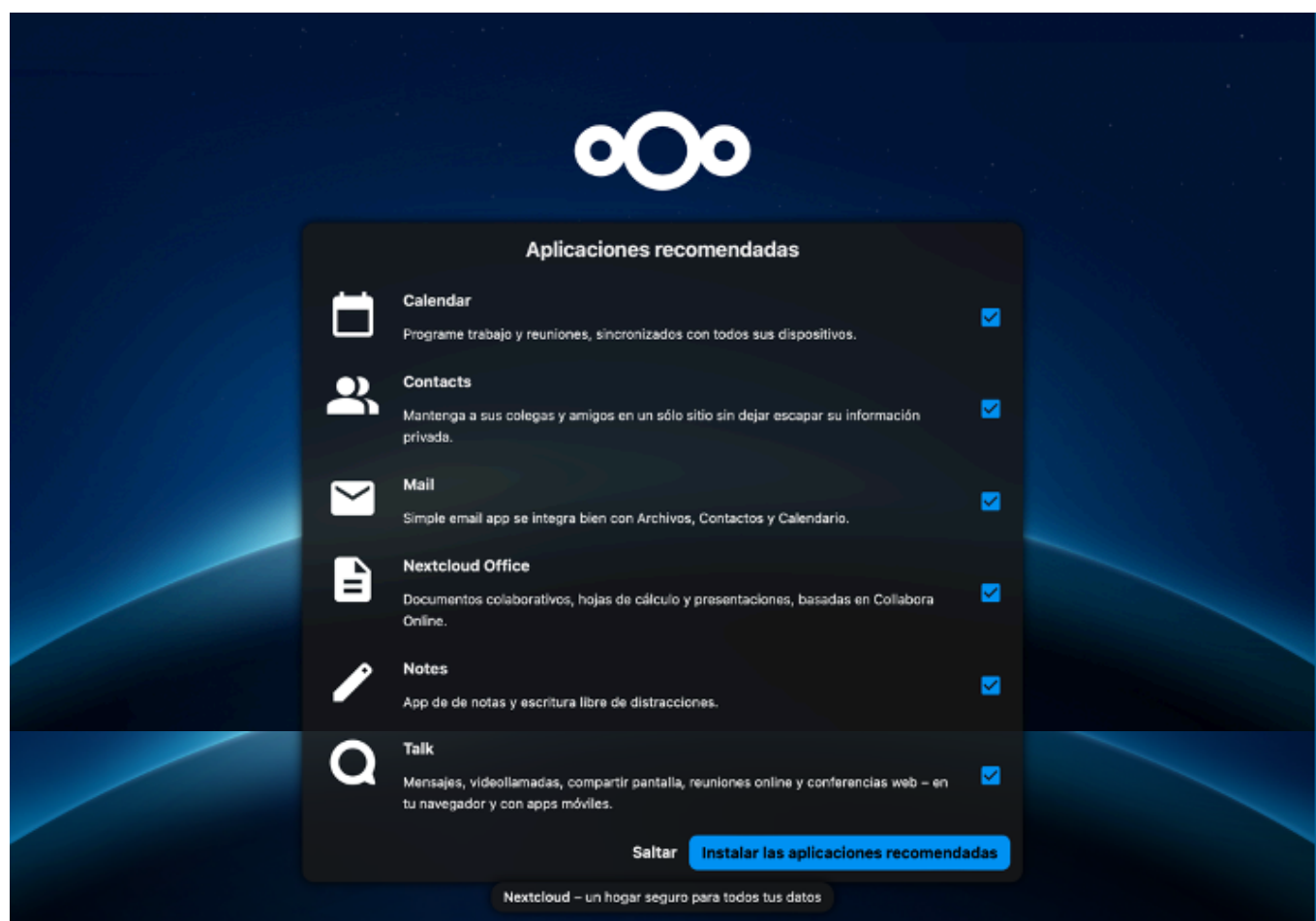


Figura 1.25. Aplicaciones recomendadas



Figura 1.26. Guía informativa de Nextcloud

Esto nos llevará a una página de inicio, que es la pantalla principal de Nextcloud. En ella podremos ver diferentes secciones, como un menú superior con dos apartados: uno donde se pueden ver algunas extensiones y otro donde se muestran notificaciones, filtros de búsqueda y la información del perfil, Nextcloud agrega algunos archivos de prueba, lo recomendable es borrarlos, esto lo aremos accediendo en la pestaña de archivos mostrada en la figura 1.27 en un rectángulo rojo.

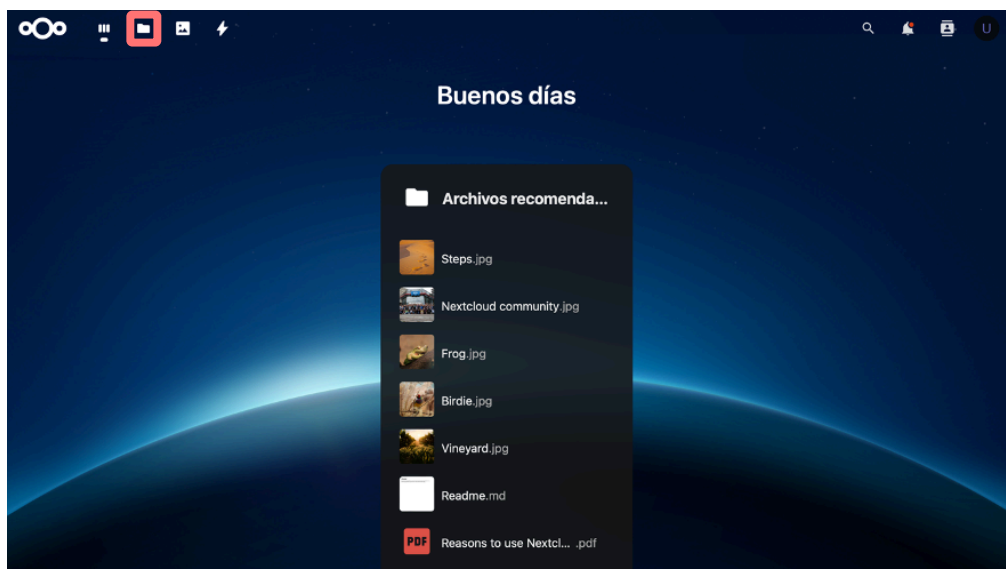


Figura 1.27. Inicio de Nextcloud

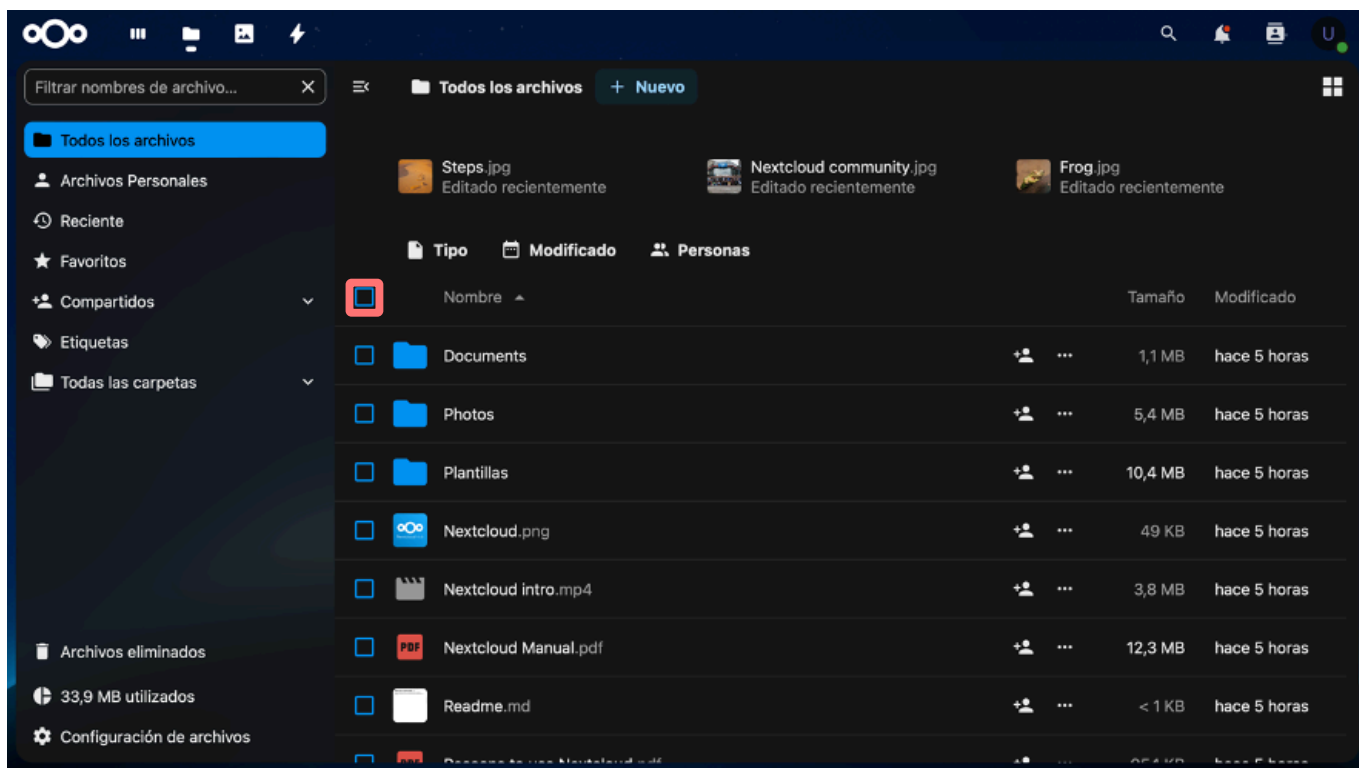


Figura 1.28. Pestaña de archivos

Dentro de la pestaña mostrada en la figura 1.28 marcaremos todos los archivos y pulsaremos eliminar, en este apartado tendremos un manual con funciones más extensas de Nextcloud, este se recomienda conservar o en su defecto revisar antes de eliminar, con esto terminaríamos la configuración e instalación limpia de Nextcloud sobre un servidor/equipo con Ubuntu.

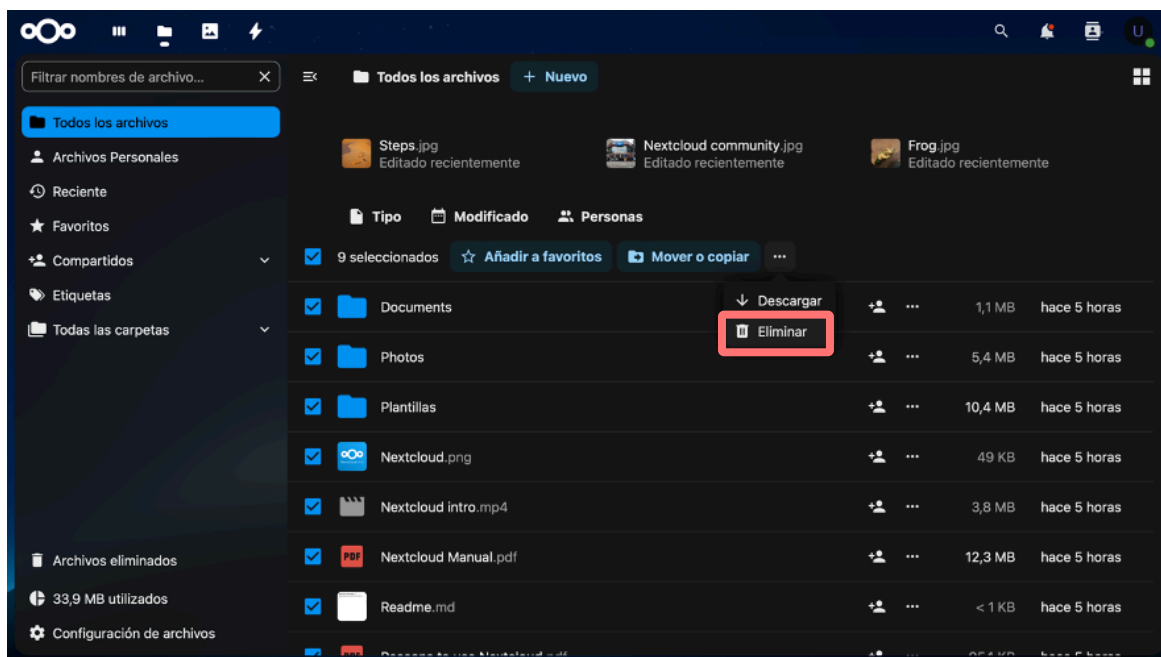


Figura 1.29. Eliminar archivos de prueba de Nextcloud

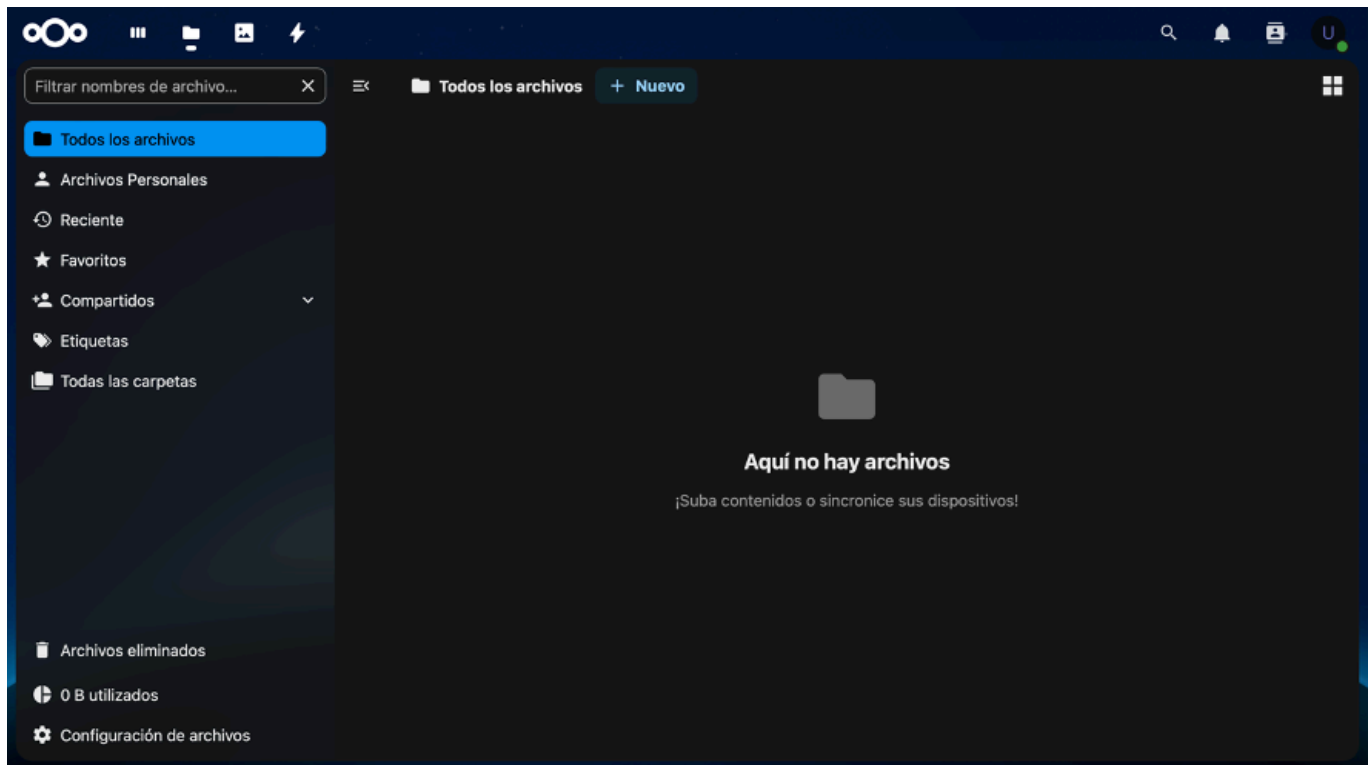


Figura 1.30. Instalación limpia de Nextcloud

- **Sobre
seguridad y
rendimiento**

SOBRE SEGURIDAD Y RENDIMIENTO

Esta instalación de Nextcloud, aunque funcional, no es completamente segura. Para lograr una configuración óptima, es necesario realizar algunas configuraciones adicionales que aseguren una comunicación adecuada entre el servidor y el cliente, además de ocultar ciertas características que no deberían ser accesibles.

Si accedemos a configuraciones de administración como se ve en la figura 1.31 podremos ver algunas alertas que deberemos corregir para mejorar la seguridad de Nextcloud.

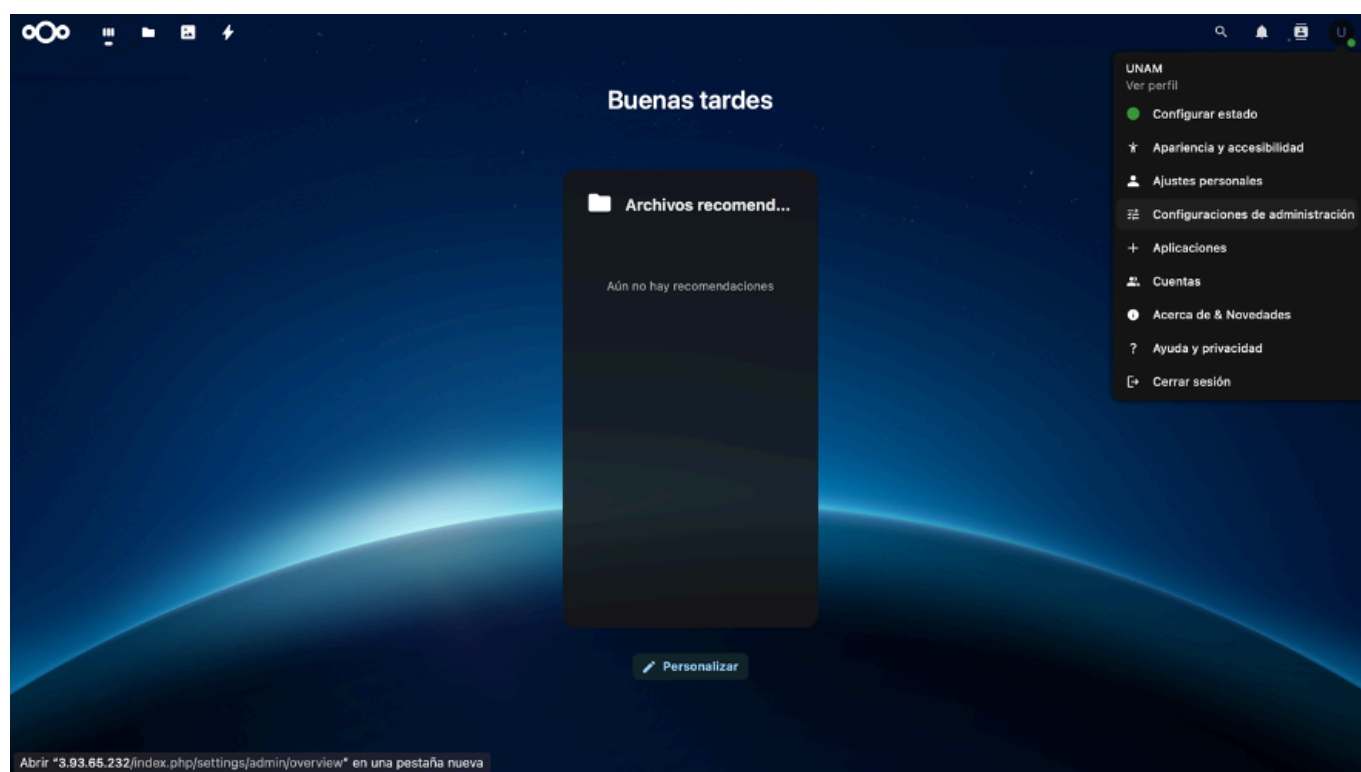


Figura 1.31. Configuraciones de administración

Comenzando con las alertas de color rojo, que son las más relevantes, es posible que estas varíen según la configuración específica del sistema. Aquí abordaremos las alertas más comunes que pueden aparecer y cómo resolverlas.

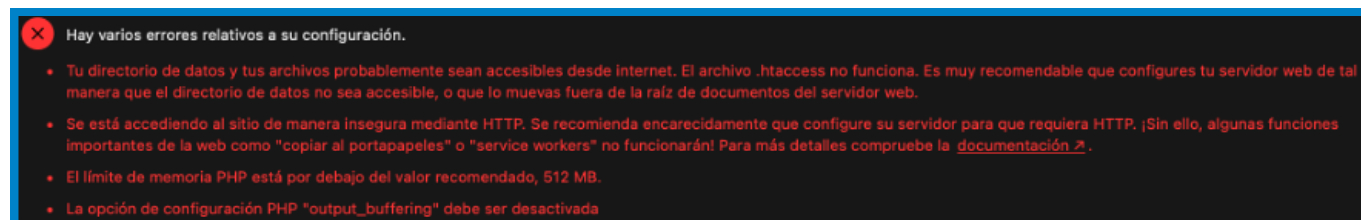


Figura 1.32. Errores relativos a la configuración

MOVER EL DIRECTORIO DE DATOS FUERA DE LA RAÍZ

Para mejorar la seguridad, es recomendable mover el directorio de datos de Nextcloud fuera del directorio raíz del servidor web (por ejemplo, fuera de /var/www/). Esto evita que los datos sean accesibles directamente desde internet.

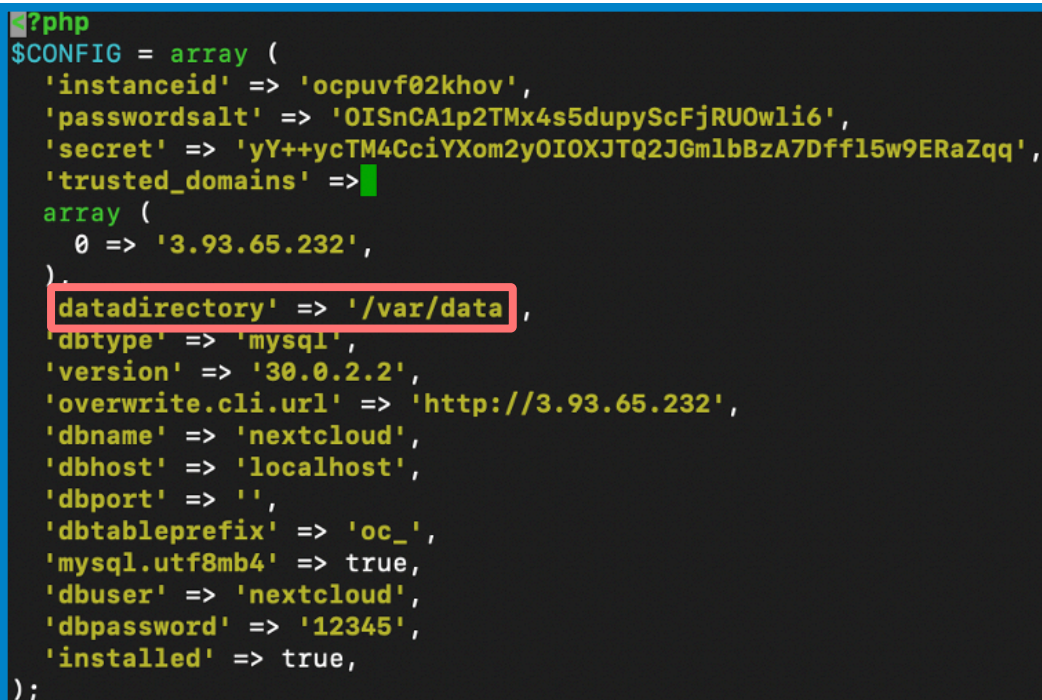
Para realizar esta operación utilizaremos el comando:

```
sudo mv /var/www/nextcloud/data <NuevaRuta>/data
```

Donde NuevaRuta puede ser cualquier ubicación dentro del servidor, incluyendo discos externos o volúmenes distintos al de la instalación del servidor Apache. Nextcloud guarda la ruta donde almacena sus datos, por lo que también será necesario modificar esta dirección en su archivo de configuración config.php entrados con el comando:

```
sudo nano /var/www/nextcloud/config/config.php
```

Cambia el valor de 'datadirectory' para que apunte a la nueva ubicación:



```
?php
$CONFIG = array (
    'instanceid' => 'ocpuvf02khov',
    'passwordsalt' => '0ISnCA1p2TMx4s5dupyScFjRU0wli6',
    'secret' => 'yY++ycTM4CciYXom2y0IOXJTQ2JGmlbBzA7Dff15w9ERaZqq',
    'trusted_domains' =>
    array (
        0 => '3.93.65.232',
    ),
    'datadirectory' => '/var/data',
    'dbtype' => 'mysql',
    'version' => '30.0.2.2',
    'overwrite.cli.url' => 'http://3.93.65.232',
    'dbname' => 'nextcloud',
    'dbhost' => 'localhost',
    'dbport' => '',
    'dbtableprefix' => 'oc_',
    'mysql.utf8mb4' => true,
    'dbuser' => 'nextcloud',
    'dbpassword' => '12345',
    'installed' => true,
);
```

Figura 1.33. Cambiando datadirectory a nueva ruta /var/data

Recordar que salimos del editor de texto pulsando **Ctrl + O** y **Ctrl + X**.

Al mover los datos a una nueva carpeta, es normal que Nextcloud no reconozca esta ubicación de inmediato, ya que los permisos necesarios sobre los archivos dentro de la carpeta no están configurados por lo que los asignaremos de la siguiente forma.

```
sudo chown -R www-data:www-data <NuevaRuta>/data  
sudo chmod 755 <NuevaRuta>/data
```

Dentro el directorio de datos debe existir un archivo llamado `.ncdata`, este especifica cual es la ruta del mismo archivo:

```
sudo nano <NuevaRuta>/data/.ncdata
```

y dentro el archivo `.ncdata` se debe colocar la línea `# Nextcloud data directory`, como se ve en la figura 1.34 guardar y salir del directorio con **Ctrl+O** y **Ctrl+X**.

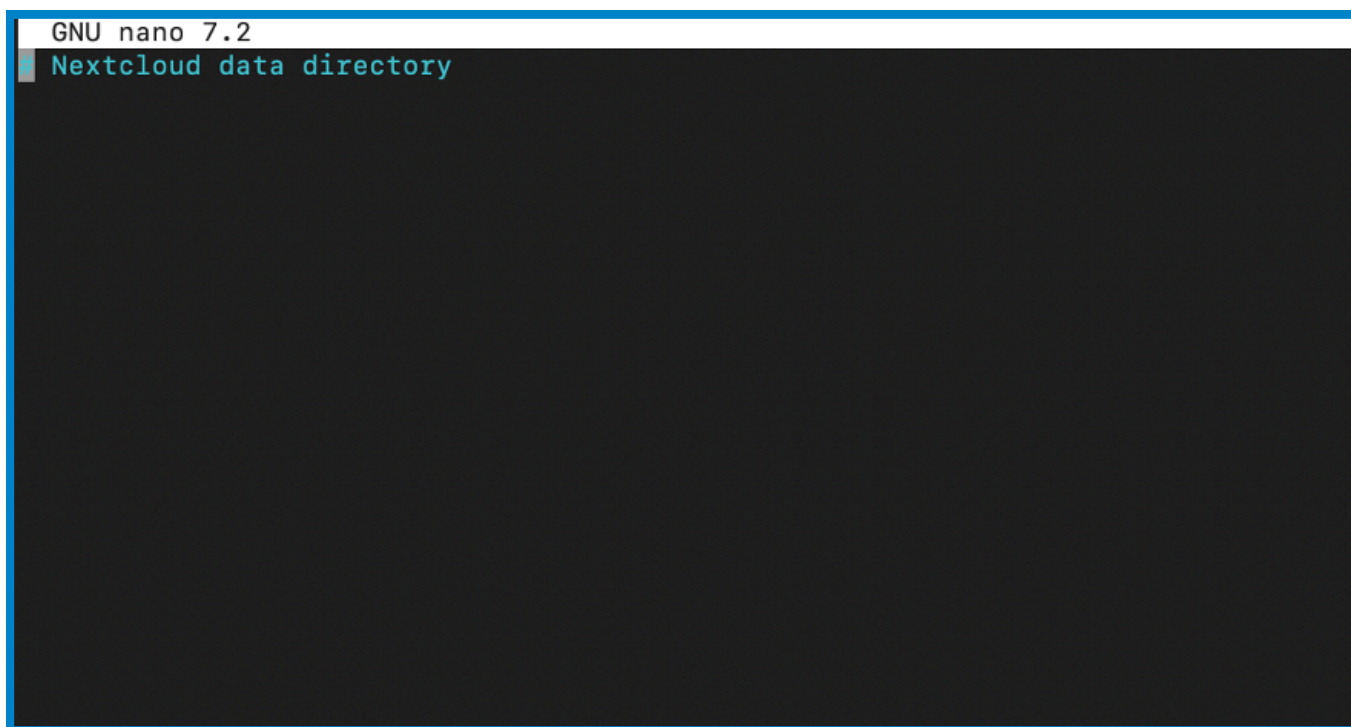


Figura 1.34. Archivo .ncdata

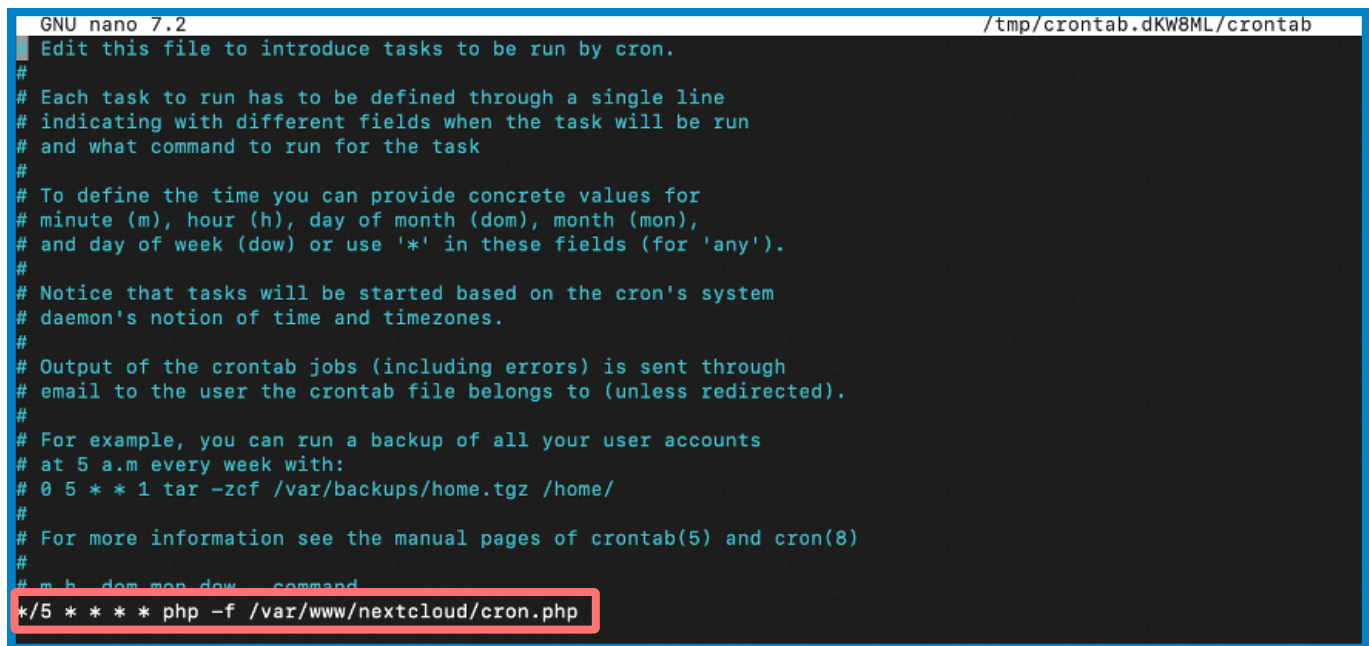
Asignamos los permisos para el usuario de apache:

```
sudo chown www-data:www-data <NuevaRuta>/data/.ncdata  
sudo chmod 755 <NuevaRuta>/data/.ncdata
```

También se recomienda modificar algún proceso de cron. Para hacerlo, accedemos al siguiente archivo con:

```
sudo -u www-data crontab -e
```

Luego, agregaremos la línea `* / 5 * * * php -f /var/www/nextcloud/cron.php` como se muestra en la imagen 1.35.



```
GNU nano 7.2 /tmp/crontab.dKW8ML/crontab
Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow command
*/5 * * * * php -f /var/www/nextcloud/cron.php
```

Figura 1.35. Configuración de cron

Y, por último, para resolver el error relacionado con los datos accesibles desde internet, reiniciaremos el servidor web y el proceso de cron con los siguientes comandos:

```
sudo systemctl restart cron
sudo systemctl restart apache2
```

Estos comandos aplicarán los cambios de configuración necesarios para asegurar el acceso adecuado a los datos y la correcta ejecución de las tareas de cron, podemos ver en la figura 1.36 como el error a desaparecido de Nextcloud.

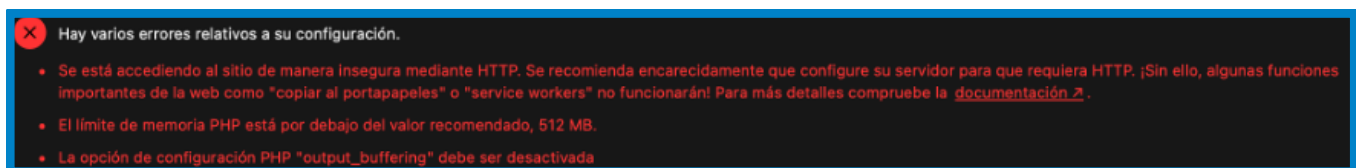


Figura 1.36. Error de directorio data corregido

HTTPS POR DEFECTO:

Actualmente, la información que viaja entre nuestra nube y los dispositivos conectados no está cifrada. Esto significa que, si alguien intercepta los datos mientras están en tránsito, podría leerlos sin restricciones, representando un riesgo grave de seguridad. Para solucionar este problema, es fundamental implementar un certificado SSL o TLS. Este tipo de certificado permite cifrar la información durante su transmisión, garantizando que solo los dispositivos autorizados puedan leer y entender los datos. A este tipo de comunicación segura se le conoce como HTTPS (Hyper Text Transfer Protocol Secure).

Existen tres formas de obtener certificados SSL/TLS:

Certificado emitido por una entidad certificadora: Estos certificados son proporcionados por organizaciones reconocidas y son altamente confiables para entornos de producción.

Certificado emitido por nuestra propia entidad certificadora: Nos permite emitir certificados internos, ideal para redes privadas, aunque podría no ser reconocido por todos los navegadores.

Certificado autofirmado: Generado por el propio servidor sin intervención de una entidad externa. Es útil para entornos de prueba o uso personal, aunque los navegadores suelen mostrar advertencias de seguridad.

En este manual, crearemos un **certificado autofirmado**. Sin embargo, si cuentas con alguno de los otros dos tipos de certificados, será una opción mucho mejor para asegurar la comunicación en tu nube Nextcloud.

La mayoría de las distribuciones de Linux vienen con **OpenSSL** preinstalado. **OpenSSL** es una herramienta fundamental para la creación de certificados de seguridad, ya que nos permite generar tanto la clave pública como la clave privada de nuestro certificado. Estos son los comandos para generar el certificado autofirmado

Primero, generaremos la clave privada del certificado, openssl se utiliza para generar una clave privada RSA de 2048 bits con el comando:

```
sudo openssl genrsa -out <NombreDeLaClave>.key 2048
```

```
ubuntu@ip-172-31-82-65:~$ sudo openssl genrsa -out UNAM_priv.key 2048
ubuntu@ip-172-31-82-65:~$ ls
UNAM_priv.key
ubuntu@ip-172-31-82-65:~$
```

Figura 1.37. Generar clave privada

Como segundo paso, generaremos nuestra clave pública y nuestra entidad certificadora. Esto también lo haremos con OpenSSL usando el siguiente comando. Durante el proceso, OpenSSL nos hará algunas preguntas; se recomienda responder todas y establecer una contraseña segura, que será necesaria para las solicitudes de conexión.

```
openssl req -new -key <clavePrivada> -out < NombreDeLaClave >.csr
```

```
ubuntu@ip-172-31-82-65:~$ sudo openssl req -new -key UNAM_priv.key -out UNAM_CA.csr
```

Figura 1.38. Generar entidad certificadora

Ahora generamos el certificado completo utilizando el comando:

```
openssl x509 -req -days 365 -in <nombreCA>.csr -signkey
<nombreClavePrivada>.key -out <nombreDelCertificado>.crt
```

```
ubuntu@ip-172-31-82-65:~$ sudo openssl x509 -req -days 365 -in UNAM_CA.csr -signkey UNAM_priv.key -out UNAM_cert.crt
Certificate request self-signature ok
subject=C = MX, ST = Mexico, L = Mexico, O = UNAM, CN = DGAPA-server, emailAddress = mseragonf@gmail.com
ubuntu@ip-172-31-82-65:~$ ls
UNAM_CA.csr  UNAM_cert.crt  UNAM_priv.key
ubuntu@ip-172-31-82-65:~$
```

Figura 1.39. Generar certificado final

Para finalizar, moveremos los tres certificados al almacén de certificados predeterminado de Apache, ubicado en /etc/ssl/certs/nextcloud_certs. Es posible que esta carpeta no exista, en cuyo caso podemos crearla con el siguiente comando:

```
sudo mkdir -p /etc/ssl/certs/nextcloud_certs
```

Luego, movemos los certificados generados a esta carpeta:

```
sudo mv ./*.key ./*.crt ./*.csr /etc/ssl/certs/nextcloud_certs/
```

```
ubuntu@ip-172-31-82-65:~$ sudo mkdir -p /etc/ssl/certs/nextcloud_certs
ubuntu@ip-172-31-82-65:~$ sudo mv ./*.key ./*.cert ./*.csr /etc/ssl/certs/nextcloud_certs/
ubuntu@ip-172-31-82-65:~$ ls /etc/ssl/certs/nextcloud_certs/
UNAM_CA.csr  UNAM_cert.crt  UNAM_priv.key
ubuntu@ip-172-31-82-65:~$
```

Figura 1.40. Mover los certificados para nextcloud a nextcloud_certs

Apache proporciona un ejemplo de cómo agregar configuraciones de certificados en un archivo llamado default-ssl.conf. Para agregar una nueva conexión con los certificados de Nextcloud, copiaremos y modificaremos este archivo. Primero, ingresamos a la carpeta /etc/apache2/sites-available con:

```
cd /etc/apache2/sites-available
```

```
ubuntu@ip-172-31-82-65:/etc/apache2/sites-available$ ls
000-default.conf  default-ssl.conf  nextcloud.conf
ubuntu@ip-172-31-82-65:/etc/apache2/sites-available$
```

Figura 1.41: Archivo de ejemplo default-ssl.conf

Lo copiamos y le pondremos el nombre nextcloud-ssl.conf con el comando:

```
sudo cp default-ssl.conf nextcloud-ssl.conf
```

Al abrir el archivo nextcloud-ssl.conf con el comando `sudo nano nextcloud-ssl.conf`, modificaremos las líneas marcadas en la figura 1.42. Estas líneas son, específicamente:

ServerName: aquí debe colocarse la dirección IP pública o el dominio/subdominio que apunte al servidor.

SSLCertificateFile: especifica la ruta completa del archivo del certificado público (por ejemplo, /etc/ssl/certs/nextcloud_certs/nombreCertificadoFinal.crt).

SSLCertificateKeyFile: especifica la ruta completa del archivo de la clave privada (por ejemplo, /etc/ssl/certs/nextcloud_certs/nombreClavePrivada.key).

SSLCertificateChainFile: apunta al archivo que contiene la cadena de certificados para el servidor, si es necesario (por ejemplo, /etc/ssl/certs/nextcloud_certs/nombreCertificadoFinal.crt).

```

<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    ServerName <server ip, dominio o subdominio>
    DocumentRoot /var/www/nextcloud

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/nextcloud_ssl_error.log
    CustomLog ${APACHE_LOG_DIR}/nextcloud_ssl_access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf

    #
    # SSL Engine Switch:
    # Enable/Disable SSL for this virtual host.
    SSLEngine on

    #
    # A self-signed (snakeoil) certificate can be created by installing
    # the ssl-cert package. See
    # /usr/share/doc/apache2/README.Debian.gz for more info.
    # If both key and certificate are stored in the same file, only the
    # SSLCertificateFile directive is needed.
    SSLCertificateFile /etc/ssl/certs/nextcloud_certs/<nombreCertificadoFinal>.cert
    SSLCertificateKeyFile /etc/ssl/certs/nextcloud_certs/<nombreClavePrivada>.key

    #
    # Server Certificate Chain:
    # Point SSLCertificateChainFile at a file containing the
    # concatenation of PEM encoded CA certificates which form the
    # certificate chain for the server certificate. Alternatively
    # the referenced file can be the same as SSLCertificateFile
    # when the CA certificates are directly appended to the server
    # certificate for convenience.
    SSLCertificateChainFile /etc/ssl/certs/nextcloud_certs/<nombreCertificadoFinal>.cert

```

Figura 1.42. Modificaciones sobre nextcloud-ssl.conf

Después de modificar y guardar el archivo, debemos habilitar el módulo SSL de Apache y el archivo de configuración SSL para que se aplique a Nextcloud. Esto se puede hacer con los siguientes comandos:

```

sudo a2enmod ssl
sudo a2ensite nextcloud-ssl.conf
sudo systemctl restart apache2

```

Con esto, el servidor estará configurado para utilizar SSL, permitiendo conexiones seguras mediante HTTPS.

```

ubuntu@ip-172-31-82-65:~$ sudo a2enmod ssl
sudo a2ensite nextcloud-ssl.conf
sudo systemctl restart apache2
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
Enabling site nextcloud-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
ubuntu@ip-172-31-82-65:~$

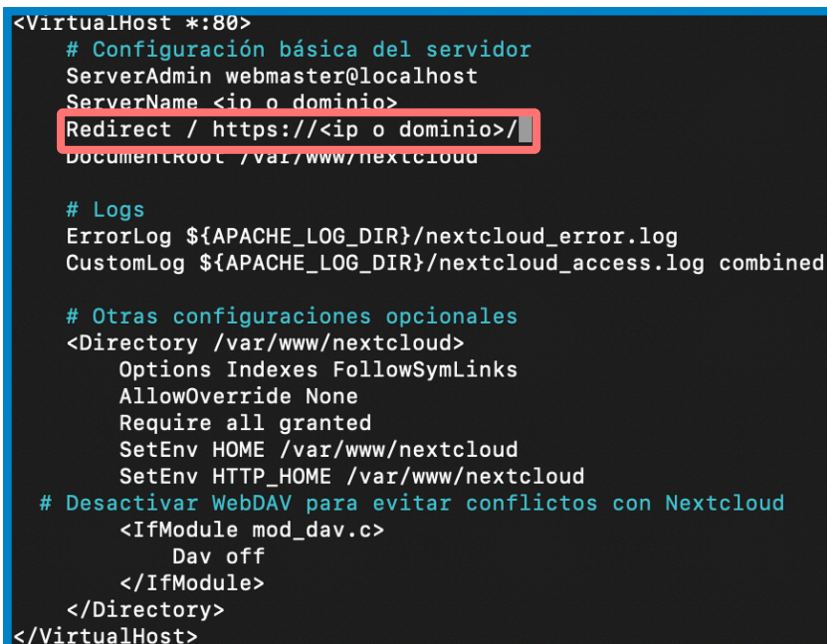
```

Figura 1.43. Reiniciar servicio y actualizar cambios

Al forzar el uso del certificado y configurar las conexiones HTTPS, podemos verificar que el mensaje de advertencia de conexión insegura en la pantalla de Nextcloud ha desaparecido. Esto indica que la conexión ahora está protegida. Sin embargo, dado que estamos usando un certificado autofirmado, la mayoría de los navegadores lo identificarán como una posible amenaza y mostrarán una advertencia de seguridad al intentar acceder.

Es muy recomendable obtener un certificado de una autoridad de certificación confiable para evitar estas advertencias en los navegadores y mejorar la seguridad y la confianza de los usuarios en el servicio de Nextcloud

Para solucionar definitivamente este problema y asegurarnos de que la conexión siempre sea segura, es necesario redirigir todas las conexiones a HTTPS. Para lograr esto, debemos modificar el archivo `/etc/apache2/sites-available/nextcloud.conf` y agregar la siguiente línea como se ve en la figura 1.44:



```
<VirtualHost *:80>
# Configuración básica del servidor
ServerAdmin webmaster@localhost
ServerName <ip o dominio>
Redirect / https://<ip o dominio>/
DocumentRoot /var/www/nextcloud

# Logs
ErrorLog ${APACHE_LOG_DIR}/nextcloud_error.log
CustomLog ${APACHE_LOG_DIR}/nextcloud_access.log combined

# Otras configuraciones opcionales
<Directory /var/www/nextcloud>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
    SetEnv HOME /var/www/nextcloud
    SetEnv HTTP_HOME /var/www/nextcloud
# Desactivar WebDAV para evitar conflictos con Nextcloud
<IfModule mod_dav.c>
    Dav off
</IfModule>
</Directory>
</VirtualHost>
```

Figura 1.44. Modificar nextcloud.conf

Ahora reiniciamos apache y al acceder a la dirección, siempre se redirigirá a las conexiones HTTPS y el error o brecha de seguridad desaparecerá.

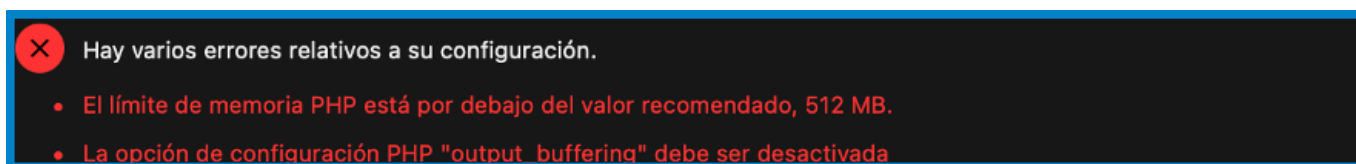


Figura 1.45. Error sobre https solucionado

LIMITE DE MEMORIA DE PHP:

Para aumentar la memoria asignada a PHP en Nextcloud, necesitamos modificar la configuración en el archivo `php.ini`. Este archivo se encuentra en el directorio `/etc/php/<versión>/apache2/`. De los archivos presentes, el que nos interesa editar es `php.ini`, y lo haremos con el siguiente comando:

```
sudo nano /etc/php/<versión>/apache2/php.ini
```

Dado que este archivo es extenso, podemos buscar rápidamente la variable que nos interesa usando la combinación de teclas **Ctrl + W**, y luego escribiendo `memory_limit`.

En la configuración, verás una línea similar a esta:

```
memory_limit = 128M
```

Aumenta el valor según las necesidades de tu servidor para que Nextcloud pueda manejar mejor la carga de trabajo, como se ve en la figura 1.46.

```
; Maximum amount of memory a script may consume  
; https://php.net/memory-limit  
memory_limit = 512M
```

Figura 1.46. PHP limit_memory

Dentro de este mismo archivo buscaremos `output_buffering`, y usando la combinación de teclas **Ctrl + W**, buscamos **`output_buffering = 4096`**, cambiamos el valor de 4096 a `off` como se ve en la figura 1.47.

```
; Note: This directive is hardcoded to Off for the CLI SAPI  
; Default Value: Off  
; Development Value: 4096  
; Production Value: 4096  
; https://php.net/output-buffering  
output_buffering = off
```

Figura 1.47. Desactivar output_buffering

Ahora reiniciamos `apache` y al acceder a Nextcloud los errores abran desaparecido.

ADVERTENCIAS COMUNES

Algunas advertencias comunes se pueden arreglar con el comando:

```
sudo -u www-data php /var/www/nextcloud/occ db:add-missing-indices
sudo -u www-data php /var/www/nextcloud/occ maintenance:repair --include-expensive
```

```
ubuntu@ip-172-31-82-65:~$ sudo -u www-data php /var/www/nextcloud/occ maintenance:repair --include-expensive
ubuntu@ip-172-31-82-65:~$ sudo -u www-data php /var/www/nextcloud/occ db:add-missing-indices
Adding additional systag_by_objectid index to the oc_systemtag_object_mapping table, this can take some time...
oc_systemtag_object_mapping table updated successfully.
```

Figura 1.48. Agregar índices faltantes en tablas de MariaDB

- Algunos encabezados no están correctamente configurados en su instancia - El encabezado HTTP `Strict-Transport-Security` no está configurado (debería ser de al menos `15552000` segundos). Para una seguridad mejorada, se recomienda habilitar HSTS. Para más detalles compruebe la documentación 21.

Figura 1.49. Advertencia sobre encabezados

Otra advertencia que podemos quitar es la mostrada en la figura 1.51, esta se soluciona entrando al archivo de configuración nextcloud-ssl.conf y agregar las siguientes líneas:

```
<IfModule mod_headers.c>
    Header always set Strict-Transport-Security "max-age=15552000; includeSubDomains"
</IfModule>
```

```
# This exports the standard SSL/TLS related 'SSL_*' environment variables.
# Per default this exportation is switched off for performance reasons,
# because the extraction step is an expensive operation and is usually
# useless for serving static content. So one usually enables the
# exportation for CGI and SSI requests only.
# o OptRenegotiate:
# This enables optimized SSL connection renegotiation handling when SSL
# directives are used in per-directory context.
#SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
<FilesMatch "\.(?:cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>
<Directory /usr/lib/cgi-bin>
    SSLOptions +StdEnvVars
</Directory>
<IfModule mod_headers.c>
    Header always set Strict-Transport-Security "max-age=15552000; includeSubDomains"
</IfModule>
</VirtualHost>
```

Figura 1.50. Encabezados agregados

Activamos los headers con los comandos:

```
sudo a2enmod headers
sudo systemctl restart apache2
```

FORTALECIMIENTO DE A PACHE:

Con esto habremos cubierto en gran medida el rendimiento y la seguridad, pero aún es recomendable reforzar algunos aspectos adicionales de nuestro servicio Apache. Esto ayudará a evitar que posibles atacantes se aprovechen de ciertas vulnerabilidades en el sistema

Empezaremos por ocultar ciertos aspectos de Apache. En algunas ocasiones, si se manejan archivos de manera incorrecta o se intenta acceder a un enlace inexistente, es posible que aparezca una página como la mostrada en la figura 1.51. Esta página revela características de nuestro servidor, como la versión de Apache y el sistema operativo que se está utilizando. Esto no es recomendable, ya que esta información puede ser utilizada para identificar vulnerabilidades específicas y atacar los puntos débiles del sistema. Por esta razón, es fundamental ocultar estos datos.

Not Found

The requested URL was not found on this server.

Apache/2.4.58 (Ubuntu) Server at 3.93.65.232 Port 443

Figura 1.51. Pagina de Not Found a la que dirige apache

Abrimos el archivo de configuración de apache con:

```
sudo nano /etc/apache2/apache2.conf
```

y agregaresmo las siguientes lineasal final del archivo:

```
ServerSignature Off  
ServerTokens Prod
```

```
LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined  
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined  
LogFormat "%h %l %u %t \"%r\" %>s %O" common  
LogFormat "%{Referer}i -> %U" referer  
LogFormat "%{User-agent}i" agent  
  
# Include of directories ignores editors' and dpkg's backup files,  
# see README.Debian for details.  
  
# Include generic snippets of statements  
IncludeOptional conf-enabled/*.conf  
  
# Include the virtual host configurations:  
IncludeOptional sites-enabled/*.conf  
ServerSignature Off  
ServerTokens Prod
```

Figura 1.52. Líneas agregadas en apache2.conf

Al reiniciar Apache y acceder a una página desconocida, podemos confirmar que ya no se muestran datos sensibles, como la versión de Apache y el sistema operativo en uso. Esto ayuda a mejorar la seguridad del servidor, ya que limita la información disponible que podría ser aprovechada por posibles atacantes.

Not Found

The requested URL was not found on this server.

Figura 1.53. Pagina de Not Found sin datos

Otra característica de seguridad importante a considerar es la desactivación del listado de directorios. Esto evita que los usuarios puedan ver el contenido de carpetas en ubicaciones no públicas. Para lograrlo, es recomendable configurar Apache de manera que el acceso a estas carpetas esté restringido, evitando que el servidor muestre automáticamente el listado de archivos cuando no hay un archivo de índice disponible.

Desactivar esta opción es muy simple, solo desactivamos el módulo autoindex, eso lo logramos con el comando:

```
sudo a2dismod --force autoindex
```

Con esto tendríamos protección contra ataques básicos, si se desea fortalecer más apache **se recomienda instalar MOD SECURITY y MOD EVASIVE, así como cambiar usuario por defecto de apache.**

NOTA:

La configuración detallada de la instalación de los módulos security y evasive lo podemos encontrar en el *Manual de Apache: Instalación y fortalecimiento (Galindo Reyes, 2024, p. 23)*. Para más información, consulte el apartado *“Fortalecer Apache”*.

- **Manual de
usos
Nextcloud**

CREAR Y ADMINISTRAR USUARIOS DE NEXTCLOUD

Nextcloud, como vimos en la introducción, es una plataforma que permite almacenar y administrar información, ofreciendo una alternativa a las nubes comerciales convencionales. Sin embargo, Nextcloud incluye muchas funcionalidades adicionales que resultan útiles, especialmente al momento de gestionar múltiples usuarios en un entorno colaborativo.

Una de las principales ventajas de Nextcloud es la posibilidad de crear y administrar usuarios, lo que facilita el acceso compartido y la organización de datos entre varios usuarios o equipos. Con la capacidad de asignar roles, crear grupos, y establecer permisos específicos, Nextcloud permite una administración detallada y segura de los recursos. En esta sección, aprenderemos a crear usuarios y a gestionar sus permisos y roles dentro de la plataforma, asegurando un entorno controlado y eficiente para todos los usuarios.

Para acceder a este apartado, inicia sesión en Nextcloud con tu cuenta root o de administrador. Una vez dentro, dirígete a tu perfil pulsando en el círculo ubicado en la esquina superior derecha de la página, como se muestra en la figura 2.1 y pulsa en el apartado de cuentas.

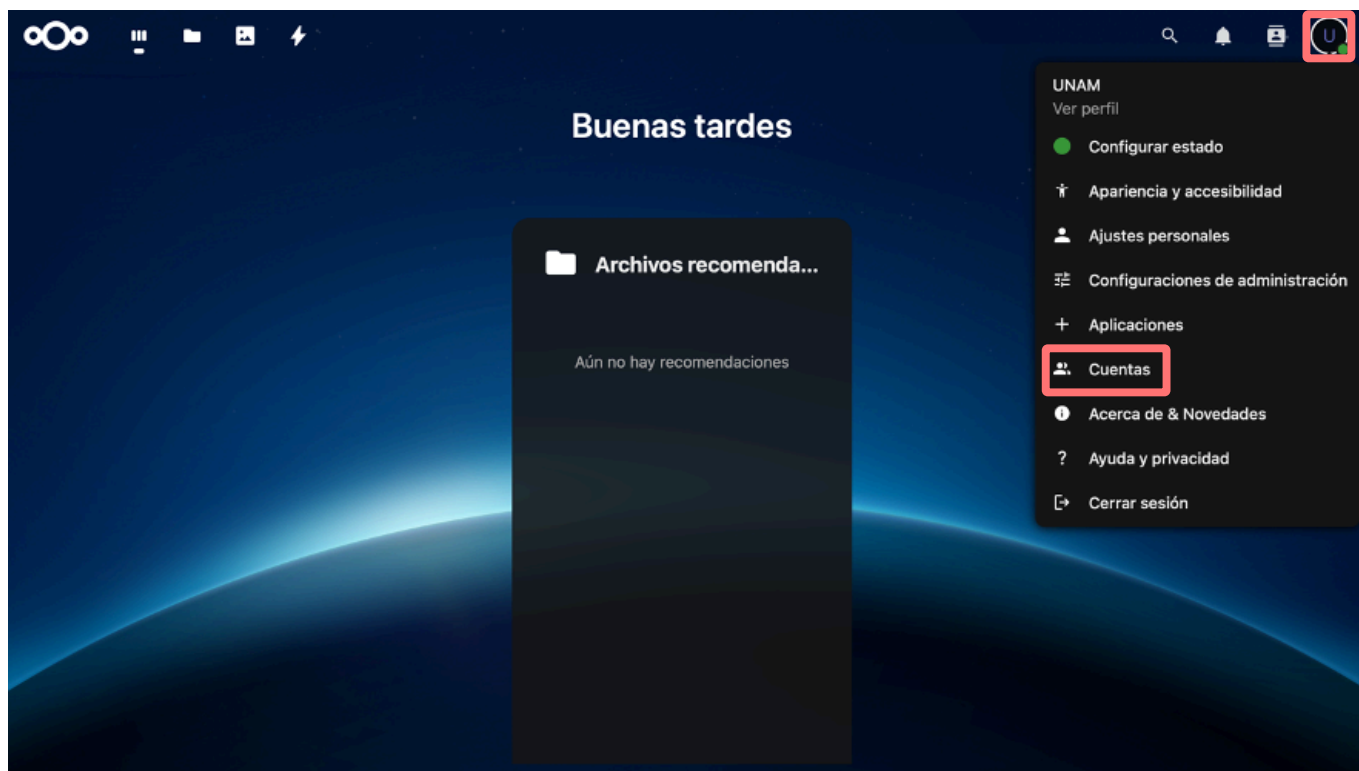


Figura 2.1. Acceder a Cuentas

Comenzando con la creación de un nuevo usuario, esto se realizará pulsando en el botón + Nueva cuenta, señalado en color rojo en la figura 2.2.

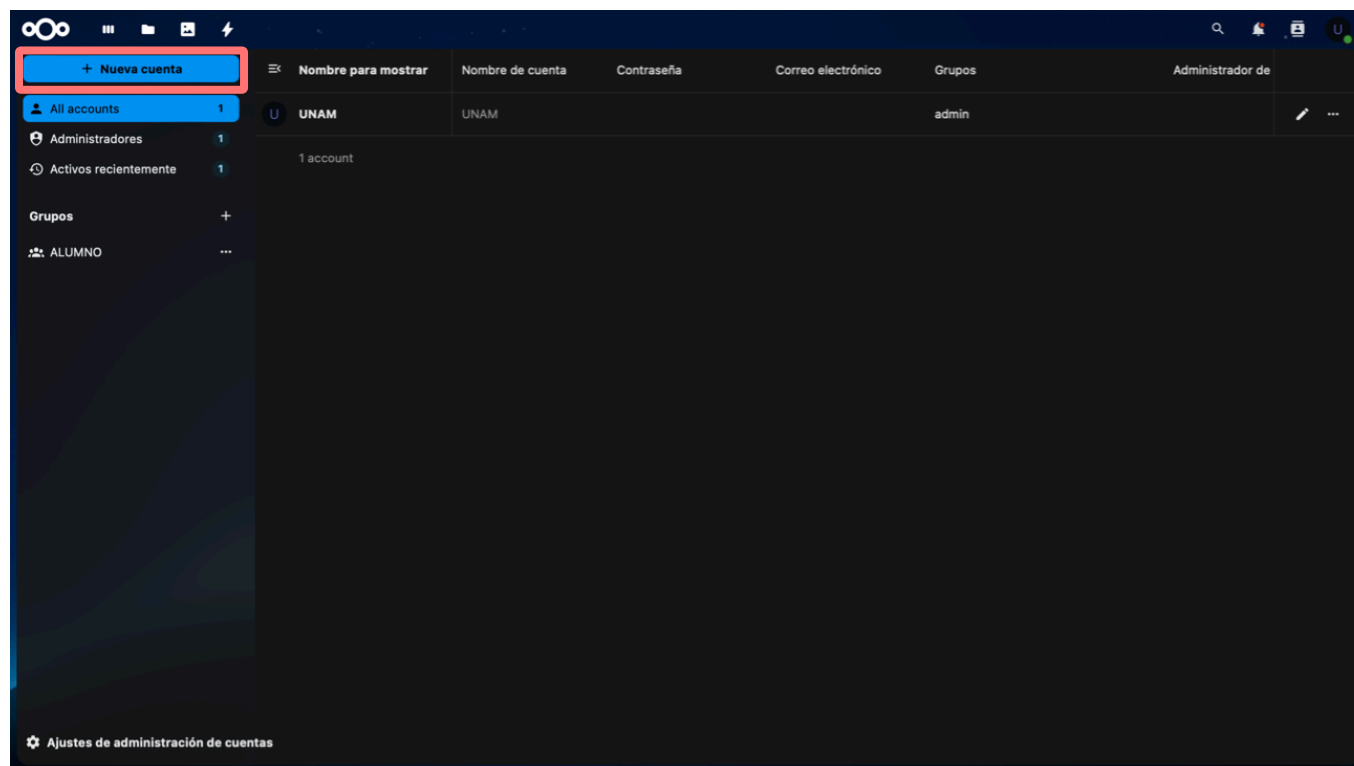


Figura 2.2. Creación de cuentas

Para crear una cuenta en Nextcloud, solo debes completar los campos requeridos en el formulario de usuario. Aunque no todos los campos son obligatorios, puedes modificarlos más adelante si es necesario. Esto facilita una configuración inicial rápida y flexible de las cuentas, con la opción de actualizar los datos cuando se requiera. Una vez creada la cuenta, es importante proporcionar al usuario correspondiente los datos de acceso para que pueda utilizar su nueva cuenta.

En este mismo menú es posible crear grupos para organizar y agrupar cuentas de usuario, lo cual resulta útil para varias acciones administrativas. Agrupar usuarios permite asignar permisos específicos a todos los miembros de un grupo de una sola vez. Además, los grupos simplifican la compartición de archivos y carpetas, ya que los administradores pueden compartir recursos con un grupo completo sin tener que configurar el acceso usuario por usuario, agilizando la colaboración. Los grupos también permiten enviar notificaciones a conjuntos específicos de usuarios, asegurando que todos los miembros reciban actualizaciones importantes.

Estas características facilitan la creación de una jerarquía dentro de la organización, permitiendo personalizar cómo se muestra la información a los usuarios y estableciendo límites claramente definidos. Además, es posible otorgar permisos de administración parciales, de modo que un usuario tenga control administrativo únicamente sobre ciertos grupos específicos. Esto permite delegar la administración de áreas o equipos particulares sin conceder acceso total a toda la organización, lo que optimiza el control y la seguridad en la gestión de usuarios.

Una vez que el usuario inicie sesión, podrá cambiar su contraseña para mantener su cuenta segura y asegurar que solo él tenga control completo sobre su espacio de nube asignado, aunque continúe existiendo una jerarquía superior. Esta actualización de contraseña se debe realizar en el apartado de Seguridad, como se muestra en la figura 2.3, el usuario tendrá acceso a múltiples características de su configuración con las cuales puede ir jugando y modificando dentro de su nube sin alterar nada fuera de ella.

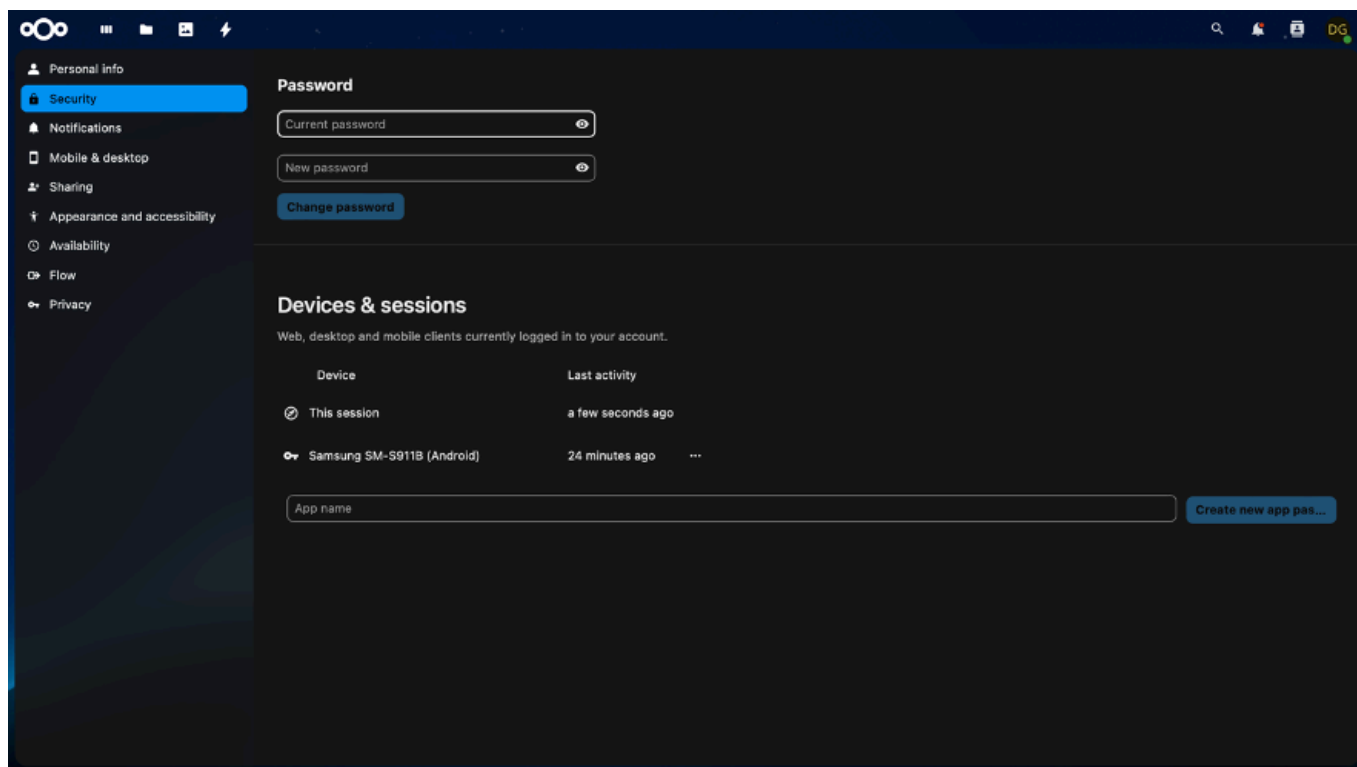


Figura 2.3. Cambiar contraseña como usuario

SUBIR ARCHIVOS Y ADMINISTRAR PERMISOS SOBRE LOS MISMO

Como vimos anteriormente, Nextcloud permite subir y administrar archivos en la cuenta root o de administrador. A continuación, veremos una breve introducción sobre cómo realizar estas operaciones desde la cuenta de administrador.

Subir archivos en Nextcloud es un proceso muy sencillo. Primero, dirígete al apartado de Archivos. Desde allí, puedes crear carpetas o subir archivos directamente en la carpeta raíz. Para crear una nueva carpeta, haz clic en el botón Nuevo o New, donde verás opciones como subir un archivo o una carpeta, así como crear una nueva carpeta o incluso algunos tipos de archivos, como se muestra en la figura 2.4. Esto facilita organizar el contenido en Nextcloud según tus necesidades y mantener una estructura ordenada.

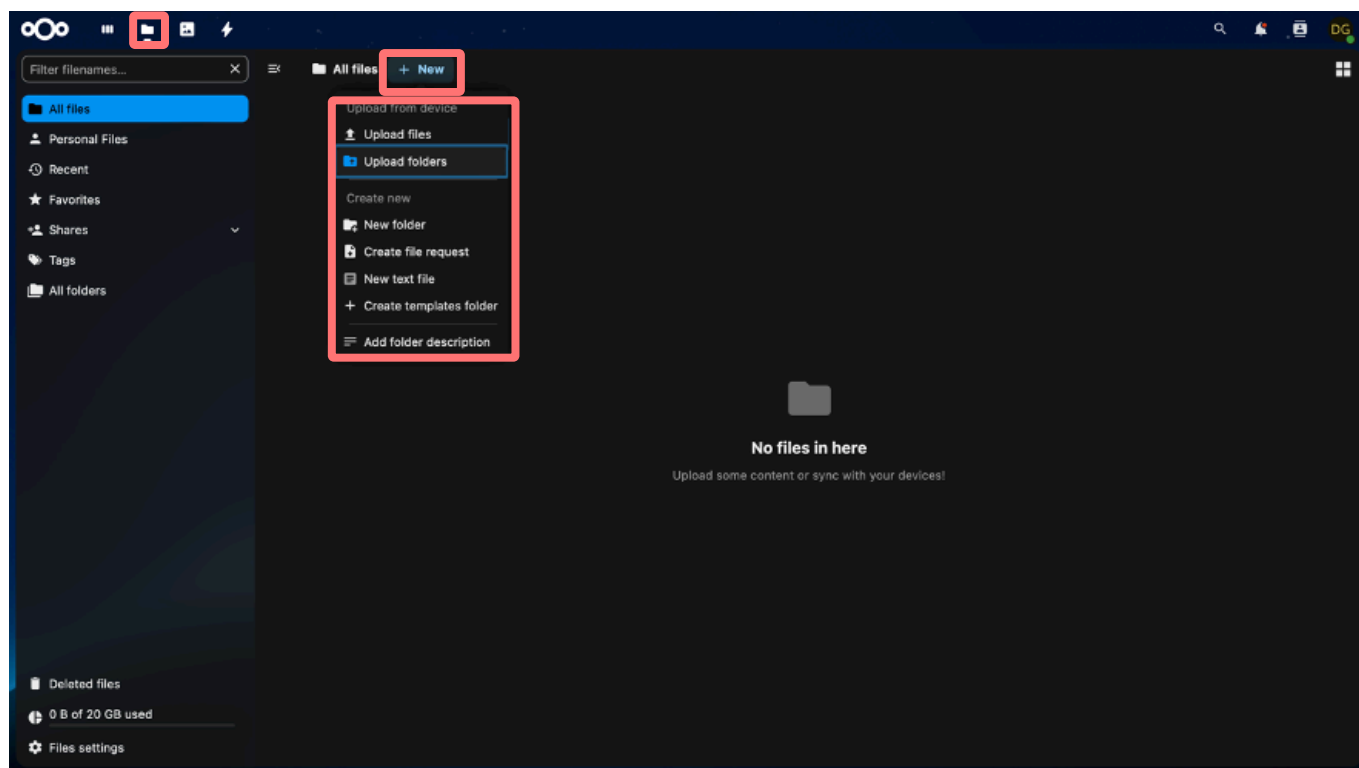


Figura 2.4. Crear o cargar archivos

Estas opciones permiten crear carpetas y archivos de manera sencilla, pero lo más interesante es la función de compartir. Para compartir un archivo, simplemente selecciona el que deseas y pulsa la opción de compartir, como se muestra en la figura 2.5. Esto te dará acceso a distintas opciones para compartirlo con otros usuarios o grupos.

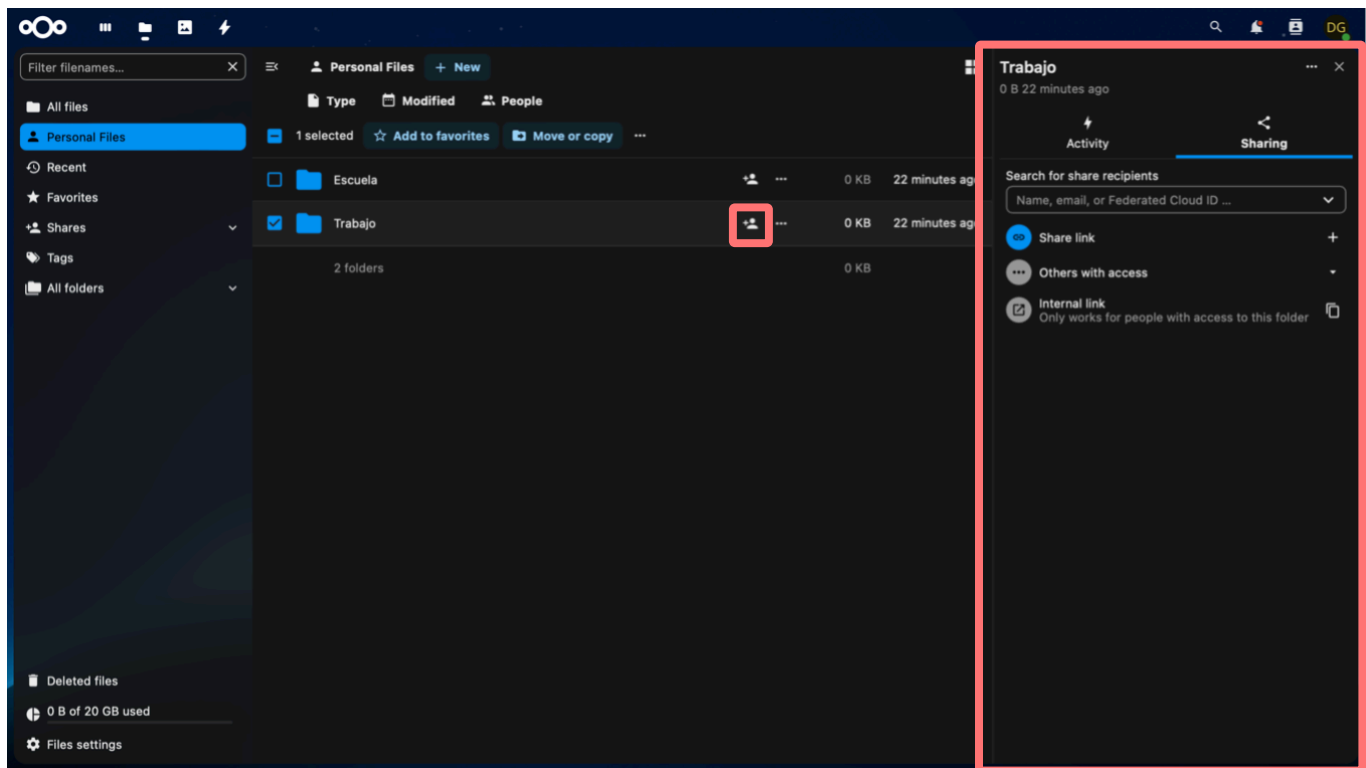


Figura 2.5. Compartir carpetas o archivos

En el apartado de búsqueda, puedes encontrar grupos o personas que pertenecen a la organización. Por ejemplo, si existe un grupo llamado "Alumno", podrás compartir archivos o carpetas con todos los miembros de ese grupo y definir los permisos que tendrán, como solo lectura, solo escritura o ambos, así como también cuenta con muchos permisos personalizados que pueden ser de utilidad para acciones más específicas, como se muestra en la figura 2.6, también es posible crear un link para compartir con personas que no tengan una cuenta dentro de la nube privada, esto con la opción compartir link.

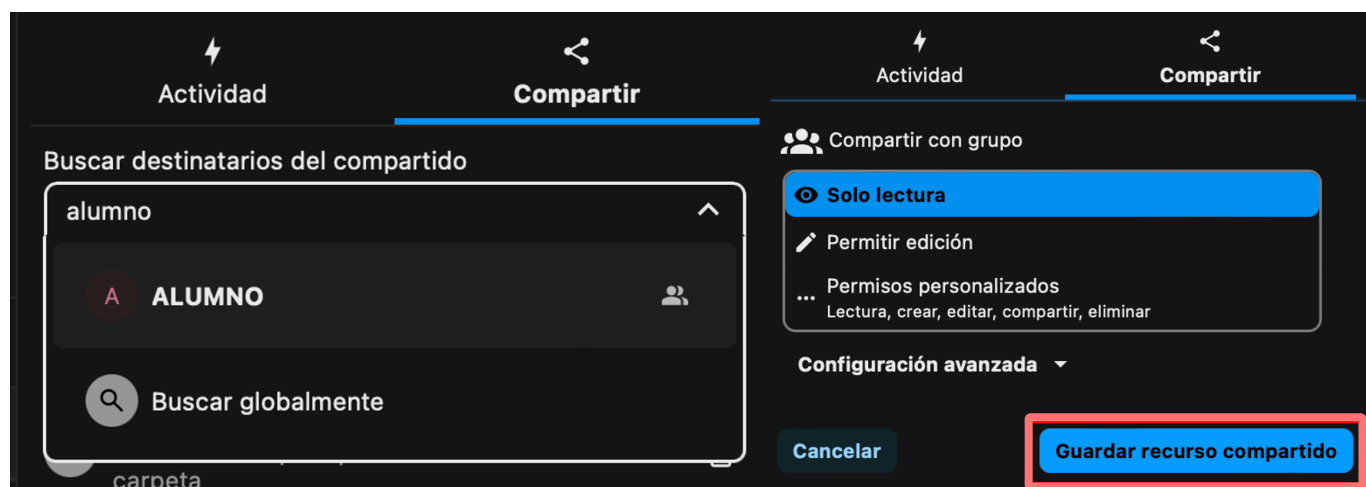


Figura 2.6. Compartir con grupos

INSTALACIÓN DE APLICACIONES

Nextcloud ofrece una amplia variedad de funcionalidades impresionantes que continúan evolucionando. Por ejemplo, permite el uso de editores de texto y archivos en tiempo real, edición de video, edición fotográfica y aplicaciones visuales, entre muchas otras opciones con las que podremos jugar desde el perfil de admin o root.

Para buscar las aplicaciones que puedan interesarnos dentro de nuestra nube, solo es necesario ir a la página de Aplicaciones, como se muestra en la figura 2.7. Aquí encontrarás una variedad de herramientas y extensiones que puedes añadir para ampliar las funcionalidades de Nextcloud según tus necesidades.

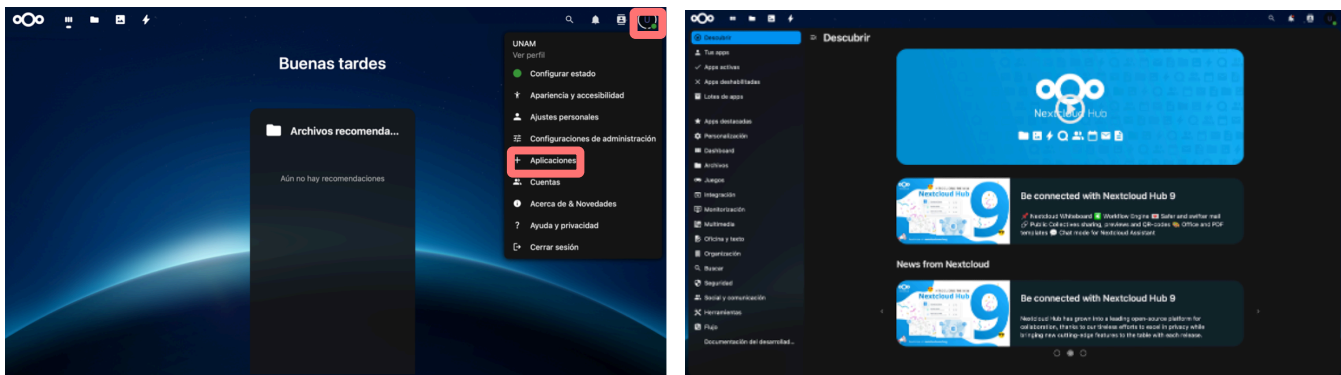


Figura 2.7. Acceder a aplicaciones

En esta sección, podremos ver un menú con varias extensiones en el apartado Descubrir, además de acceder a las aplicaciones ya instaladas. También tenemos la opción de habilitar o deshabilitar aplicaciones en el sistema, similar a una tienda de aplicaciones organizada por categorías, como se muestra en el menú lateral.

INSTALACIÓN DE NEXTCLOUD PARA USUARIOS

Nextcloud cuenta con aplicaciones móviles para dispositivos celulares, así como aplicaciones de escritorio para equipos de cómputo. Además, es accesible desde cualquier navegador. Esto permite acceder a la plataforma desde cualquiera de estos recursos, siempre que se disponga de una cuenta válida y la dirección o dominio de la nube a la que se quiere ingresar. Simplemente es necesario iniciar sesión y listo: se tiene acceso a una nube privada en la que se pueden almacenar, compartir y sincronizar archivos de forma segura desde cualquier lugar.

Instalación para dispositivos Android:

Para instalar Nextcloud en un dispositivo Android, primero abre la tienda de aplicaciones, Play Store. Luego, busca "Nextcloud" en la barra de búsqueda y selecciona la aplicación oficial que aparece en los resultados, como se muestra en la figura 2.8. A continuación, presiona el botón de Descargar para instalar la aplicación en tu dispositivo.

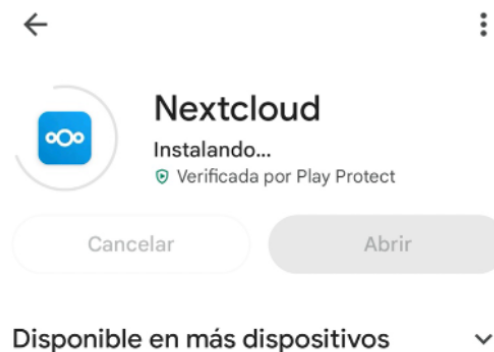


Figura 2.8. Descarga de Nextcloud Android

Una vez sea descargada la aplicación, ábrela y serás recibido con una pantalla que solicita la dirección del servidor que hospeda nube Nextcloud, como se muestra en la figura 2.9. Aquí deberás ingresar la dirección ip o dominio correspondiente a tu servidor Nextcloud.

Posteriormente, la aplicación te pedirá ingresar los datos de tu cuenta, que debe haber sido creada previamente en el servidor Nextcloud para permitir el acceso. Después de proporcionar esta información, podrás acceder a tu nube y comenzar a sincronizar y gestionar tus archivos desde el dispositivo móvil con Android.

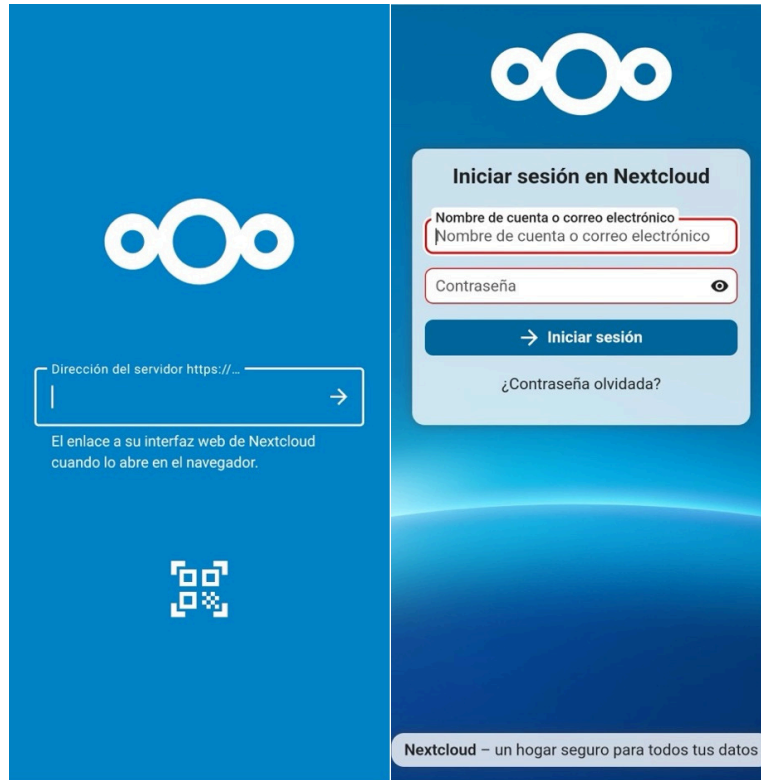


Figura 2.9. Datos para ingresar a nextcloud desde Android

Nextcloud se destaca como una plataforma que no solo permite almacenar y compartir archivos, sino también organizar equipos de trabajo y optimizar el flujo de colaboración mediante aplicaciones adicionales. Su enfoque en la seguridad, la administración de usuarios, y la facilidad de uso hace de Nextcloud una alternativa confiable y personalizable a las opciones comerciales de almacenamiento en la nube, con la ventaja de mantener el control sobre los datos.

Como último paso, recuerda revisar regularmente las actualizaciones y opciones de seguridad, y considerar implementar prácticas adicionales de respaldo y recuperación para proteger la integridad de los datos. Aprovechar las extensiones y personalizaciones disponibles te permitirá mejorar continuamente la experiencia de usuario y adaptarla a las necesidades cambiantes de tu organización.

Con Nextcloud, cuentas con una plataforma potente y escalable, diseñada para crecer contigo y simplificar el manejo de archivos y la colaboración en tu equipo.

Bibliografía:

- Nextcloud. (2024). Nextcloud user manual. Nextcloud Documentation. https://docs.nextcloud.com/server/latest/user_manual/en/
- PHP. (n.d.). Instalación de PHP. Recuperado el 16 de noviembre de 2024, de <https://www.php.net/manual/es/install.php>
- MariaDB Foundation. (2024). MariaDB Server Knowledge Base [PDF]. Recuperado de <https://mariadb.org/wp-content/uploads/2024/10/MariaDBServerKnowledgeBase.pdf>
- Apache Software Foundation. (n.d.). Documentación de Apache HTTP Server 2.4. Recuperado el 16 de noviembre de 2024, de <https://httpd.apache.org/docs/2.4/es/>
- Cutipa, G. (n.d.). Apache 2.4 Hardening. Recuperado el 16 de noviembre de 2024, de <https://guidocutipa.blog.bo/apache-2-4-hardening/>
- Galindo Reyes, D. A. (Ed.). (s.f.). Manual de Apache: Instalación y fortalecimiento. Instituto de Ciencias Aplicadas y Tecnología (ICAT), UNAM.
- Galindo Reyes, D. A. (Ed.). (s.f.). Manual de Ubuntu: Instalación y funcionamiento. Instituto de Ciencias Aplicadas y Tecnología (ICAT), UNAM.