

1. INTRODUCCIÓN	3
1.1 REQUISITOS PARA SEGUIR LA GUIA	3
2. CREAR UN DROPLET E INSTALACIÓN DE APACHE	4
3. AÑADIENDO UN FIREWALL	9
4. SEGURIDAD DE SSH	11
4. AÑADIENDO UN DNS (DOMINIO)	14
5. INSTALAR UNA BASE DE DATOS	16
6. CONFIGURACIÓN DE APACHE	17
7. INSTALACIÓN DE ADMINISTRADOR DE BASE DE DATOS “NEXTCLOUD”	18
7.1 CREAR UN USUARIO ADMINISTRADOR EN NEXTCLOUD	22
8. HTTPS CON LET'S ENCRYPT	25
FUENTES DE CONSULTA PARA REALIZAR ESTA DOCUMENTACIÓN:	28

1.INTRODUCCIÓN

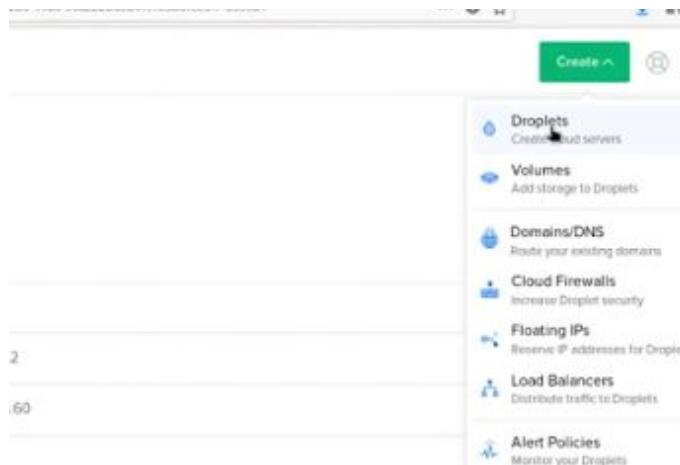
Un servidor virtual privado (o VPS por sus siglas en inglés) es una máquina virtual a la cual se accede por medio de Secure Shell (SSH) , donde desplegamos un servidor virtual de cualquier sistema operativo para realizar cualquier tarea que involucre el networking . Esta guía es para la instalación de un VPS para una página web utilizando el servicio de DigitalOcean llamado Droplets. Droplets es un servicio de pago por los espacios para servidores virtuales , los costos que tiene son muy accesibles, estos dependen del tamaño y las necesidades que requiere nuestro servidor. Otro beneficio de la plataforma es que proporciona soporte a los usuarios.Otro sitio de pago que usaremos es Hover, una página donde podemos comprar dominios por precios bastante económicos ,que también proporciona soporte a sus usuarios. Una recomendación es leer toda la guía y después iniciar a seguir cada paso de esta , ya que pueden surgir dudas en un inicio que se resuelven más adelante de ciertos temas.

1.1 REQUISITOS PARA SEGUIR LA GUIA

- 1.Cuenta en DigitalOcean con créditos.
- 2.Cuenta de Hover con método de pago (opcional).
- 3.Tener Ubuntu Server 20.4 (o más reciente estable) y dispositivo/sistema operativo como windows/GNU/LINUX ,donde podamos acceder y visualizar sitios web.
- 4.Conexión estable a internet , de preferencia vía WiFi para facilitar la asignación de puertos.
- 5.Tener conocimientos básicos de Vi/Vim.
- 6.Tener conocimientos básicos de terminal GNU/Linux

2. CREAR UN DROPLET E INSTALACIÓN DE APACHE

Accedemos a la cuenta de DigitalOcean y vamos al icono de “Create”, ahí seleccionaremos Droplets.

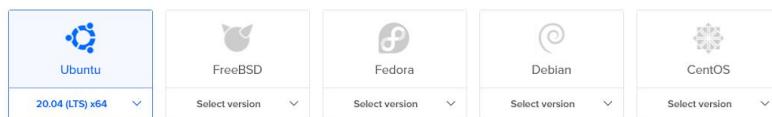


Seleccionamos el sistema operativo para nuestro servidor, en este caso Ubuntu 20.4

Create Droplets

Choose an image ?

Distributions Container distributions Marketplace Backups Custom images



Elegimos el plan Básico y la suscripción mensual de \$5 dólares al mes por 25 GB.

Choose a plan

[Help me choose ↗](#)

SHARED CPU	DEDICATED CPU		
Basic	General Purpose	CPU-Optimized	Memory-Optimized
NEW			

Basic virtual machines with a mix of memory and compute resources. Best for small projects that can handle variable levels of CPU performance, like blogs, web apps and dev/test environments.

\$5/mo \$0.007/hour	\$10/mo \$0.015/hour	\$15/mo \$0.022/hour	\$20/mo \$0.030/hour	\$40/mo \$0.060/hour	\$80/mo \$0.119/hour
1 GB / 1 CPU 25 GB SSD Disk 1000 GB transfer	2 GB / 1 CPU 50 GB SSD Disk 2 TB transfer	2 GB / 2 CPUs 60 GB SSD Disk 3 TB transfer	4 GB / 2 CPUs 80 GB SSD Disk 4 TB transfer	8 GB / 4 CPUs 160 GB SSD Disk 5 TB transfer	16 GB / 8 CPUs 320 GB SSD Disk 6 TB transfer

ⓘ Our Basic Droplet plans, formerly called Standard Droplet plans, range from 1 GB of RAM to 16 GB of RAM. [General Purpose Droplets](#) have more overall resources and are best for production environment, and [Memory-Optimized Droplets](#) have more RAM and disk options for RAM intensive applications.

Seleccionamos el datacenter más cercano a nuestra región.

Add block storage [?](#)

[Add Volume](#)

Choose a datacenter region

 New York	 Amsterdam	 San Francisco	 Singapore	 London	 Frankfurt
1	2	3	1	2	3
 Toronto	 Bangalore				1
1	1				

New Datacenter Available!

You can now create resources in a third datacenter in the San Francisco region

Got It

Nos vamos directamente a la opción de autenticación donde crearemos una contraseña de acceso al servidor virtual (Droplet).

Authentication

SSH keys
A more secure authentication method

Password
Create a root password to access Droplet (less secure)

Create root password *

✖

PASSWORD REQUIREMENTS

- ✓ At least 8 characters long
- ✓ Must contain 1 uppercase (first and last characters don't count)
- ✓ Must contain 1 number
- ✓ Cannot end in a number or special character

i You will not be sent an email containing the Droplet's details or password. Please store your password securely.

Añadimos un nombre al Droplet en “Choose a hostname” y finalizamos en Create Droplet.

Finalize and create

How many Droplets?

Deploy multiple Droplets with the same [configuration](#).

—
1 Droplet
+

Choose a hostname

Give your Droplets an identifying name you will remember them by. Your Droplet name can only contain alphanumeric characters, dashes, and periods.

Add tags

Use tags to organize and relate resources. Tags may contain letters, numbers, colons, dashes, and underscores.

Select Project

Assign Droplets to a project

190300624@ucaribe.edu.mx

▼

This project has been selected as you only have one project

Add backups

Enable backups RECOMMENDED

A system-level backup is taken once a week, and each backup is retained for 4 weeks.

\$1.00/mo (per Droplet)
20% of the Droplet price

Al finalizar su creación iremos a la página principal de nuestra cuenta y veremos que se ha generado un droplet. A lado derecho del nombre del droplet veremos una IP , esa será la IP de nuestro servidor web (posteriormente página web). Si pasamos el mouse sobre de esta y damos click en ella nos aparece la opción copiar, igualmente si no podemos copiarla y pegarla en la misma pantalla que estemos trabajando ,se recomienda tener a la mano lápiz y papel , para anotar tanto la IP como las contraseñas que vayamos generando.

The screenshot shows the DigitalOcean dashboard. At the top, there's a header with a logo, the text '@ucaribe.edu.mx', and a 'DEFAULT' button. Below the header, there are tabs for 'Resources', 'Activity', and 'Settings'. Under 'Resources', there are two sections: 'DROPLETS (1)' containing one item named 'ubuntu-s-1vcpu-1gb-nyc1-01' with IP 159.65.220.156; and 'DOMAINS (1)' containing one item named 'ksbt-progweb.space' with 1A / 3 NS / 1SOA. At the bottom left, there are buttons for 'Create something new' with options like 'Create a Managed Database', 'Start using Spaces', 'Spin up a Load Balancer', and 'Learn more' with links to 'Product Docs' and 'Tutorials'.

Ahora accedemos desde nuestra terminal de Ubuntu a la IP dada del Droplet.

Sustituye **tu IP** por la IP de tu Droplet.

```
Last login: Sun Jan 31 00:17:09 UTC 2021 on tty1
karen-01@clase-prog-web:~$ ssh root@tu_IP_
```

Al dar enter , aceptar el mensaje y colocar la contraseña que se creó junto con el Droplet, este paso nos dará acceso al Droplet desde la terminal de nuestro Ubuntu Server. Al estar dentro del Droplet , estamos en un servidor y puede que le hagan falta algunos updates de paquetes , por lo que debemos correr el siguiente comando:

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

Este comando ejecuta como superusuario los updates y los upgrades automatizando dar a SI (y) a cada una de ellas(puede ser que alguna de ella pida una autorización , dar a SI (y / yes)). Al finalizar debemos ejecutar el siguiente comando, para borrar los paquetes que estén duplicados o ya no sirvan:

```
sudo apt autoremove
```

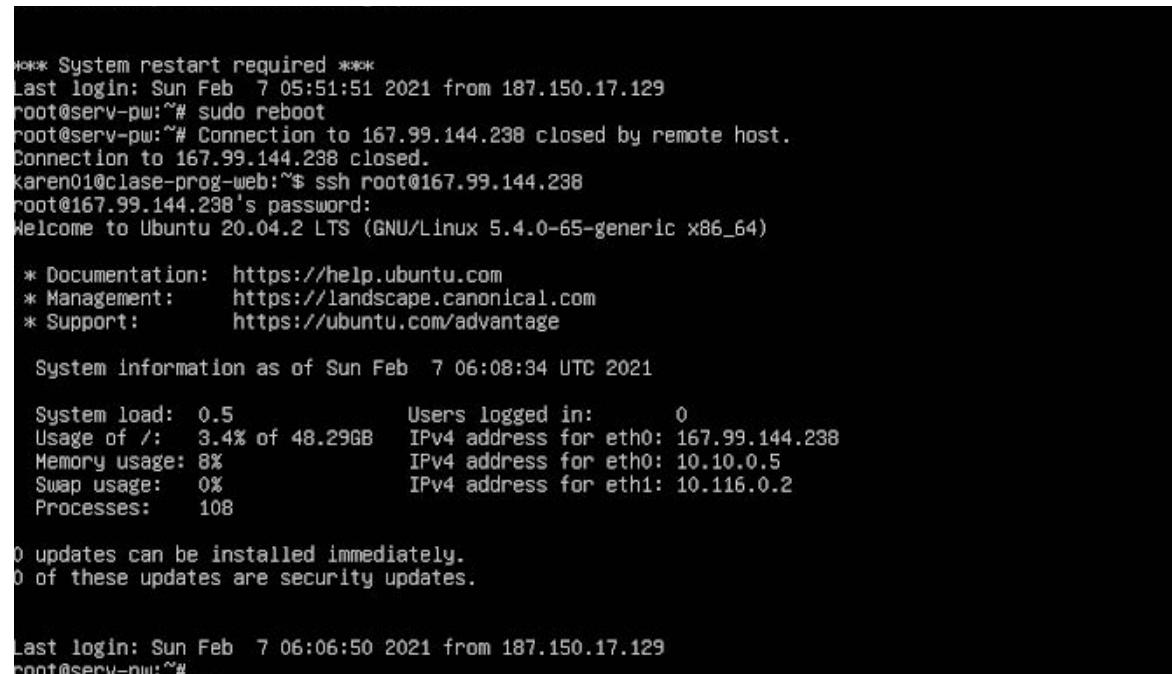
Después ejecutar el siguiente comando:

```
sudo apt install net-tools
```

Este comando instalará net-tools para usar la función `netstat`. Después ejecuta :

```
sudo reboot
```

Este comando reiniciará nuestro Droplet de Ubuntu , nos sacará de la sesión (de vuelta a nuestro usuario del servidor Ubuntu de nuestra PC) y volveremos a logearnos al Droplet por medio de `ssh`. Al volvemos a conectar al Droplet , debemos tener una pantalla de bienvenida sin notificaciones de updates , como la siguiente:



```
*** System restart required ***
Last login: Sun Feb  7 05:51:51 2021 from 187.150.17.129
root@serv-pw:~# sudo reboot
root@serv-pw:~# Connection to 167.99.144.238 closed by remote host.
Connection to 167.99.144.238 closed.
Karen01@clase-prog-web:~$ ssh root@167.99.144.238
root@167.99.144.238's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-65-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 System information as of Sun Feb  7 06:08:34 UTC 2021

 System load:  0.5          Users logged in:      0
 Usage of `/:   3.4% of 48.29GB   IPv4 address for eth0: 167.99.144.238
 Memory usage: 8%
 Swap usage:   0%           IPv4 address for eth0: 10.10.0.5
 Processes:    108          IPv4 address for eth1: 10.116.0.2

0 updates can be installed immediately.
0 of these updates are security updates.

Last login: Sun Feb  7 06:06:50 2021 from 187.150.17.129
root@serv-pw:~#
```

En esta pantalla de bienvenida podemos ver que nos indica el último login que hemos hecho desde una IP , esa es nuestra IP externa , la cual necesitamos anotar en papel para las siguientes configuraciones.

Una vez realizado los pasos anteriores comenzaremos con la instalación de Apache en nuestro Droplet. Ejecutamos el siguiente comando:

```
sudo apt install apache2
```

Al terminar de instalarse ejecutar :

```
systemctl status apache2
(Presionar "q" para salir del despliegue de systemctl)
```

Y ejecutar :

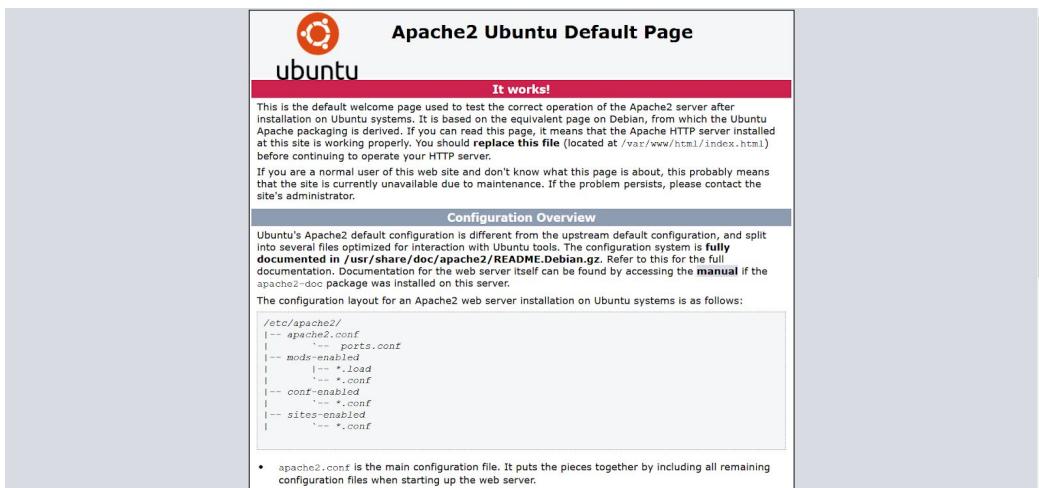
```
sudo netstat -tulpn
```

```
Last login: Sun Feb  7 06:12:55 2021 from 187.150.17.129
root@serv-pw:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2021-02-07 06:13:53 UTC; 7min ago
     Docs: https://httpd.apache.org/docs/2.4/
      Main PID: 1572 (apache2)
        Tasks: 55 (limit: 2345)
       Memory: 5.2M
          CGroup: /system.slice/apache2.service
                  ├─1572 /usr/sbin/apache2 -k start
                  ├─1574 /usr/sbin/apache2 -k start
                  └─1575 /usr/sbin/apache2 -k start

Feb 07 06:13:53 serv-pw systemd[1]: Starting The Apache HTTP Server...
Feb 07 06:13:53 serv-pw apachectl[1571]: AH00558: apache2: Could not reliably determine the server's name
Feb 07 06:13:53 serv-pw systemd[1]: Started The Apache HTTP Server.
root@serv-pw:~# sudo netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*            LISTEN     509/systemd-resolve
tcp        0      0 0.0.0.0:22             0.0.0.0:*            LISTEN     659/sshd: /usr/sbin
tcp6       0      0 ::1:22                ::*:*                 LISTEN     659/sshd: /usr/sbin
tcp6       0      0 ::1:80                ::*:*                 LISTEN     1572/apache2
udp        0      0 127.0.0.53:53           0.0.0.0:*            LISTEN     509/systemd-resolve
root@serv-pw:~#
```

Estos comando nos mostraran que nuestra página Apache esté activa ,osea que podamos entrar desde el navegador con la IP del Droplet, y también ver en qué puerto se están escuchando las conexiones. Por lo que debemos de ir a nuestro navegador web (si trabajamos en Oracle VM , minimizar e ir a nuestro sistema operativo host . De otra forma ir a otro dispositivo dentro de la misma red para consultar) y copiar la IP de nuestro Droplet en la barra del navegador.

Si nuestra instalación de Apache fue exitosa , debemos ver la página default que proporciona Apache, como la siguiente:



Algunos errores de conectividad pueden surgir ,asegurarse de la estabilidad de la red.Un error común es el de **broken pipe** este error es por estar un tiempo ausente de actividad o la conectividad es inestable. La solución es volver a loguearse ,por el momento como root con **ssh**

3.AÑADIENDO UN FIREWALL

Un firewall controla quienes entran a nuestro servidor , en este caso a nuestra página default de apache . DigitalOcean ofrece servicio de firewall para Droplets , así que usaremos ese servicio.

En la página principal de nuestra cuenta de DigitalOcean , en la barra lateral izquierda , veremos la opción de networking.



Dentro de la opción vamos a Create Firewall.

Create Firewall

Una vez dentro debemos de asignar un nombre al firewall y lo **único** que debemos modificar será **Inbound Rules** .

Create Firewall

Name

Nombrefirewall ✓

En las opciones de Inbound Rules , modificaremos la default por ALL TCP y agregaremos una nueva regla ALL UDP .

Inbound Rules

Set the Firewall rules for incoming traffic. Only the specified ports will accept inbound connections. All other traffic will be dropped.

Type	Protocol	Port Range	Sources	
All TCP	TCP	All ports	Add a source	Delete
All UDP	UDP	All ports	Add a source	Delete
New rule				

En el espacio de Sources debemos de colocar nuestra IP externa de la red en la que estamos trabajando, que anotamos en los pasos anteriores. De no haberla anotado podemos ir a cualquier sitio web de consulta de IP para saber cual es nuestra IP. Una vez llenos y agregados. Bajamos a Apply to droplets y seleccionamos el droplet que va a tener ese firewall. El botón de **create firewall** se tornará **verde** y daremos click en este para finalizar.

Apply to Droplets

Select Droplets to apply your Firewall rules to.

- Droplets
-  serv-pw 190300624... / NYC1

Create Firewall

Lo que acabamos de realizar es para asegurarnos de que únicamente se pueda acceder desde nuestra red en lo que preparamos el server con el contenido para desplegar públicamente.

4. SEGURIDAD DE SSH

Mantener segura nuestra página web es muy importante , ya que al estar en la nube cualquiera puede entrar , y no queremos que nuestros datos sean robados . Las siguientes configuraciones nos ayudarán a mantener seguro el servidor.

Empezamos por loguearnos en nuestro Droplet como `root@TU_IP`

Crearemos un usuario sudo (con permisos de administrador) para evitar usar el root en nuestro server , y limitaremos a root:

```
adduser NOMBRE_DE_NUEVO_USUARIO
```

Completamos los datos que nos solicita adduser (anotar nuestra contraseña correctamente en papel o dispositivo). Ejecutamos :

```
tail /etc/passwd
```

para verificar que se ha creado el usuario no-root. Nos desconectamos del droplet y nos conectaremos a este con el nuevo usuario para confirmar que se ha creado.

```
ssh TU_USUARIO@TU_IP
```

Ahora entramos al droplet con `ssh root@TU_IP` para agregar nuestro usuario a la lista de usuarios sudo con el siguiente comando:

```
usermod -aG sudo TU_USUARIO
```

Para verificar que se ha agregado a la lista de usuarios sudo, deberá aparecer el nombre de nuestro usuario junto con sudo:

```
groups TU_USUARIO
```

Nos desconectamos del droplet y volvemos a entrar con nuestro usuario

```
ssh TU_USUARIO@TU_IP
```

Abriremos el archivo de configuración de ssh con un editor de texto , en este caso Vim:

```
sudo vim /etc/ssh/sshd config
```

Debemos ser cuidadosos de no cambiar más que lo indicado y escribirlo correctamente ya que es case-sensitive.

Al abrir el documento debemos ir a **PermitRootLogin** y cambiarlo de **yes** a **no**.

```
#LoginGraceTime 2m
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
```

Agregar una línea para permitir que los únicos que podamos acceder a sudo seamos nosotros ,con nuestro usuario.Con : **AllowUsers TU USUARIO**

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

AllowUsers karenadmin

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
```

Ejecutaremos **sudo systemctl restart ssh**

Nos desconectamos de nuestro droplet y generamos una llave ssh en nuestro servidor ubuntu con ssh-keygen dejando las opciones por default , únicamente introducir la frase contraseña . Al finalizar anotar en papel/dispositivo alterno , la dirección donde se guardó nuestra llave pública.

Ejecutar :

```
ssh-copy-id -i ~/.ssh/id_rsa.pub TU USUARIO@TU IP
```

Esto hará que se relacionen las llaves ssh.Al conectarnos a nuestro droplet con nuestro usuario, ya no nos pedirá contraseña , únicamente la frase contraseña. Nos desconectamos y volvemos a entrar al droplet.Volvemos a entrar al archivo de configuración de ssh :

```
sudo vim /etc/ssh/sshd config
```

Y cambiamos **PasswordAuthentication** de **yes** a **no**.Guardamos el documento.

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

Ejecutaremos `sudo systemctl restart ssh`

Nos desconectamos y volvemos a conectarnos al droplet.

Ahora ejecutamos el siguiente comando:

```
sudo apt update && sudo apt dist-upgrade
```

Por si tenemos una actualización de los paquetes. Damos Y a todo y en caso de salir una pantalla rosa seleccionar `install the package maintainers version`. Despues debemos reiniciar el server con `sudo reboot`. Nos sacará de la sesión en el droplet y debemos esperar un tiempo en lo que se reinicia el droplet para volver a conectarnos.

4. AÑADIENDO UN DNS (DOMINIO)

El DNS o sistema de nombres de dominio , nos facilita el recordar los sitios web por IP de todo internet. El DNS al ser ligado al Droplet se esparcirá por el internet para que esté accesible en cualquier lugar del mundo.

Para crear un dominio iremos a nuestra cuenta de Hover y compraremos el dominio que más nos guste y podamos pagar , ya que hay nombre de dominios que son muy populares e incluso están en subasta (mejor oferta). Al haber comprado nuestro dominio , iremos a manage Domains y agregaremos un récord en Add A Record , que nos permitirá hacer saber a nuestro droplet de nuestro dominio.

The screenshot shows the Hover DNS management interface. At the top, there's a navigation bar with links for Domains, Emails, Nameservers, Forwards, and Settings. On the right, there are Help and Sign Out options. Below the navigation, the domain 'ksbt-progweb.space' is selected. The main area shows a table of DNS records:

Type	Host	Value	TTL	Added By
A	*	64.98.145.30	15 Minutes	Hover

Below the table, there's a 'Bulk edit: Select' dropdown and a search bar labeled 'Filter your records'. A green 'ADD A RECORD' button is visible at the bottom left.

Asignamos el tipo A ,le damos un nombre al hostname y agregamos el récord.

This is a screenshot of the 'Add A Record' dialog box. It has fields for TYPE (set to A), HOSTNAME (set to 'cloud'), IP ADDRESS (set to 'IP_DROPLET'), and TTL (set to 'Default (15 Minutes)'). There are 'CANCEL' and 'ADD RECORD' buttons at the bottom.

The screenshot shows the Hover DNS management interface again. The domain 'ksbt-progweb.space' is selected. The main area shows a table of DNS records:

Type	Host	Value	TTL	Added By
A	*	64.98.145.30	15 Minutes	Hover
A	@	64.98.145.30	15 Minutes	Hover
MX	@	10 mx.hover.com.cust.hostedemail.com	15 Minutes	Hover
A	cloud	167.99.144.238	15 Minutes	Hover
CNAME	mail	mail.hover.com.cust.hostedemail.com	15 Minutes	Hover

Below the table, there's a 'Bulk edit: Select' dropdown and a search bar labeled 'Filter your records'. A note at the top says 'This domain is using third-party nameservers. DNS records added here won't have an effect.'

Ahora vamos a nuestra cuenta de DigitalOcean y agregamos en Dominio dentro de la opción de Networking a nuestro DNS , al agregarlo debemos crear un récord para el record que creamos en Hover , por lo que iremos a **Create new record** donde colocaremos el nombre del récord que creamos en hover en **HOSTNAME** , después seleccionamos nuestro droplet o colocamos la IP del mismo en **WILL DIRECT TO** y dejamos el valor default de **TTL**, y creamos. Nos debe de quedar algo parecido la captura :

Type	Hostname	Value	TTL (seconds)	More
A	cloud.ksbt-progweb.space	directs to 167.99.44.238	3600	More
NS	ksbt-progweb.space	directs to ns3.digitalocean.com.	1800	More
NS	ksbt-progweb.space	directs to ns1.digitalocean.com.	1800	More
NS	ksbt-progweb.space	directs to ns2.digitalocean.com.	1800	More

Esto hace que DigitalOcean sepa que el dominio está ligado a la droplet y comience a esparcir esa información sobre el DNS por el internet. Este proceso puede tomar minutos u horas , por lo que se recomienda esperar al menos una hora o visitar <https://www.whatsmydns.net/> y colocar en su barra de búsqueda ,nuestro **subdominio.dominio.término** ,que acabamos de crear, si por lo menos en nuestro país está con una palomita verde , eso quiere decir que el internet de nuestro país ya sabe de la existencia de nuestro dominio.

Ya que hayamos esperado un tiempo para volver a conectarnos a nuestro Droplet , iremos a nuestro server de ubuntu y consultaremos con un comando si nuestro dominio ya está en la red :

```
nslookup SUBDOMINIO.DOMINIO.TERMINO
```

Podremos ver que el **address** que muestra es el de nuestro droplet , por lo que ya está en Internet.Ahora ligaremos ese dominio al ssh para que podamos acceder usando nuestro dominio, usando este comando:

```
ssh TU_USUARIO@SUBDOMINIO.DOMINIO.TERMINO
```

5. INSTALAR UNA BASE DE DATOS

Ejecutamos en nuestra terminal:

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

Verificamos que esté activa y corriendo:

```
sudo systemctl status mariadb -> active and running
```

Ahora utilizaremos un comando del tipo mysql , para asegurar nuestra base de datos:

```
sudo mysql_secure_installation
```

responder a las preguntas , añadir contraseña y las siguientes opciones que no sean la anterior debemos de dejarlas como default.

ahora estamos como root :

```
sudo mysql
```

ahora estamos dentro del shell de mariadb

creamos la base datos para instalar nuestro manager de base de datos en nuestro subdominio:

```
CREATE DATABASE nombre_de_tu_base_de_datos;
```

ahora la llegaremos a nuestro subdominio , con esta syntax:

```
GRANT ALL PRIVILEGES ON base_de_datos.* TO "tu_subdominio"@"localhost"  
IDENTIFIED BY "nueva_contraseña";
```

Seguido ejecutamos :

```
FLUSH PRIVILEGES;
```

Para salir de mariadb ctrl+c.

6. CONFIGURACIÓN DE APACHE

Como ya hemos instalado apache2 en nuestro server del droplet

Ahora vamos a instalar php para poder visualizar en nuestro subdominio un cliente administrador para nuestra base de datos

Debemos introducir el siguiente comando , que instalará php y sus módulos / drivers que se necesitan:

```
sudo apt install php libapache2-mod-php php7.4-common  
php7.4-mbstring php7.4-xmlrpc php7.4-soap php php-cli php-fpm  
php-json php-common php-mysql php-zip php-gd php-mbstring  
php-curl php-xml php-pear php-bcmath php-imagick php7.4-ldap  
php-redis php-apcu
```

Al finalizar la instalación reiniciar apache2:

```
sudo systemctl restart apache2
```

Editaremos un archivo html para hacer php compatible con nuestro administrador de base de datos (en este caso instalaremos Nextcloud), ejecutamos:

```
sudo vim /etc/php/7.4/apache2/php.ini
```

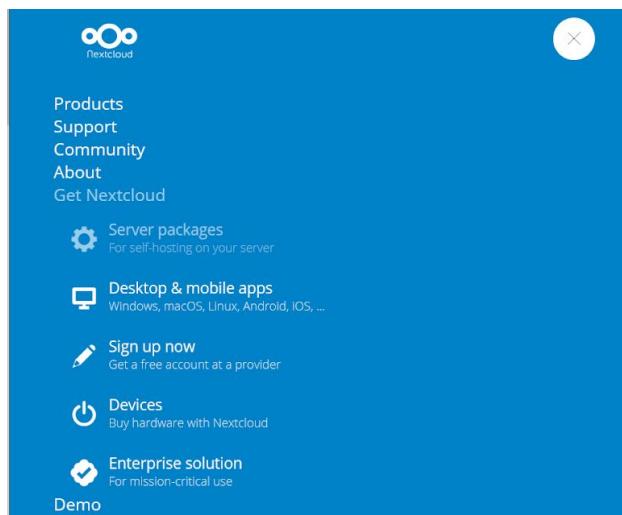
Habilitaremos (quitando el símbolo ; del inicio de línea de cada valor) estos valores , cambiando los valores default por los siguientes:

```
opcache.enable=1  
opcache.enable_cli=1  
opcache.interned_strings_buffer=8  
opcache.max_accelerated_files=1000  
opcache.memory_consumption=128  
opcache.save_comments=1  
opcache.revalidate_freq=1
```

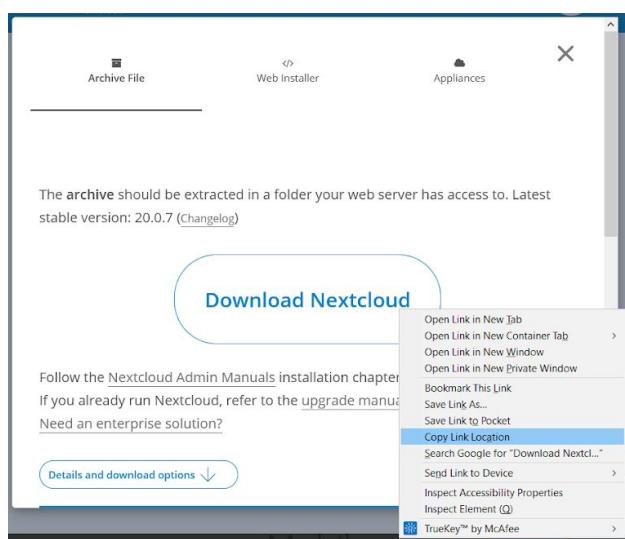
7. INSTALACIÓN DE ADMINISTRADOR DE BASE DE DATOS “NEXTCLOUD”

Nextcloud es un servicio en la nube para almacenar datos , pero también ofrece soluciones para servidores , una de ellas y la más importante es la de visualización.

Para instalarlo necesitaremos la url de descarga de nextcloud para servidores . Iremos a la pagina principal de nextcloud.com , vamos al icono desplegable -> get nextcloud -> server packages



Damos click derecho sobre el botón de Download Next Cloud para copiar la locación del link:



Debemos obtener el siguiente link:

```
https://download.nextcloud.com/server/releases/nextcloud-20.0.7.zip
```

Ahora iniciamos sesión en nuestro Droplet y en la terminal ejecutamos :

```
wget https://download.nextcloud.com/server/releases/nextcloud-20.0.7.zip
```

Lo que iniciará la descarga del zip de Next Cloud for Servers .

Verificamos la descarga con `ls -h`

Instalaremos la utilidad de “unzip” para extraer nuestro archivo zip :

```
sudo apt install unzip
```

Extraemos el archivo zip de Nextcloud:

```
sudo unzip nextcloud-20.0.7.zip
```

Esto creará un directorio de `nextcloud` , lo relacionaremos a Apache para que tenga control de Nextcloud:

```
sudo chown www-data:www-data -R nextcloud
```

`www-data` es el usuario que Apache utiliza , por lo que ya le hemos dado los permisos a Apache. Verificamos con `ls -l` que el usuario de apache tenga los permisos de la carpeta.

En este punto moveremos esta carpeta al lugar donde Apache hace uso de directorios y archivos:

```
sudo mv nextcloud /var/www/html
```

Verificamos que se haya movido correctamente con el siguiente comando:

```
ls -l /var/www/html
```

Observaremos que en esa carpeta está la pagina default de apache , pero aun **no** debemos desecharla.

Crearemos un archivo de configuración para Apache y que sepa de la existencia de next cloud y de cómo tratar el archivo :

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

En ese archivo debemos anotar la siguiente información:

```
<VirtualHost *:>
    DocumentRoot /var/www/html/nextcloud/
    ServerName subdomain.tu_dominio.termino <- SÓLO DEBEMOS  
CAMBIAR ESTO CON  
NUESTRA  
INFORMACIÓN

    <Directory /var/www/html/nextcloud/>
        Options +FollowSymlinks
        AllowOverride All
        Require all granted
        <IfModule mod_dav.c>
            Dav off
        </IfModule>
        Set Env HOME /var/www/nextcloud
        SetEnv HTTP_HOME /var/www/html/nextcloud
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Guardamos el archivo,salimos del editor y lo habilitaremos con el comando de Apache a2ensite

```
sudo a2ensite nextcloud.conf
```

Reiniciamos apache para que se actualicen todos los cambios realizados :

```
sudo systemctl restart apache
```

Verificamos que esté activo y corriendo:

```
sudo systemctl status apache2
```

Ahora deshabilitamos la configuración de la página default de Apache con otro de sus comandos:

```
sudo a2dissite 000-default
```

Ahora nos aseguraremos que algunos de los módulos que necesita nextcloud estén activados :

```
sudo a2enmod rewrite headers env dir mime
```

Volvemos a reiniciar apache y en nuestro navegador web verificaremos que la página de default de apache ya no este , en vez de eso estará nextcloud si realizamos correctamente las indicaciones anteriores.

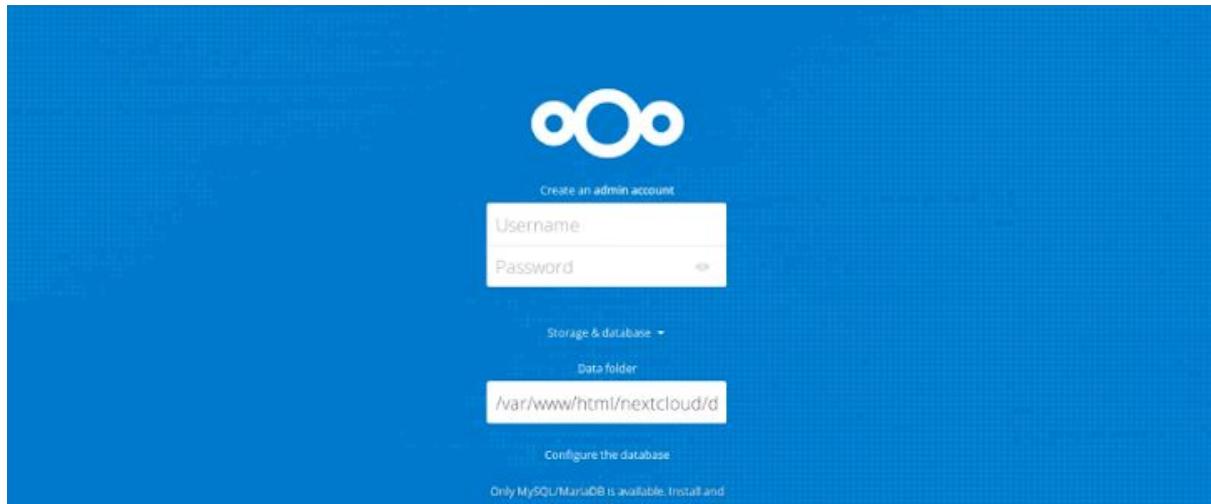
En caso de salir errores deberás verificar si colocaste bien los valores en el archivo **php.ini** o verificar si faltaron instalar módulos de php, esto deberá de corregir el problema. Lo siguiente es crear nuestro usuario de administrador en la pagina podemos visualizar de nextcloud en nuestro subdominio.

IMPORTANTE

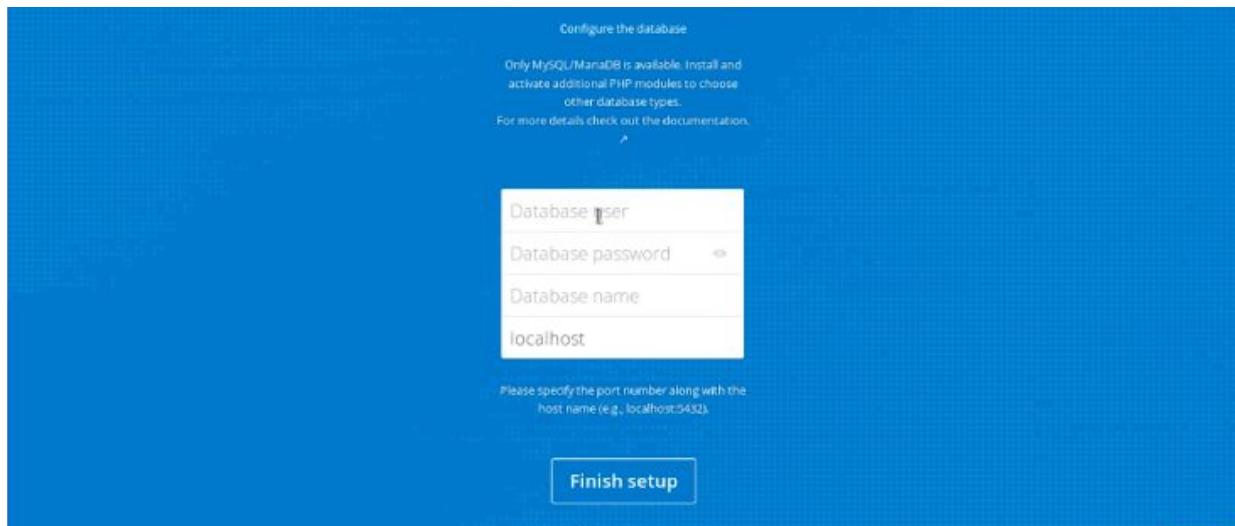
LOS DATOS QUE PROPORCIONES LOS DEBERÁS DE GUARDAR Y RECORDAR , ESCRIBIR BIEN Y SEGUIR CADA PASO QUE SE INDIQUE, DE LO CONTRARIO PUEDES NO VOLVER A ENTRAR A TU SERVIDOR.

7.1 CREAR UN USUARIO ADMINISTRADOR EN NEXTCLOUD

En nuestro subdominio deberá aparecer la página de nextcloud de esta forma :



Ahí crearemos un usuario nuevo de tipo administrador , los datos que nos pide no son los que hemos creado en pasos anteriores (ÚNICAMENTE EN LA PARTE DEL USUARIO Y CONTRASEÑA). En Data Folder dejaremos el valor default , en esa ruta de directorio es donde se guardará la información que se introduzca desde el navegador.



Este campo se deberá de llenar con la información que asignamos en el momento que creamos nuestra base de datos.

Database user : es el usuario que asignamos en mariadb

“**usuario**”@“localhost”

^

Database user

Database Password: es la contraseña que asignamos en mariadb

IDENTIFIED BY “**contraseña**”;

^

Database Password

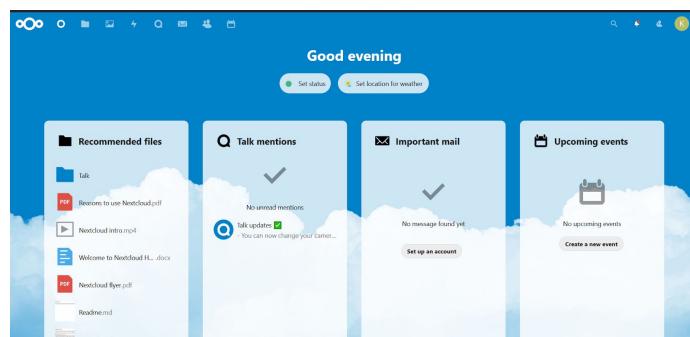
Database name: es el nombre que asignamos en mariadb

GRANT ALL PRIVILEGES ON nombre_de_la_base_de_datos.* TO

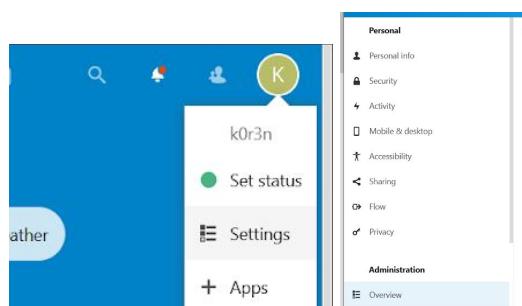
^

Database Name

Dejaremos localhost como default.Finalizamos haciendo click en **Finish Setup**. Tendremos una pantalla como la siguiente:



Nuestra instalación ha sido exitosa , podemos hacer uso de todas las aplicaciones que vienen con nextcloud para hacer más agradable para nuestros usuarios usar esta nube para sus archivos.ahora iremos a settings y luego a overview para ver nuestras notificaciones de alerta sobre la instalación:



Aunque la instalación fue correcta , puede que algunos módulos hagan falta ,configuraciones de php.ini o drivers para mejorar la experiencia con nextcloud. Lo cual con la experiencia que hemos aprendido hasta ahora lo podremos solucionar.Un ejemplo de lo que podríamos observar :

The screenshot shows a section titled "Security & setup warnings" with a subtitle "It's important for the security and performance of your instance that everything is configured correctly. To help you with that we are doing some automatic checks. Please see the linked documentation for more information." Below this, there is a list of errors and tips:

- There are some warnings regarding your setup.
 - The "Strict-Transport-Security" HTTP header is not set to at least "15552000" seconds. For enhanced security, it is recommended to enable HSTS as described in the [security tips](#).
 - No memory cache has been configured. To enhance performance, please configure a memcache, if available. Further information can be found in the [documentation](#).
 - The database is missing some indexes. Due to the fact that adding indexes on big tables could take some time they were not added automatically. By running "occ db:add-missing-indexes" those missing indexes could be added manually while the instance keeps running. Once the indexes are added queries to those tables are usually much faster.
 - Missing index "cards_abidun" in table "oc_cards".

Please double check the [installation guides](#) and check for any errors or warnings in the [log](#).
Check the security of your Nextcloud over our [security scan](#).

Nextcloud nos ofrece este análisis de errores del setup y como extra guías referentes al problema , por lo que será muy sencillo corregir los errores.

8. HTTPS CON LET'S ENCRYPT

Let's encrypt es un servicio gratuito para dar un certificado de seguridad SSL a nuestro dominio.

Si tuvimos algún error de acceso por el firewall después de instalar nextcloud, en este paso podremos solucionar eso. De lo contrario , podemos usar la configuración de `ufw` para abrir puertos.

Primero verificaremos que tengamos el archivo de configuración con ,por lo menos el nombre de nuestro subdominio, en el :

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

```
-----  
ServerName your_domain  
ServerAlias www.your_domain  
-----
```

Salimos de nuestro editor y ejecutamos este comando , el cual nos debe de arrojar un Syntax OK:

```
sudo apache2ctl configtest
```

Reiniciamos :

```
sudo systemctl reload apache2
```

Ahora habilitaremos el http a través de nuestro Firewall. VERIFICAR QUE NUESTRA CONEXIÓN SEA ESTABLE PARA LOS SIGUIENTES PASOS.

Ejecutamos :

```
sudo ufw status
```

Nos debe de arrojar que está activo , de lo contrario activarlo con `sudo ufw enable` , nos aparecerá un mensaje sobre que las conexiones ssh se pueden perder , damos a `y` (si).

IMPORTANTE NO SALIR (O DESCONECTARNOS) DE NUESTRO SERVER AL EJECUTAR LO ANTERIOR , DE LO CONTRARIO NO PODREMOS INGRESAR DE NUEVO A NUESTRO SERVER .

Para asegurarnos de que al haber quitado nuestras conexiones ssh podamos volver a salir y entrar de nuestro server , ejecutaremos cualquiera de los siguiente comandos :

```
sudo ufw allow ssh
```

```
sudo ufw allow 22/tcp
```

Ya que exista la regla ufw de permitir comunicaciones del tipo ssh o de permitir comunicaciones por el puerto 22/tcp. Verificamos si están correctamente permitidas con `sudo ufw status` las conexiones por ssh o 22/tcp y Apache .

Ahora añadimos las reglas de permisos completos para Apache ejecutando estos dos comandos (uno a la vez):

```
sudo ufw allow 'Apache Full'
```

```
sudo ufw delete allow 'Apache'
```

Hacemos un `sudo ufw status` y debemos tener a Apache Full como regla .

Iremos a nuestra terminal en nuestro droplet e instalaremos Let's encrypt :

```
sudo apt install certbot python3-certbot-apache
```

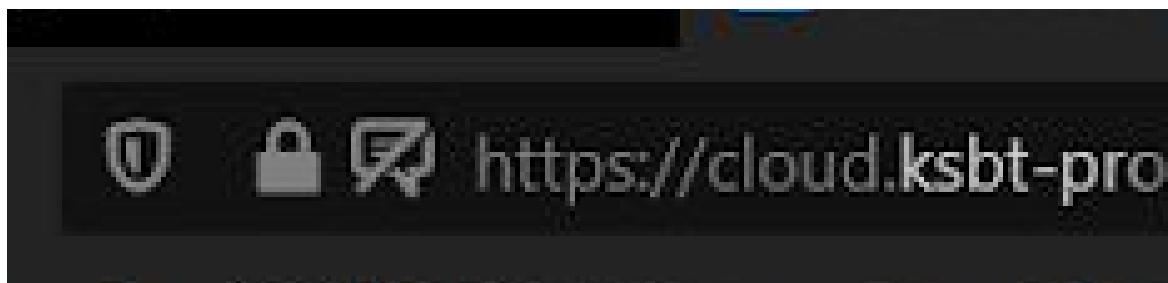
Ahora ejecutamos cert bot , que es un bot de encriptación de Let's encrypt:

```
sudo certbot --apache
```

Nos hará una serie de preguntas , podremos responder libremente , ya que son opciones de privacidad de datos personales. Al finalizar las preguntas daremos a continuar introduciendo los valores permitidos que nos indica y finalmente tendremos un certificado de seguridad para nuestro sitio web. Algo como la siguiente imagen :

```
-----  
Congratulations! You have successfully enabled https://your_domain and  
https://www.your_domain  
  
You should test your configuration at:  
https://www.ssllabs.com/ssltest/analyze.html?d=your_domain  
https://www.ssllabs.com/ssltest/analyze.html?d=www.your_domain  
-----  
  
IMPORTANT NOTES:  
- Congratulations! Your certificate and chain have been saved at:  
/etc/letsencrypt/live/your_domain/fullchain.pem  
Your key file has been saved at:  
/etc/letsencrypt/live/your_domain/privkey.pem  
Your cert will expire on 2020-07-27. To obtain a new or tweaked  
version of this certificate in the future, simply run certbot again  
with the "certonly" option. To non-interactively renew *all* of  
your certificates, run "certbot renew"  
- Your account credentials have been saved in your Certbot  
configuration directory at /etc/letsencrypt. You should make a  
secure backup of this folder now. This configuration directory will  
also contain certificates and private keys obtained by Certbot so  
making regular backups of this folder is ideal.  
- If you like Certbot, please consider supporting our work by:  
  
Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate  
Donating to EFF: https://eff.org/donate-le
```

Al abrir nuestro navegador , veremos que ya no somos un sitio no seguro :



Ahora tenemos un subdominio con https , lo que dará más confianza a nuestros usuarios. Solo recordemos que estamos trabajando en modo seguro , lo que significa que nuestro sitio no puede ser visualizado por otras personas mas que por nuestra IP(s) externa que configuramos en el Firewall. Si nuestro sitio está finalmente listo y queremos que todo el mundo lo pueda ver , tendremos que asignar una nueva regla en `ufw` , que sera abrir el puerto 80 o cualquier otro puerto que necesites con esta sintaxis `sudo ufw allow <port>/<optional: protocol>`:

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

Damos terminada esta guía para la instalación rápida de un servidor virtual con Apache y visualizar algo diferente a la página default del mismo.

FUENTES DE CONSULTA PARA REALIZAR ESTA DOCUMENTACIÓN:

<https://eltallerdelbit.com/actualizar-paquetes-ubuntu/>

<https://www.digitalocean.com/>

<https://computingforgeeks.com/how-to-install-php-on-ubuntu/>