

## Servidor DNS en Ubuntu

### ÍNDICE DE CONTENIDO

1) INSTALACIÓN.....	2
2) SERVIDOR DNS CONFIGURADO COMO CACHÉ O REENVIADOR (FORWARDER).....	5
2.A) Comando cliente DNS dig.....	7
2.B) Comando cliente DNS ping.....	11
2.C) Comando cliente DNS host.....	11
2.D) Comando cliente DNS nslookup.....	11
3) SERVIDOR DNS PRIMARIO EN UBUNTU.....	12
4) CONFIGURAR UN DOMINIO PARA QUE APUNTE A UN SERVIDOR DE NOMBRES DE UN HOSTING.....	16

#### **Nota:**

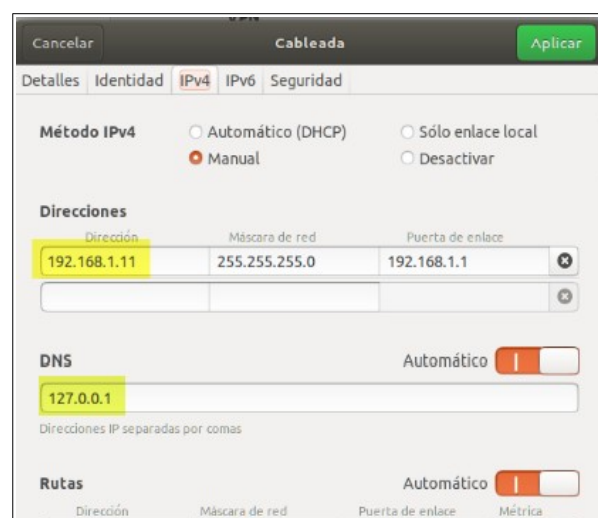
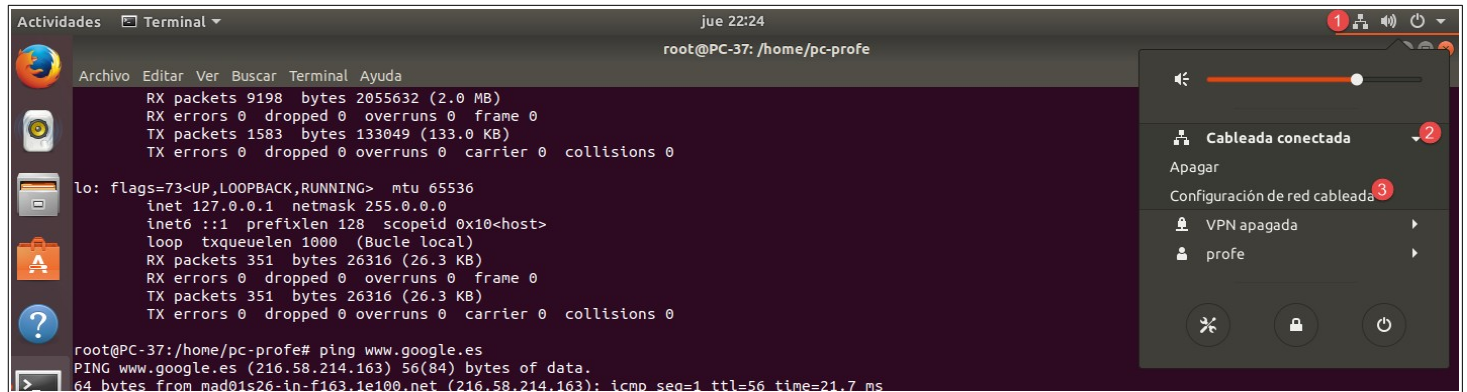
**Los archivos de configuración se pueden editar con programas como nano, gnome-text-editor o gedit (instalable con `sudo apt install gedit`)**

## 1) INSTALACIÓN

En modo root (en Actividades buscamos **Terminal**, lo ejecutamos y luego ponemos **sudo su** y la contraseña)

```
apt-get install bind9 bind9utils bind9-doc
```

Después cambiamos las propiedades de red de la tarjeta de red cableada, según vemos en la figuras siguientes:



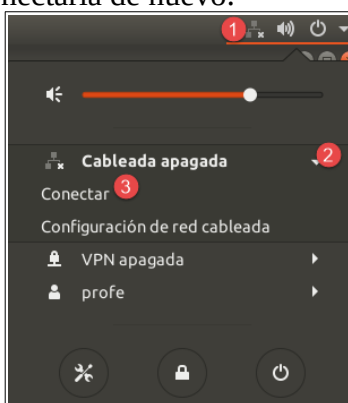
La dirección IP ha de ser estática (para tener siempre localizado al servidor). Observa que solamente hay un servidor DNS: el 127.0.0.1<sup>1</sup>, que es NUESTRO PROPIO ORDENADOR (con el que estamos trabajando), que vamos a convertir en un servidor DNS.

**MUY IMPORTANTE:** para estos ejercicios se supone que estamos conectados a la red local de nuestro ciclo, cableada (nada de Andared inalámbrica o cableada)

**Importante:** en Ubuntu no hace falta reiniciar el equipo para cambiar la configuración de la tarjeta de red. Basta con



para desactivar la tarjeta de red, y luego conectarla de nuevo:



### **AVISO MUY IMPORTANTE:**

Desde Ubuntu 18.04 se incluye un sistema de resolución de nombres primitivo (DNS) llamado systemd-resolved que está activo y que funciona en la dirección 127.0.0.53

Hay que deshabilitarlo para poder usar nuestro servidor DNS profesional recién instalado (bind9) de forma satisfactoria. Para ello, desde una terminal hacemos 5 pasos:

1) Nos hacemos superusuarios:

```
sudo su
```

2) Deshabilitamos el servicio systemd-resolved y lo paramos:

```
systemctl disable systemd-resolved.service  
service systemd-resolved stop
```

1 localhost es una tarjeta de red virtual que tiene cada ordenador, suele ponerse como 127.0.0.1, aunque son válidas todas las direcciones desde 127.0.0.1 a 127.255.255.254, esto es, 127.0.0.0/8

3) Editamos el archivo `/etc/NetworkManager/NetworkManager.conf`

```
sudo nano /etc/NetworkManager/NetworkManager.conf
```

```
/etc/NetworkManager/NetworkManager.conf
[main]
plugins=ifupdown,keyfile
dns=default
[ifupdown]
managed=false

[device]
wifi.scan-rand-mac-address=no
```

y añadimos en la sección `[main]` la línea

```
dns=default
```

4) Borramos el archivo `/etc/resolv.conf`

```
rm /etc/resolv.conf
```

Y ya está.

Un servidor DNS puede ser configurado de 3 formas:

- servidor DNS caché o reenviador (forwarder), que solo dispondrá de una memoria caché para almacenar las traducciones de nombres de dominio a IP que vaya conociendo. Si una IP no está en su caché, dispondrá de servidores DNS reales para consultarlos.

- servidor DNS primario, con su propio espacio de zonas, esto es, su base de datos con las traducciones de nombres de dominios a sus IP correspondientes.

- servidor DNS secundario, que almacena una copia de una base de datos de un servidor primario, del cual depende.

En las próximas preguntas de este documento se explica cómo configurar un servidor DNS de cada una de las formas anteriores.

## 2) SERVIDOR DNS CONFIGURADO COMO CACHÉ O REENVIADOR (FORWARDER)

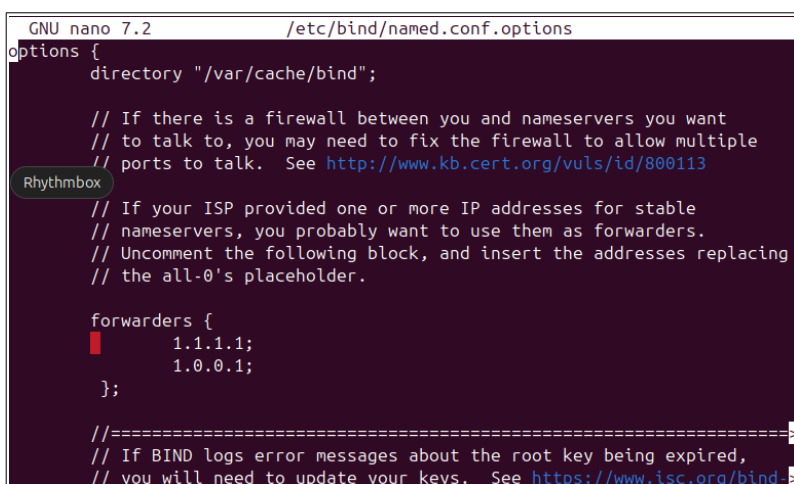
Es el más fácil de configurar. Para ello, hay que editar el archivo `/etc/bind/named.conf.options`<sup>2</sup>, **quitar los comentarios // de cada línea desde la palabra forwarders hasta };**

y escribir:

```
forwarders {  
    1.1.1.1;  
    1.0.0.1;  
};
```

Debe quedar así:

Los servidores DNS 1.1.1.1 y 1.0.0.1 pertenecen a la compañía Cloudflare, que a medianoche todos los días borra los accesos que hayan tenido para no usar esos datos con propósito de ganar dinero. Los servidores gratuitos de Google 8.8.8.8 y 8.8.4.4 no lo hacen.



```
GNU nano 7.2 /etc/bind/named.conf.options  
options {  
    directory "/var/cache/bind";  
  
    // If there is a firewall between you and nameservers you want  
    // to talk to, you may need to fix the firewall to allow multiple  
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113  
  
    // If your ISP provided one or more IP addresses for stable  
    // nameservers, you probably want to use them as forwarders.  
    // Uncomment the following block, and insert the addresses replacing  
    // the all-0's placeholder.  
  
    forwarders {  
        1.1.1.1;  
        1.0.0.1;  
    };  
  
    //=====  
    // If BIND logs error messages about the root key being expired,  
    // you will need to update your keys.  See https://www.isc.org/bind-
```

Cuando se haga una consulta al servidor DNS que hemos instalado, la mirará en su caché; si está, la devuelve como resultado, y si no, la pide al primero de los DNS que se ha puesto en la sección forwarders (si no responde se acudirá al segundo escrito), que darán el resultado y el servidor DNS local lo guardará en su memoria caché para tenerla disponible cuando alguien pida de nuevo esa IP.

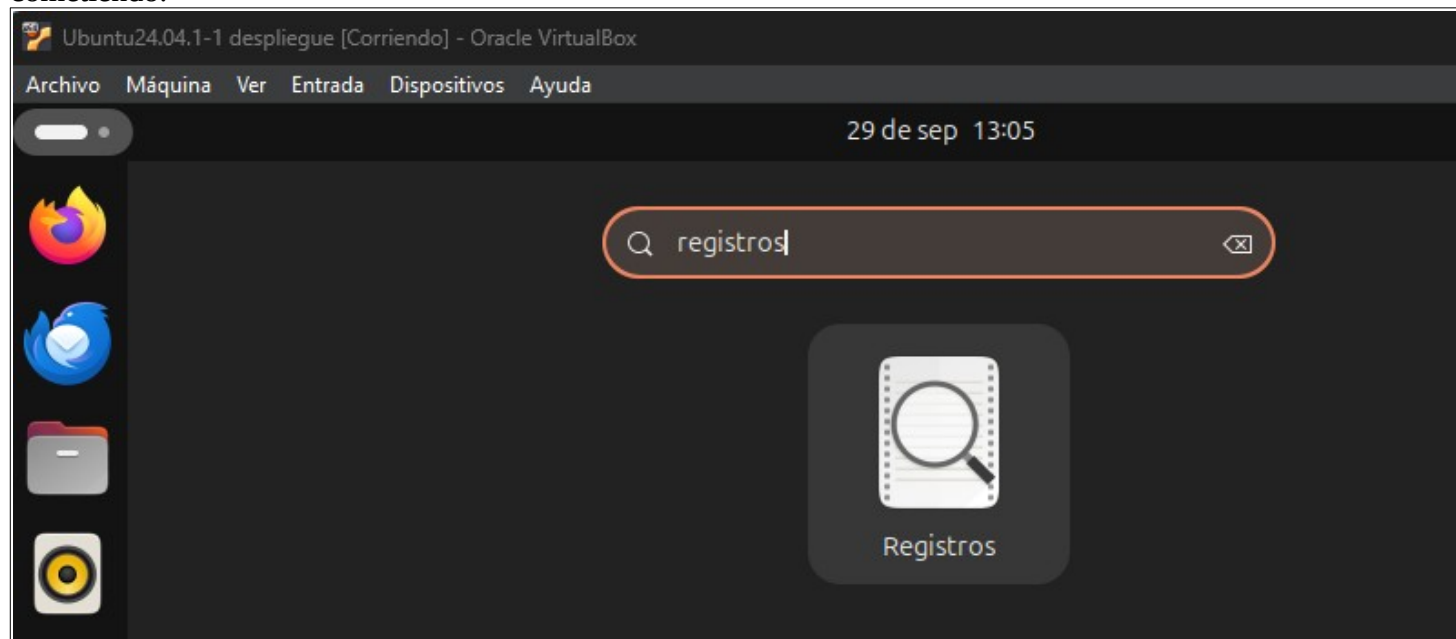
Luego se guarda y se reinicia el servidor DNS (como superusuario, en una terminal teclear **service bind9 restart**) para que lea su nueva configuración.

Los comandos más usuales para usar con el servidor son: **service bind9**

**start**  
**stop**  
**restart**  
**status**

<sup>2</sup> Se recomienda, como siempre, hacer una copia de seguridad del fichero ANTES de modificarlo, denominándolo, por ejemplo, `named.conf.options.original`

Es interesante conocer el programa Registros, que permitirá encontrar errores que hayamos podido ir cometiendo.



Registros			12:52 – 13:05			
Importante	Sistema	index 1 is out of range for type 'RTGCPHYS64 [1]'				12:55
Todo	Sistema	UBSAN: array-index-out-of-bounds in /tmp/vbox.0/VBoxGuestR0...				
Aplicaciones	Seguridad	Failed to start app-gnome-user\x2ddirs\x2dupdate\x2dgtk-25...	3			12:52
Sistema	Otros	gkr-pam: unable to locate daemon control file				
Seguridad	Otros	Failed to resolve interface "NetworkManager": No existe el ...				
Hardware	Otros	chroot.c: open() failed: No such file or directory				
	Otros	vboxuser: /etc/udev/rules.d/60-vboxadd.rules:2 Only netwo...	2			
	Hardware	vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a sup...	3			
	Sistema	Invalid DMI field header.				
	Sistema	RETbleed: WARNING: Spectre v2 mitigation leaves CPU vulnera...				

### IMPORTANTE:

Si en algún momento no funciona el servidor DNS y, tras múltiples intentos, sigue sin actuar debidamente, lo desinstalas y lo instalas de nuevo, así: **apt-get remove --purge bind9**

Una vez desinstalado, lo instalamos de nuevo, **como vimos al principio de este tutorial**.

Para probar el funcionamiento de nuestro servidor DNS se pueden usar comandos CLIENTES DNS, como son:

dig  
ping  
host

## 2.A) Comando cliente DNS dig

EJEMPLO 0 : dig dominio devuelve la IP de dicho dominio (búsqueda directa)

```
pc-profe@pcv-01:~$ dig www.isidrodearceneguiycarmona.es

;<<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> www.isidrodearceneguiycarmona.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52138
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: f05ad3a0890ca4e601000000636cac6cf74918976630a0e7 (good)
;; QUESTION SECTION:
;www.isidrodearceneguiycarmona.es. IN A

;; ANSWER SECTION:
www.isidrodearceneguiycarmona.es. 3600 IN A      217.160.230.79

;; Query time: 99 msec
;; SERVER: ::1#53(::1) (UDP)
;; WHEN: Thu Nov 10 08:46:52 CET 2022
;; MSG SIZE rcvd: 105

pc-profe@pcv-01:~$
```

Observa:

- que hay respuesta (ANSWER:1) a nuestra consulta
- que la consulta ha tardado en hacerse 99 milisegundos
- que hay un número en una elipse roja (3600)
- que la consulta ha sido realizada por el servidor DNS ::1#53, que es nuestro ordenador (ipv4 127.0.0.1 puerto 53 udp)

El número en una elipse roja es el parámetro TTL (Time To Live, Tiempo de Vida), que es el tiempo en segundos que estará ese dato alojado en la caché del servidor DNS. Si este servidor recibe una petición en ese tiempo para averiguar la IP de `www.isidrodearceneguiycarmona.es`, tomará esa IP de su caché. En efecto, si repetimos el comando:

```
pc-profe@pcv-01:~$ dig www.isidrodearceneguiycarmona.es

;<<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> www.isidrodearceneguiycarmona.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57657
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a4dda4b5f1f4552b01000000636cad34def90508d08f41e0 (good)
;; QUESTION SECTION:
;www.isidrodearceneguiycarmona.es. IN A

;; ANSWER SECTION:
www.isidrodearceneguiycarmona.es. 3400 IN A      217.160.230.79

;; Query time: 0 msec
;; SERVER: ::1#53(::1) (UDP)
;; WHEN: Thu Nov 10 08:50:12 CET 2022
;; MSG SIZE rcvd: 105

pc-profe@pcv-01:~$
```

Podemos comprobar:

- que el número TTL ha bajado (es una cuenta atrás). Esto quiere decir que queda ese tiempo de esa correspondencia nombre de dominio (`www.isidrodearceneguiycarmona.es`) IP (217.160.230.79) dentro de la cache, pasado ese tiempo (el contador pasa a 0) se borrará de la caché.



- que el tiempo que ha costado realizar la consulta (query) ha sido de 0 milisegundos, ya que acceder a la caché es muy rápido.

EJEMPLO 1: si ponemos

```
dig isidrodearceneguicarmona.es ns
```

nos aparecerá el servidor (o varios servidores) DNS responsable de almacenar la traducción de ese dominio a su correspondiente dirección IP:

```
pc-profe@pcv-01:~$ dig isidrodearceneguicarmona.es ns
;; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> isidrodearceneguicarmona.es ns
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 15277
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: f51678d94fb67f3c01000000636caebbf4432ccf69d2822b (good)
;; QUESTION SECTION:
;isidrodearceneguicarmona.es.      IN      NS

;; ANSWER SECTION:
isidrodearceneguicarmona.es. 21600 IN NS      ns1025.ui-dns.de.
isidrodearceneguicarmona.es. 21600 IN NS      ns1025.ui-dns.biz.
isidrodearceneguicarmona.es. 21600 IN NS      ns1025.ui-dns.com.
isidrodearceneguicarmona.es. 21600 IN NS      ns1025.ui-dns.org.

;; Query time: 19 msec
;; SERVER: ::1#53(:1) (UDP)
;; WHEN: Thu Nov 10 08:56:43 CET 2022
;; MSG SIZE rcvd: 208

pc-profe@pcv-01:~$
```

Las 4 respuestas indican que hay 4 servidores DNS para ese dominio. **Fíjate que cuando se usa ns la consulta se hace a un dominio y no a una máquina** (si se hubiese puesto "dig www.isidrodearceneguicarmona.es ns" no habría habido respuesta)

Fijémonos de nuevo en la consulta directa, esto es, dado el nombre de dominio encontrar la IP:

```
root@PC-37:/home/pc-profe# dig www.google.es

;; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.google.es
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 50686
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.es.                IN      A

;; ANSWER SECTION:
www.google.es.                 101     IN      A      216.58.214.163

;; Query time: 160 msec
```

Como puede comprobarse, nuestro servidor DNS Bind9 ha respondido, la consulta ha tardado 160 milisegundos y ha habido respuesta correcta (existe ANSWER SECTION y status:NOERROR).

El proceso seguido ha sido el siguiente:

- el comando dig pide saber la IP de [www.google.es](http://www.google.es)



- se consulta al servidor DNS configurado en el ordenador, el nuestro, con dirección 127.0.0.1  
- 127.0.0.1 lo busca en su caché. No lo encuentra. Se dirige entonces a buscar en el primer servidor DNS que está puesto en su sección "forwarders", que es 8.8.8.8 (ver páginas anteriores). Entonces el servidor 8.8.8.8 le da la respuesta y nuestro servidor bind9 (127.0.0.1) responde, y almacena dicha respuesta en su caché por si se pide de nuevo en un plazo relativamente corto.

Hacemos otra consulta igual:

```
root@PC-37:/home/pc-profe# dig www.google.es
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.google.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52240
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.es.                IN      A
;; ANSWER SECTION:
www.google.es.                88      IN      A      216.58.214.163
;; Query time: 0 msec
```

Ahora el tiempo de respuesta es MUCHO MENOR (0 milisegundos), ya que el servidor DNS ha buscado en su caché y ha encontrado la respuesta, no necesitando acceder al exterior -Internet- para pedírsela a otro servidor DNS (en nuestro caso 8.8.8.8)

Recuerda que puedes borrar la caché del servidor DNS con el comando:

rndc flush

Con esta orden, nuestro servidor DNS ya no tendrá información alguna de los nombres de dominio, y cualquier petición hará que la solicite a un forwarder que tiene configurado.

**Nota para pensar:** Es posible que si más tarde (ya caducada la caché) hacemos de nuevo dig [www.google.es](http://www.google.es) nos aparezca una IP diferente; esto ocurre porque [www.google.es](http://www.google.es) tiene varias IP con el mismo contenido (el buscador), y el servidor de nombres DNS propiedad de Google reparte esas IP entre los clientes para equilibrar (balancear) la carga de su buscador en varias IP, de forma que se reparte el trabajo de búsqueda que ofrece Google entre varios ordenadores (no solo uno, ya que quedaría desbordado ante la gran cantidad de peticiones que tiene Google, el buscador más importante a día de hoy, activo desde 1998)

**EJEMPLO 2 :** dig -x hace una búsqueda inversa (dada una dirección IP, devuelve su dominio)

```
root@PC-37:/home/pc-profe# dig -x 208.84.244.10
; <<>> DiG 9.10.3-P4-Ubuntu <<>> -x 208.84.244.10
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53582
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;10.244.84.208.in-addr.arpa.    IN      PTR
;; ANSWER SECTION:
10.244.84.208.in-addr.arpa. 7199 IN      PTR      www.terra.es.
;; Query time: 631 msec
```

Comprueba siempre que existe sección ANSWER (respuesta) y que el estado ha sido NOERROR. Si lo hacemos otra vez, se comprueba que tardará menos pues tiene esa información en su caché:

```
root@PC-37:/home/pc-profe# dig -x 208.84.244.10

; <<>> DiG 9.10.3-P4-Ubuntu <<>> -x 208.84.244.10
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46690
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;10.244.84.208.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
10.244.84.208.in-addr.arpa. 7045 IN      PTR      www.terra.es.

;; Query time: 0 msec
```

- Si se pone dig @servidor y luego el resto del comando, se hará la consulta al SERVIDOR DNS que se haya puesto en @servidor. Hasta ahora, todos los ejemplos que hemos puesto es como si hubiésemos escrito **dig @127.0.0.1**, esto es, el servidor de nombres DNS que tenemos instalado en nuestra máquina, que es el que está puesto en las propiedades TCP/IP de nuestra tarjeta de red. En la captura siguiente, se pregunta al servidor DNS 1.0.0.1

```
root@pcvb-01:/home/pc-profe# dig www.juntadeandalucia.es @1.0.0.1

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> www.juntadeandalucia.es @1.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30693
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.juntadeandalucia.es.      IN      A

;; ANSWER SECTION:
www.juntadeandalucia.es. 14      IN      A      217.12.31.91

;; Query time: 12 msec
;; SERVER: 1.0.0.1#53(1.0.0.1) (UDP)
;; WHEN: Sat Oct 04 19:13:56 CEST 2025
;; MSG SIZE rcvd: 68

root@pcvb-01:/home/pc-profe#
```

## 2.B) Comando cliente DNS ping

ping es una herramienta que sirve para saber si un equipo está funcionando o no. Ping usa el servicio DNS para la resolución de nombres a direcciones IP si se emplea con máquinas identificadas por su nombre y no por IP:

```
root@pc-05:/home/pc-profe# ping isidroearceneguiycarmona.es
PING isidroearceneguiycarmona.es (82.165.235.162) 56(84) bytes of data.
64 bytes from clienteservidor.es (82.165.235.162): icmp_seq=1 ttl=53 time=66.4 ms
64 bytes from clienteservidor.es (82.165.235.162): icmp_seq=2 ttl=53 time=68.6 ms
64 bytes from clienteservidor.es (82.165.235.162): icmp_seq=3 ttl=53 time=68.3 ms
64 bytes from clienteservidor.es (82.165.235.162): icmp_seq=4 ttl=53 time=82.9 ms
^C
--- isidroearceneguiycarmona.es ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3012ms
rtt min/avg/max/mdev = 66.403/71.583/82.917/6.600 ms
root@pc-05:/home/pc-profe#
```

## 2.C) Comando cliente DNS host

Este comando permite averiguar direcciones IP a partir de nombres de dominio y viceversa:

```
root@pc-05:/home/pc-profe# host www.altavista.es
www.altavista.es is an alias for rc.yahoo.com.
rc.yahoo.com is an alias for src.g03.yahoodns.net.
src.g03.yahoodns.net is an alias for any-src.a03.yahoodns.net.
any-src.a03.yahoodns.net has address 77.238.184.150
any-src.a03.yahoodns.net has address 188.125.73.108
root@pc-05:/home/pc-profe#
```

## 2.D) Comando cliente DNS nslookup

Este comando está disponible tanto en Windows como en Linux  
Ejemplo en Windows:



```
Símbolo del sistema
nslookup
Servidor predeterminado: one.one.one.one
Address: 1.1.1.1

> www.google.es
Servidor: one.one.one.one
Address: 1.1.1.1

Respuesta no autoritativa:
Nombre: www.google.es
Addresses: 2a00:1450:4003::1203
216.58.201.163

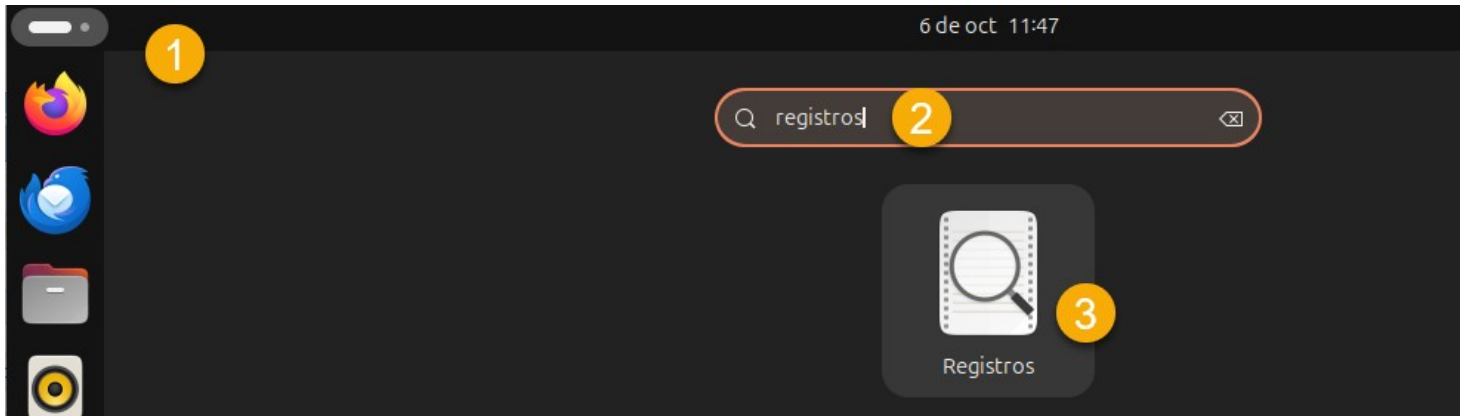
> www.rtve.es
Servidor: one.one.one.one
Address: 1.1.1.1

Respuesta no autoritativa:
Nombre: a567.b.akamai.net
Addresses: 88.221.52.40
88.221.52.58
Aliases: www.rtve.es
rtve.es.edgesuite.net

> quit
```

### 3) SERVIDOR DNS PRIMARIO EN UBUNTU

**MUY IMPORTANTE:** EL PROGRAMA "Registros" (mencionado anteriormente y que hay que instalar) PERMITIRÁ CORREGIR FALLOS DE FUNCIONAMIENTO DEL SERVIDOR. ÚSALO EN CASO DE QUE EL SERVIDOR DNS NO ACTÚE COMO DEBIERA



Como ejemplo de estudio se va a trabajar con un dominio **que no existe en realidad**, **isidroarcenegui.es**  
Para configurar la zona del servidor DNS primario hacen falta los archivos:

a) /etc/bind/named.conf

```
named.conf x
// This is the primary configuration file for the BIND DNS server
named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information
on the
// structure of BIND configuration files in Debian, *BEFORE* you
customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/
named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

b) /etc/bind/named.conf.local

```
named.conf local x
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "isidroarcenegui.es" {
    type master;
    file "/etc/bind/db.isidroarcenegui.es";
};
zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};
```



En este archivo se definen las 2 zonas, una para búsqueda directa (dado un nombre de dominio, obtener su IP) y otra de búsqueda inversa (dada una IP, obtener su nombre de dominio)

c) archivo de búsqueda directa, /etc/bind/db.isidroarcenegui.es

```
db.isidroarcenegui.es x
;
;       Zona directa para "isidroarcenegui.es"
;
$TTL 1D
@      IN      SOA      isidroarcenegui.es.  josejl68.gmail.com (
                        10      ; Serial
                        8H      ; Refresh
                        2H      ; Retry
                        4W      ; Expire
                        1D )    ; Minimum
;
;       IN      NS       pc-profe3           ;Servidor DNS del dominio
;       IN      MX       10      pc-profe3    ;Servidor de correo
;
isidroarcenegui.es.  IN      A      192.168.1.150; IP para ese dominio
pc-profe3            IN      A      192.168.1.150; IP de pc-profe3
www                  IN      CNAME    pc-profe3 ; www es alias de pc-profe3
ftp                  IN      CNAME    pc-profe3 ; ftp es otro alias de pc-profe3
;
aula2smr-pc01        IN      A      192.168.1.160 ; IP manual
aula2smr-pc02        IN      A      192.168.1.161 ; otra IP manual
```

d) archivo /etc/bind/db.192, para la zona de búsqueda inversa:

```
db.192 x
;
;       Fichero de búsqueda inversa para la red "192.168.1.0/24"
;
$TTL 1D
@      IN      SOA      pc-profe3.isidroarcenegui.es.  josejl68.gmail.com (
                        10      ; Serial
                        8H      ; Refresh
                        2H      ; Retry
                        4W      ; Expire
                        1D )    ; Minimum
;
;       IN      NS       pc-profe3.isidroarcenegui.es.
150    IN      PTR       pc-profe3.isidroarcenegui.es.
;
160    IN      PTR       aula2smr-pc01.isidroarcenegui.es. ; entrada manual
161    IN      PTR       aula2smr-pc02.isidroarcenegui.es. ; otra entrada
```

Una vez situados estos archivos en sus carpetas correspondientes, ya se puede reiniciar el servidor DNS y luego hacer consultas a este dominio ficticio desde programas clientes, como:

#### Ejemplo 1:

```
root@PC-10:/home/pc-profe# service bind9 restart
* Stopping domain name service... bind9
waiting for pid 927 to die
[ OK ]
* Starting domain name service... bind9
[ OK ]
root@PC-10:/home/pc-profe# dig isidroarcenegui.es

; <<>> DiG 9.9.2-P1 <<>> isidroarcenegui.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53413
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;isidroarcenegui.es.                IN      A

;; ANSWER SECTION:
isidroarcenegui.es. 86400 IN A 192.168.1.150
```

#### Ejemplo 2: otra consulta directa:

```
root@PC-10:/home/pc-profe# dig www.isidroarcenegui.es

; <<>> DiG 9.9.2-P1 <<>> www.isidroarcenegui.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51802
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.isidroarcenegui.es.            IN      A

;; ANSWER SECTION:
www.isidroarcenegui.es. 86400 IN CNAME pc-profe3.isidroarcenegui.es.
pc-profe3.isidroarcenegui.es. 86400 IN A 192.168.1.150
```

En la respuesta se menciona que [www.isidroarcenegui.es](http://www.isidroarcenegui.es) es un alias (CNAME) de pc-profe3.isidroarcenegui.es que tiene como dirección IP 192.168.1.150

Ejemplo 3: una consulta inversa:

```
root@PC-10:/home/pc-profe# dig -x 192.168.1.161

; <<>> DiG 9.9.2-P1 <<>> -x 192.168.1.161
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3833
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;161.1.168.192.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
161.1.168.192.in-addr.arpa. 86400 IN      PTR      aula2smr-pc02.isidroarcenegui.es.
.

;; AUTHORITY SECTION:
1.168.192.in-addr.arpa. 86400 IN      NS      pc-profe3.isidroarcenegui.es.

;; ADDITIONAL SECTION:
pc-profe3.isidroarcenegui.es. 86400 IN      A      192.168.1.150

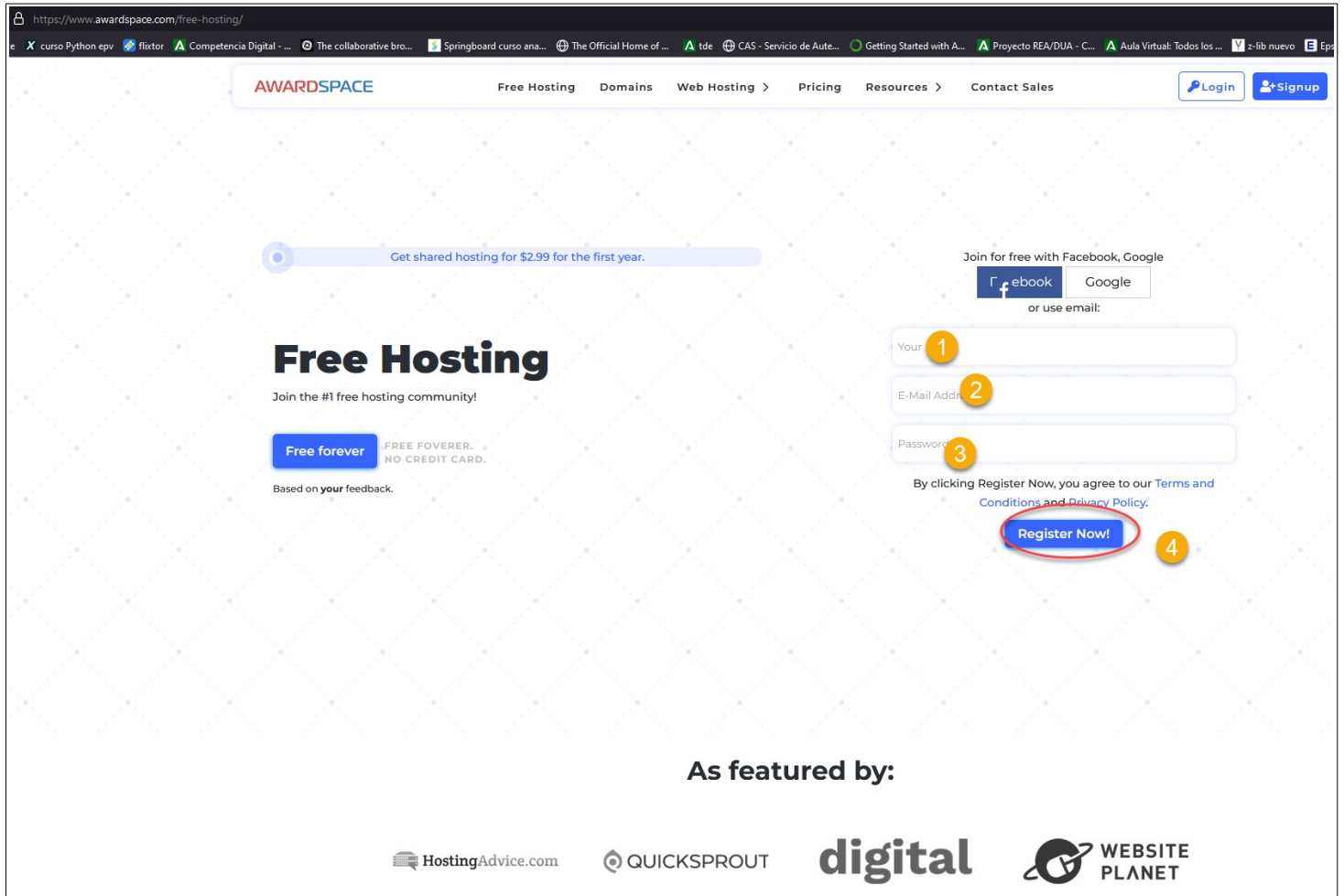
;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Oct 6 18:05:17 2013
;; MSG SIZE rcvd: 141
```



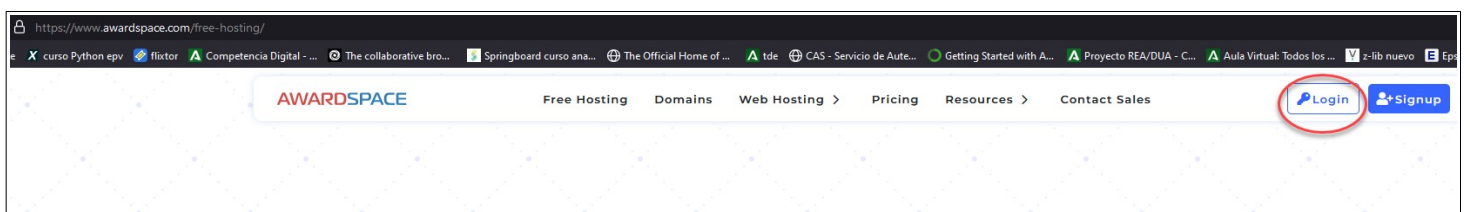
## 4) CONFIGURAR UN DOMINIO PARA QUE APUNTE A UN SERVIDOR DE NOMBRES DE UN HOSTING.

En este ejemplo vamos a suponer que deseamos que un nombre de dominio que hemos registrado apunte no a un servidor web que tengamos en casa, sino a uno gratuito, <https://www.awardspace.com/free-hosting/> que nos proporciona hosting (espacio web gratuito para poner nuestras páginas).

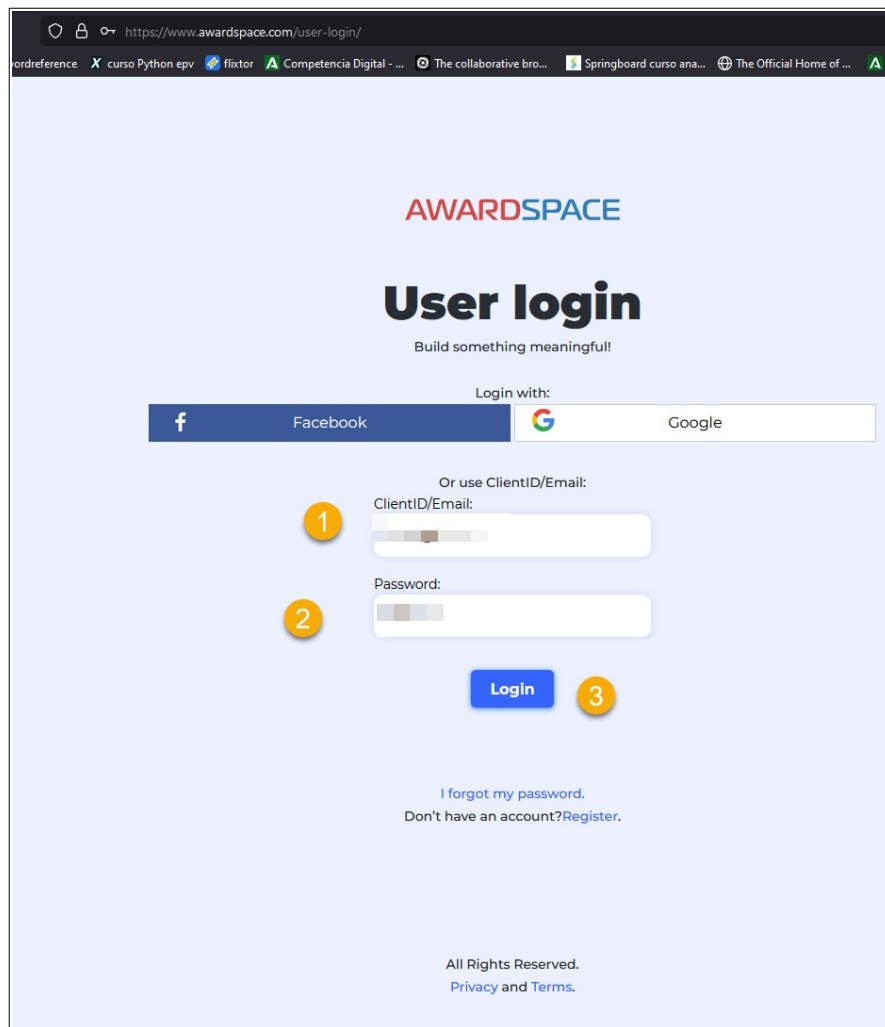
En el ejemplo que ahora sigue, el servicio de hosting gratuito proporcionado GRATUITAMENTE NOS DA ESPACIO WEB, FTP, CORREO ELECTRÓNICO Y MUCHAS MÁS POSIBILIDADES.



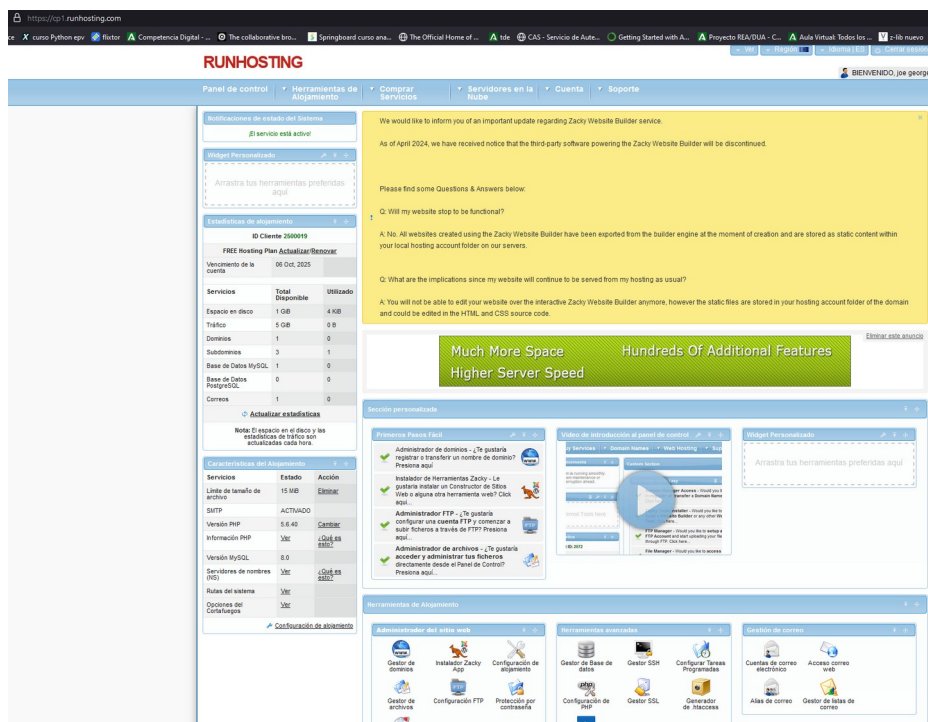
Una vez registrados, entramos:



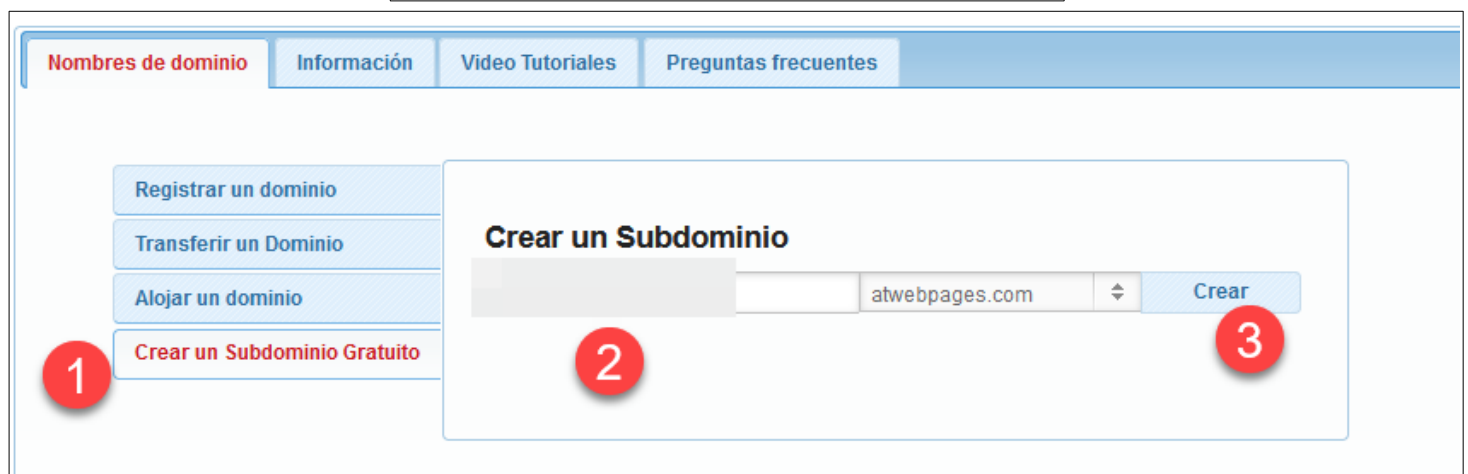
Entramos y vemos algo así:



Sale:



Hacemos:

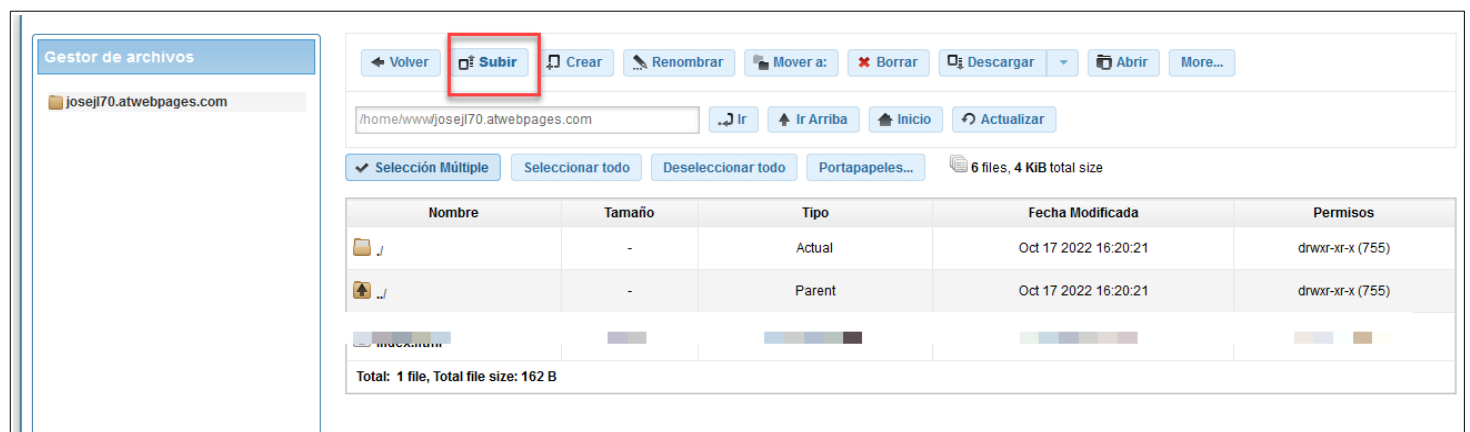
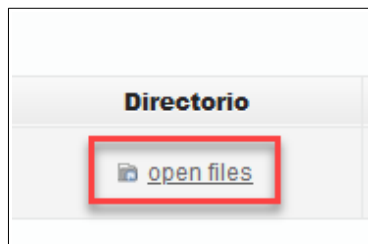


Al abrir el sitio web, se ve que no hay nada. Vamos a crear un archivo index.html y a subirlo:

Usamos un editor para escribir:

```
1 <html>
2 <head>
3 <title>Mi primera web </title>
4 </head>
5 <body>
6 <h1>IES "Isidro Arcenegui"</h1>
7 Despliegue de aplicaciones web<br><br>
8 Curso 2024-2025
9 </body>
10 </html>
```

Subimos index.html



Ya está hecho. Si escribimos en nuestro navegador el nombre de nuestro dominio, debe aparecer nuestra página web. Si no sale, como es mi caso, hay que pulsar la tecla F5 para refrescar la página:



