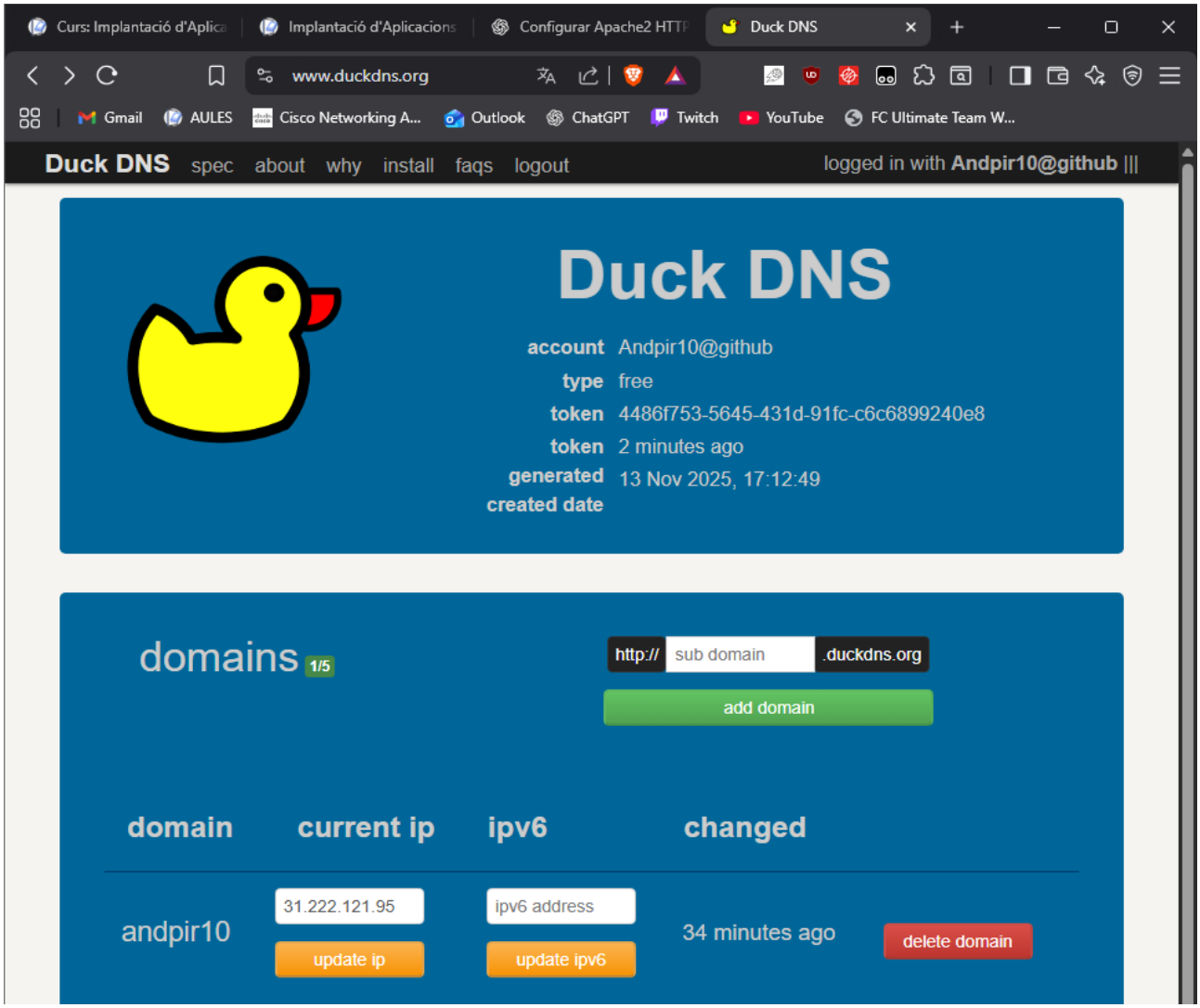
1-Crear subdominio en DuckDNS

Entra en https://www.duckdns.org

Inicia sesión

En el campo *add domain* , pon tu nombre :



Copia el token que te da DuckDNS

Haz un ping a tu DNS → *ping -c 1 andpir10.duckdns.org*

```
pirvu@pirvuserver:~$ ping -c 1 andpir10.duckdns.org
PING andpir10.duckdns.org (31.222.121.95) 56(84) bytes of data.
64 bytes from 31.222.121.95: icmp_seq=1 ttl=58 time=31.9 ms

--- andpir10.duckdns.org ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 31.939/31.939/31.939/0.000 ms
pirvu@pirvuserver:~$
```

2-Instalar Apache2 y crear web

sudo apt-get install -y apache2

Creamos el directorio de nuestra web :

export DOMAIN="andpir10.duckdns.org"
export WEBROOT="/var/www/miweb"
sudo mkdir -p $WEBROOT

```
pirvu@pirvuserver:~$ export DOMAIN="andpir10.duckdns.org"
pirvu@pirvuserver:~$ export WEBROOT="/var/www/miweb"
pirvu@pirvuserver:~$ sudo mkdir -p $WEBROOT
[sudo] password for pirvu:
pirvu@pirvuserver:~$
```

Creamos un archivo de prueba :

echo "<h1>HTTPS con Let's Encrypt (DNS-01)</h1>" | sudo tee $WEBROOT/index.html

Creamos el VirtualHost básico HTTP

sudo tee /etc/apache2/sites-available/miweb.conf > /dev/null <<'EOF'
*<VirtualHost *:80>*
ServerName andpir10.duckdns.org
DocumentRoot /var/www/miweb

<Directory /var/www/miweb>
Options -Indexes +FollowSymLinks
AllowOverride All
Require all granted
</Directory>

ErrorLog ${APACHE_LOG_DIR}/miweb_error.log
CustomLog ${APACHE_LOG_DIR}/miweb_access.log combined
</VirtualHost>
EOF

```
pirvu@pirvuserver:~$ echo "<h1>HTTPS con Let's Encrypt (DNS-01)</h1>" | sudo tee $WEBROOT/index.html
<h1>HTTPS con Let's Encrypt (DNS-01)</h1>
pirvu@pirvuserver:~$ sudo tee /etc/apache2/sites-available/miweb.conf > /dev/null <<'EOF'
> <VirtualHost *:80>
    ServerName andpir10.duckdns.org
    DocumentRoot /var/www/miweb

    <Directory /var/www/miweb>
        Options -Indexes +FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/miweb_error.log
    CustomLog ${APACHE_LOG_DIR}/miweb_access.log combined
</VirtualHost>
> EOF
pirvu@pirvuserver:~$
```

sudo sed -i "s/andpir10.duckdns.org/$DOMAIN/" /etc/apache2/sites-available/miweb.conf

Activamos el sitio y recargamos el servidor Apache2

sudo a2ensite miweb.conf
sudo systemctl reload apache2

Comprobamos que funciona con → *curl -I http://127.0.0.1*
***debe volver** HTTP/1.1 200 OK**

3-Instalar Certbot y emitir el certificado Let's Encrypt con DNS-01

Primero instalamos el python3-pip

sudo apt-get install -y python3-pip

Ahora instalamos el Certbot

sudo pip3 install certbot-dns-duckdns –break-system-packages

Creamos la carpeta donde se guardará la información del DuckDNS y todo lo necesario para su funcionamiento

sudo mkdir -p /etc/letsencrypt

echo "dns_duckdns_token=4486f753-5645-431d-91fc-c6c6899240e8" | sudo tee /etc/letsencrypt/duckdns.ini

sudo chmod 600 /etc/letsencrypt/duckdns.ini

sudo certbot certonly --authenticator dns-duckdns --dns-duckdns-credentials /etc/letsencrypt/duckdns.ini -d andpir10.duckdns.org

4-Activar HTTPS en Apache

Activamos el módulo SSL de Apache

sudo a2enmod ssl

Creamos el VirtualHost HTTPS

```
sudo tee /etc/apache2/sites-available/miweb-ssl.conf > /dev/null <<'EOF'
<VirtualHost *:443>
    ServerName andpir10.duckdns.org
    DocumentRoot /var/www/miweb

    SSLEngine on
    SSLCertificateFile /etc/letsencrypt/live/andpir10.duckdns.org/fullchain.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/andpir10.duckdns.org/privkey.pem

    <Directory /var/www/miweb>
        Options -Indexes +FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/miweb_ssl_error.log
    CustomLog ${APACHE_LOG_DIR}/miweb_ssl_access.log combined
</VirtualHost>
EOF
```

Activamos el sitio y recargamos Apache

```
sudo a2ensite miweb-ssl.conf
sudo systemctl reload apache2
```

Verificamos el certificado

sudo certbot certificates

debería salir algo así

```
pirvu@pirvuserver:~$ sudo certbot certificates
Saving debug log to /var/log/letsencrypt/letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Found the following certs:
  Certificate Name: andpir10.duckdns.org
    Serial Number: 5cb9ca8f0e85dac57bf85b9b4a85803e106
    Key Type: ECDSA
    Domains: andpir10.duckdns.org
    Expiry Date: 2026-02-11 16:56:37+00:00 (VALID: 89 days)
    Certificate Path: /etc/letsencrypt/live/andpir10.duckdns.org/fullchain.pem
    Private Key Path: /etc/letsencrypt/live/andpir10.duckdns.org/privkey.pem
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
pirvu@pirvuserver:~$
```

Comprobamos que funciona el certificado Let's Encrypt con nuestro DNS personalizado