MANUAL FILTRADO DNS EN ROUTER DEL OPERADOR DE INTERNET

EDUCACIÓN DIGITAL RESPONSABLE

IMPORTANTE: Este manual esta realizado con el objetivo de ayudar a las familias en los primeros usos de internet de los menores. Toda solución aquí propuesta puede ser "interceptada" por el menor cuando van adquiriendo conocimientos informáticos de nivel medio-avanzado, si bien estas opciones ofrecen una solución que puede resultar muy efectiva para evitar que en los primeros años de usos de las nuevas tecnologías, los menores puedan encontrarse por accidente contenido inapropiado para su edad. Las soluciones que se comentan a continuación son efectivas en PCs, tablets, Móviles, consolas, eReaders, etc... conectados a la conexión de internet del domicilio, cualquier dispositivo que tenga su conexión de datos independiente (por ejemplo con una tarjeta SIM de datos) no será filtrado su contenido, igualmente si se usan navegadores que no sean controlados por las aplicaciones de control parental tampoco será filtrado su contenido.

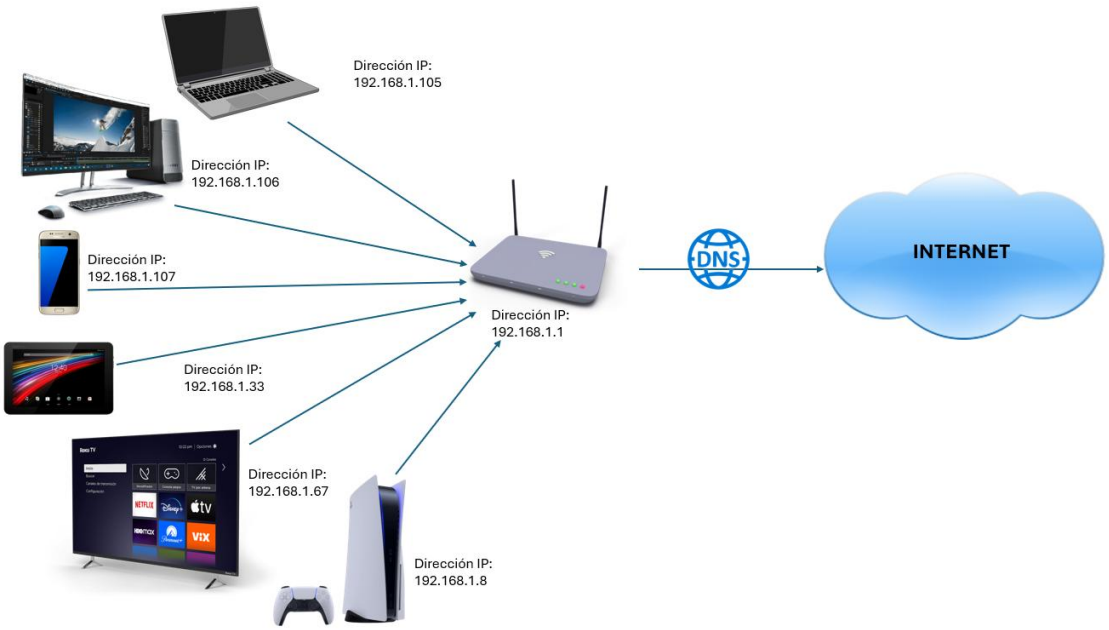
COMENZAMOS

Antes de empezar, unos conceptos básicos para entenderlo todo mejor:

¿Qué es dirección ip?

Básicamente una dirección IP es una dirección única que identifica a un dispositivo en una red (como la que tenemos en nuestra casa que crea el router de nuestro operador de internet), digamos que es como el "DNI" de nuestros dispositivos cuando están conectados en red. Cada dispositivo (Pc, Tablet, móvil, consola,tv, router...) que conectamos a esta red se le asigna una dirección ip.

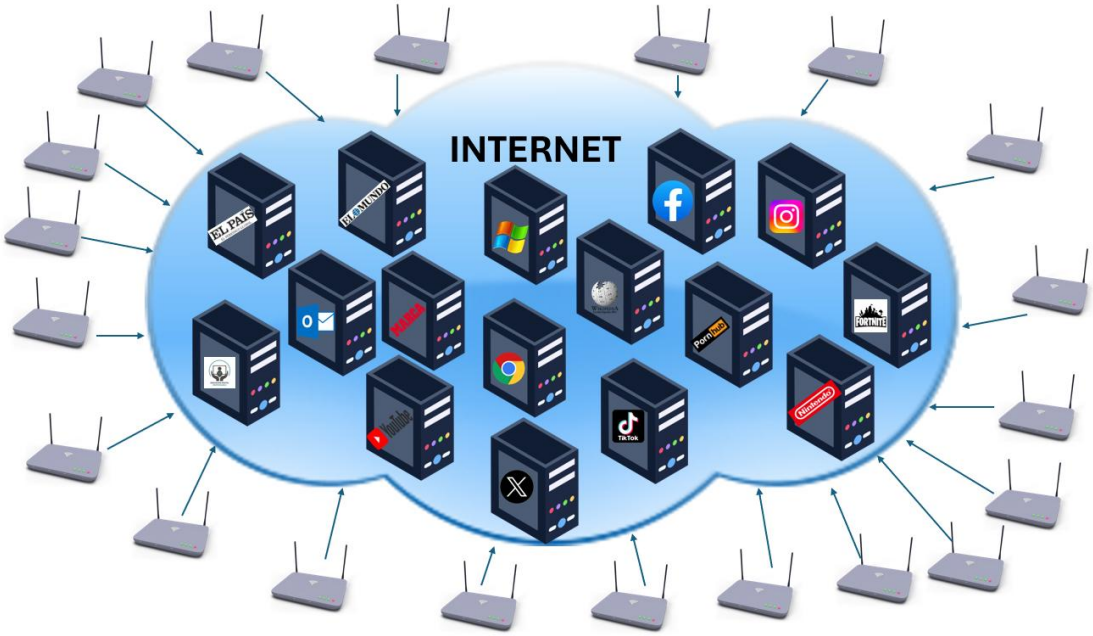
En la siguiente imagen mostramos un ejemplo:



¿Qué es un servidor web?

Piensa en él como un camarero en un restaurante que te entrega la comida que has pedido. Un servidor web es un ordenador que almacena y entrega páginas web cuando alguien las solicita. Es donde están alojadas las páginas que vemos en internet.

Como hemos visto en la primera pregunta, cada servidor web (cada ordenador que este conectado a internet) tiene una dirección IP, puesto que internet es otra red (como la que tenemos en la casa) pero más grande y con dispositivos conectados en todo el mundo. En la siguiente imagen mostramos un ejemplo:



¿Qué es DNS?

Es como una guía telefónica de internet.

El sistema de nombres de dominio (DNS) es un protocolo que traduce el nombre de una página web por la dirección ip de su servidor web.

Accedemos a las páginas web con el nombre de dominio (www.google.es, www.marca.es, www.outlook.es, etc ...) que es mucho más sencillo que si para acceder a Google tuviésemos que recordar su dirección ip y escribirla en el navegador.

Los servidores DNS suprimen la necesidad de que los humanos memoricen direcciones IP. Por ejemplo 142.251.211.227 es la dirección ip del servidor web de la página de Google. Si en tu navegador introduces esa dirección ip, accederás al mismo contenido que si escribes www.google.es.

Lo que hacemos habitualmente es escribir directamente la dirección de la web a la que queremos acceder (por ejemplo www.google.es) y mandarla a nuestro router, el cual le pide a las DNS que busque el servidor de esa web en internet, las DNS traducen la web solicitada en la ip de su servidor (142.251.211.227 en nuestro ejemplo) y este servidor devuelve la página web solicitada a nuestro dispositivo, como se ve en la imagen:

****

CONFIGURACIÓN FILTRADO DNS

****

Una vez aclarado esto podemos explicar que cada operador de internet (movistar, Orange, digi, Vodafone, ptv, Pepephone, etc...) tiene unos servidores DNS propios y a través de ellos nos dan acceso a las páginas webs que queremos acceder.

Hay determinados servicios ajenos a las operadoras, que ofrecen DNS alternativos, los cuales pueden permitir filtrar el acceso a algún tipo de páginas webs.

Hay muchos, pero por ejemplo Clean Browsing ofrece unas dns que filtran el contenido para adultos. También ofrecen servicios similares DNS0, OpenDNS y Cloudflare

En nuestro ejemplo usaremos las DNS de filtrado de Clean Browsing que son las que se muestran a continuación:

CleanBrowsing

IPv4	185.228.168.168 185.228.169.168

EDUCACIÓN DIGITAL RESPONSABLE

¿Dónde y como cambiar las dns del operador por otras que filtren el contenido?

Para cambiar las dns del operador debemos acceder al menú del router. Para hacerlo dependerá del operador que tengamos. Es importante tener en cuenta que los router que nos instalan las operadores de internet NO permiten forzar a los dispositivos que se conecten a él usar las DNS que se configuren en el router, permitiendo que los dispositivos se cambien en su propia configuración las DNS y evitando por tanto el filtrado DNS que realiza el router, pero este caso lo tratamos en el apartado 3 de las "EXCEPCIONES Y COMO RESOLVERLAS" de la página 13 de este manual.

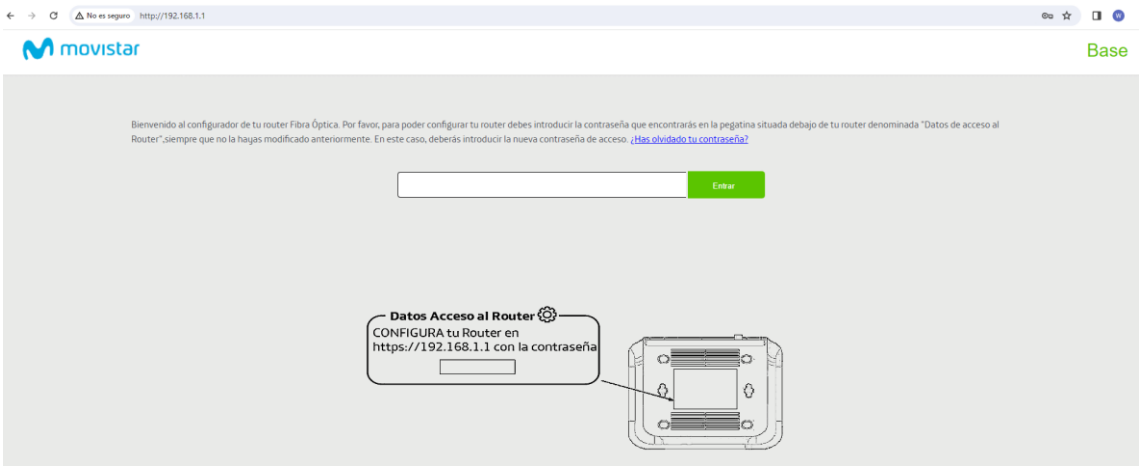
En esta guía muestro el acceso y la configuración en los principales operadores del mercado, el resto de operadores tendrán una configuración similar.

Debemos conectarnos a nuestra conexión a internet (por wifi o por cable) y dependiendo del operador realizar los siguientes pasos:

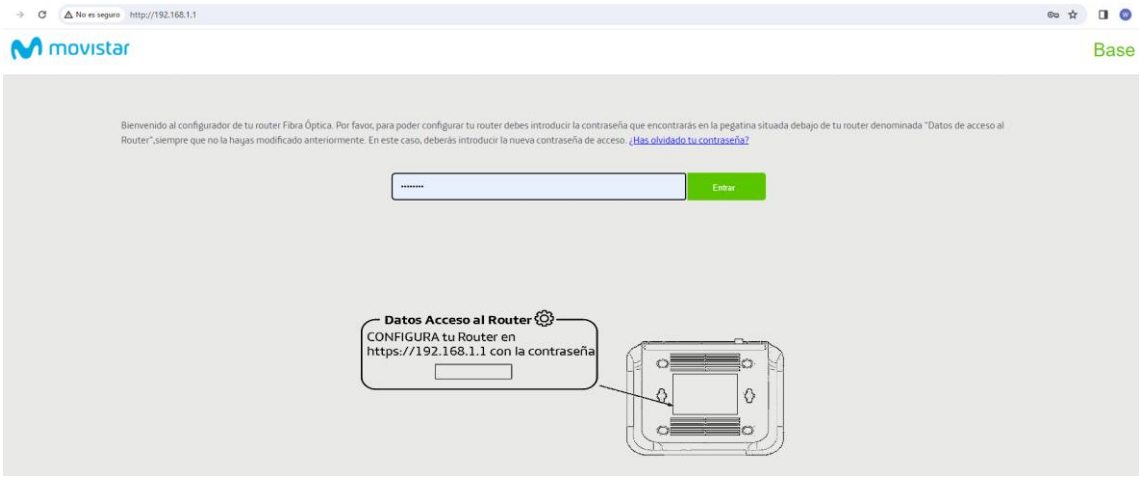
OPERADOR MOVISTAR:

En la parte posterior del router hay una pegatina con la información de la wifi (nombre de la wifi y su contraseña, y con la información para conectarse al router en el apartado "Datos de acceso al router". Ahí nos aparecerá la dirección ip del router y una contraseña de acceso.

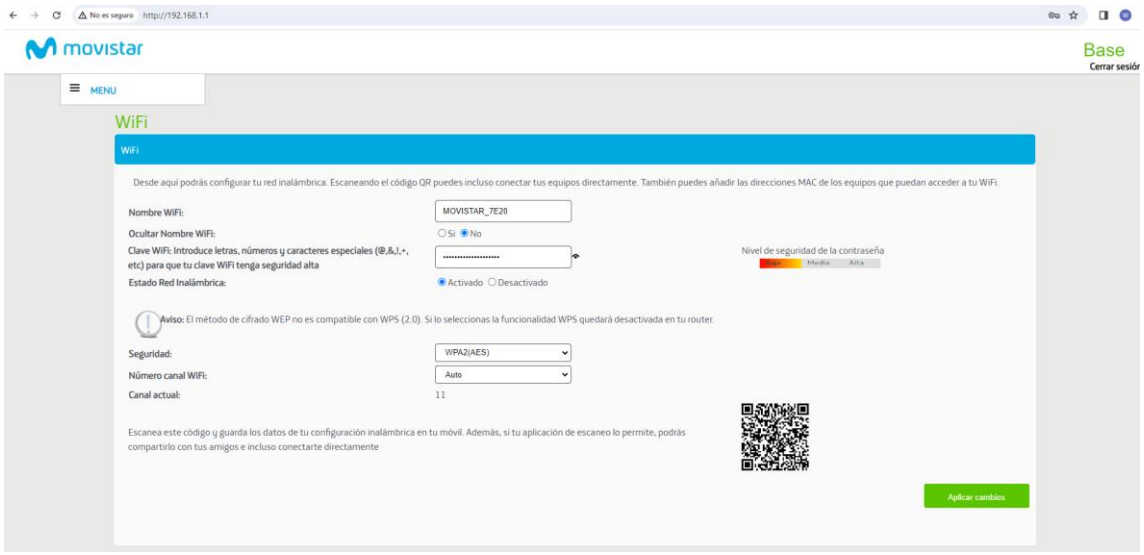
Accederemos a la configuración del router escribiendo la ip en nuestro navegador y nos aparecerá la siguiente imagen solicitando la contraseña:



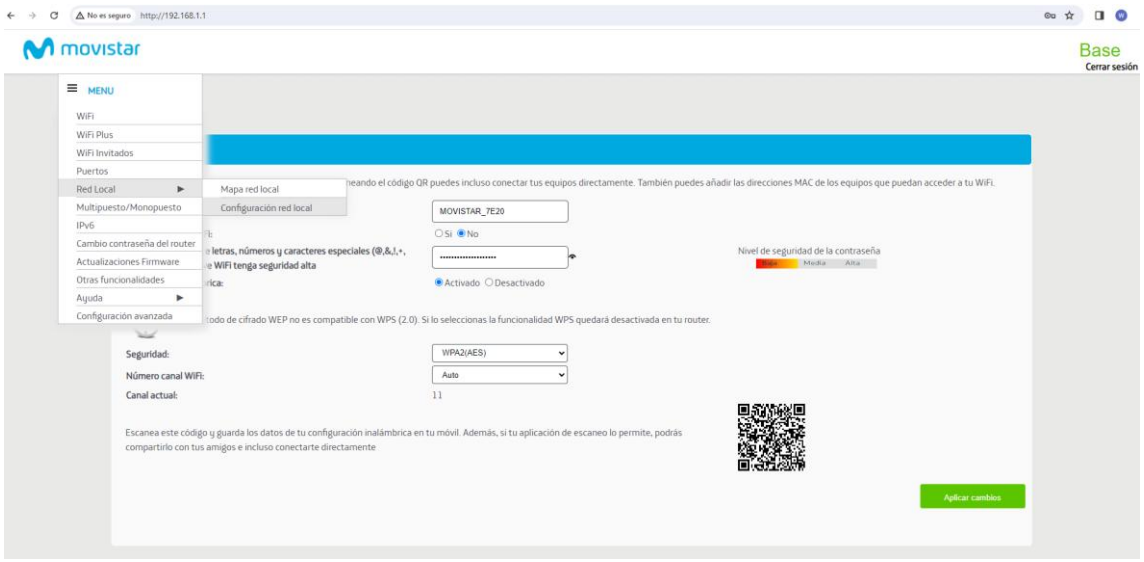
Introducimos la contraseña que vimos en la pegatina y le damos a “entrar”



Con esto entraremos en el menú de configuración del router . En la parte superior izquierda nos aparece un MENÚ indicado con 3 líneas horizontales.



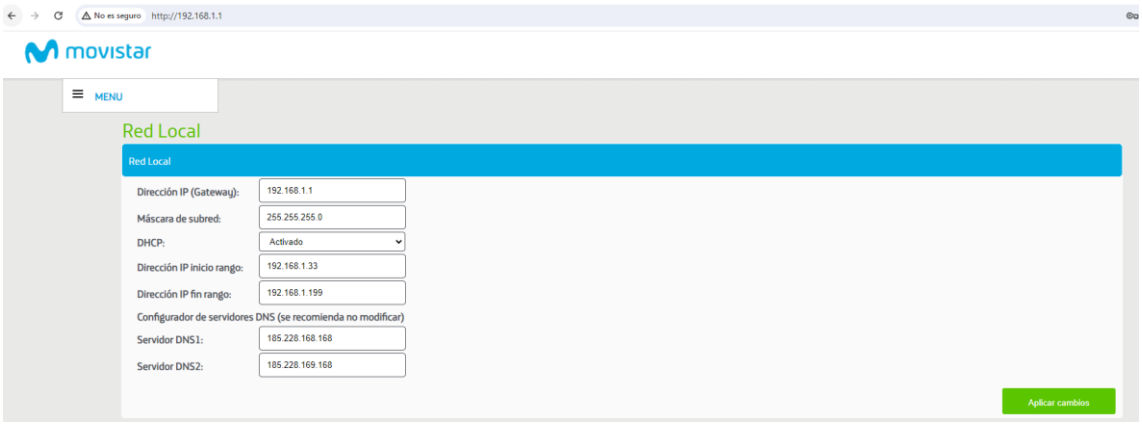
Pincharemos dicho menú y navegaremos hasta la opción “Red Local->Configuración red local”



Dentro de esa opción ns encontramos la siguiente pantalla donde encontramos los Servidores DNS que por defecto tiene configurados el router de MOVISTAR.

Los modificaremos por los DNS de filtrado que hayamos elegido, en mi caso utilizo los DNS

de Cleanbrowsing 192.228.168.168 como servidor DNS1 y 192.228.169.168 como servidor DNS2. Y le daremos al botón verde “Aplicar cambios”.



Con esto quedaría configurado, para que se haga efectivo deberemos desconectar nuestro equipo (Pc) de la conexión a internet y volverlo a conectar para que se hagan efectivos los cambios (un reinicio del pc también es válido).

En caso de que no veamos que funciones quizás sea necesario apagar y volver a encender el router.

OPERADOR ORANGE:

Lamentablemente Orange no permite modificar las dns de su router, por lo que la solución pasa por realizar los pasos indicados en el punto 3 del apartado “EXCEPCIONES Y COMO RESOLVERLAS” de la página 13 de este mismo manual y esto consiste en comprar un segundo router y realizar la configuración de filtrado de dns en él.

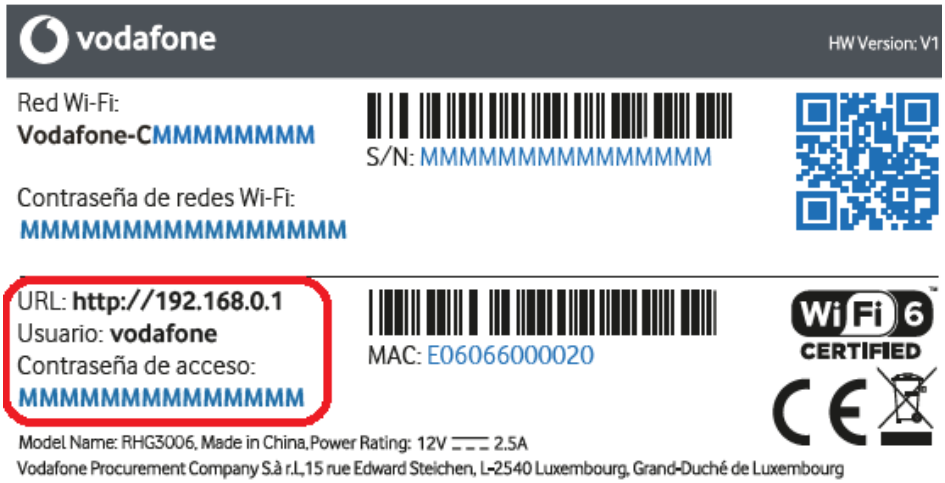
OPERADOR VODAFONE:

Cómo entrar a tu router

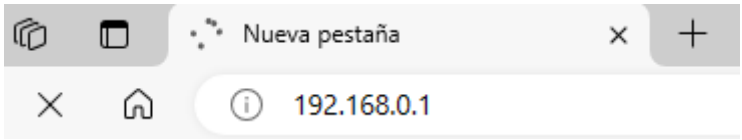
Para entrar a tu router y ver su configuración o modificarla, hay que estar conectado a él. Si tienes dudas sobre el proceso, puedes consultar cómo conectar por wifi tus equipos al router o conectarte directamente con un cable Ethernet si estás en un ordenador.

Una vez conectado a tu router, sigue estos pasos:

1. **Localiza en la pegatina del router el "Usuario" y la "Contraseña de acceso"**. Sácales una foto o apúntalos porque serán necesarios para acceder.



2. Junto al usuario encontrarás una **dirección IP o un nombre**. Introduce uno de ellos en tu navegador.

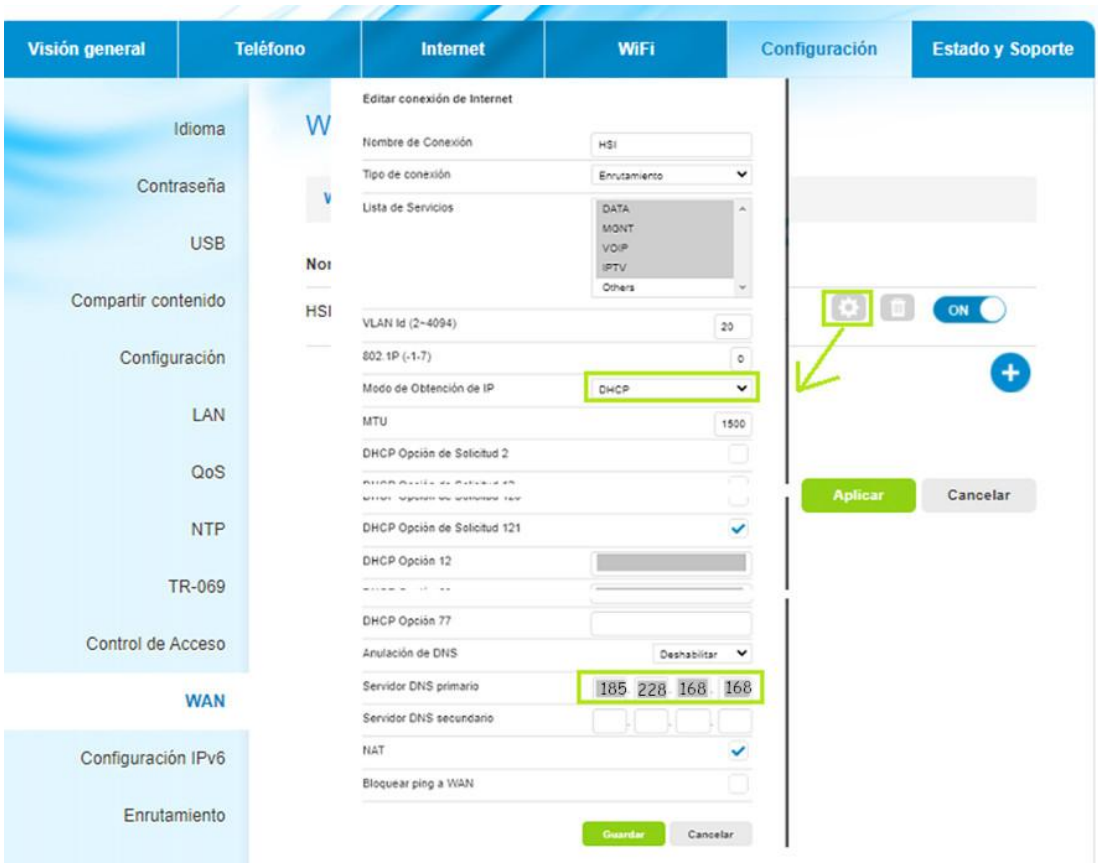


3. Escribe ahora el "Usuario" y la "Contraseña de acceso"

Con estos pasos habremos accedido al menú de configuración del router (en nuestro ejemplo es el Router Sercomm FG824CD).
En las pestañas que aparecen arriba seleccionaremos la opción Configuración, y en el menú de la parte izquierda seleccionaremos WAN.

En la pantalla que aparece pincharemos en el icono con forma de rueda dentada 

Lo que nos abrirá una ventana en donde nos aparecerán toda la configuración, incluida los servidores DNS primario y secundario. En ellos deberemos poner los DNS de Clean Browsing 185.228.168.168 en el DNS primario y 185.228.169.168 en el DNS secundario.



OPERADOR DIGI:

Si deseas **cambiar las DNS router DIGI**, sigue estos sencillos pasos que a continuación detallamos:

Accede a la configuración del router DIGI. Si no sabes cómo realizar esta operación. Para ello:

Lo primero que tienes que hacer es verificar que tu dispositivo está conectado al router por cable Ethernet o mediante WiFi. Una vez que has podido conectar router DIGI, abre el navegador y en la barra de direcciones escribe: 192.168.1.1.

Hay otra forma de saber la IP para acceder router DIGI que te resultará muy sencilla y rápida si sigues estos pasos:

- Desde la ventana de comandos de Windows o Terminal en Mac, ntroduce el comando "*ipconfig*" en Windows o "*ifconfig*" en Mac y pulsa '*Enter*'.
- Dirígete al apartado «*Default Gateway*» o «*Puerta de enlace predeterminada*«, allí encontrarás la dirección IP DIGI router.

Una vez que has seguido los pasos indicados anteriormente y te aparece la pantalla de acceso al router DIGI, deberás introducir el nombre de **usuario y contraseña router DIGI**. A continuación, te indicamos como hacerlo paso a paso:

- Abre una pestaña en tu navegador web.
- Coloca en la barra del navegador la dirección IP que te hemos indicado en el apartado anterior «IP router DIGI«.
- Para entrar en el router DIGI deberás introducir «*user*» en el campo «*Nombre de usuario*» y «*user*» en el campo «*Contraseña*«.
- Para finalizar pulsa el botón '*Iniciar sesión*'.

1. Una vez dentro, dirígete al apartado «*Red local*» en el menú superior.
2. Ahora, localiza el submenú «*LAN*«. Lo encontrarás en la parte izquierda.
3. Desplázate hacia abajo hasta el apartado «*Servidor DHCP*«.
4. Marca la opción '*Desactivado*' en la opción «*ISP DNS*» para poder ver los campos donde configurarás las DNS.
5. En los campos '*DNS principal*' y '*DNS secundario*' podrás añadir tus propias DNS. En nuestro caso cambiaríamos los que vienen por defecto (en la imagen aparecen 192.168.1.128 y 94.140.14.14) por las de Cleanbrowsing 192.228.168.168 como servidor DNS principal y 192.228.169.168 como servidor DNS secundario.
6. Para finalizar, pulsa sobre el botón '*Aplicar*'.

Nota

El proceso descrito se ha realizado con el modelo de router DIGI **ZTE H3600**, aunque en el resto de modelos que suministra DIGI, los pasos son muy similares.

Una vez realizado todo esto si se intenta acceder a una página web de contenido para adultos el navegador no cargará la página.

EXCEPCIONES Y COMO RESOLVERLAS

1. Si se usa un navegador que tenga la opción de activar una VPN (por ejemplo, Opera, Tor, Brave...) se saltan la configuración del filtrado dns y pueden navegar con libertad.

   Para solucionarlo tendremos que combinar el uso de la configuración de filtrado dns con el uso de un control parental (Family link, Qustodio, En familia de Apple)

2. Si un usuario configura en su propio dispositivo final (PC, Tablet, móvil, consola, etc...) unas dns (como puede ser las del operador, o las de Google 8.8.8.8, o cualquier otra que no filtre el contenido) podrá navegar libremente sin restricción ya que no se aplicarán las dns (en nuestro caso de Clean Browsing) que hemos configurado en el router.

3. Para solucionarlo el punto 2 habrá que instalar un segundo router en nuestro hogar, dicho router debe tener la opción de "Forzaje DNS" en su configuración, y realizaremos la configuración de unas dns de filtrado como hemos visto anteriormente, lo que obligará a todos los dispositivos que se conecten a él a usar sus dns, y no podrán usar otras ni, aunque la configuren en el propio dispositivo final. Existen varios modelos de router que tienen esta función, un ejemplo de router con esta función y con un precio asequible pueden ser los modelos Cudy WR1200, Cudy WR1300. Explicamos su configuración en el ANEXO1.

4. Por último el usuario también puede hacer uso de páginas webs que actúan como proxy, ofreciendo a través de dicha web una conexión a internet independiente (como en un ordenador virtual conectado a otra red de internet diferente a la de nuestro hogar) y por tanto si se navega en dicho proxy no se le aplicarían las restricciones de acceso de los filtrados dns que hayamos configurado en nuestro router.

   Para solucionarlo podemos crear en nuestra aplicación de control parental un listado de webs (lista negra)que tengan esa opción de Proxy para que no se puedan acceder a ellas, permitiendo el acceso al resto (menos a las que filtre nuestro filtrado de dns por supuesto) aunque este listado habrá que estar actualizando si descubrimos alguna "web proxy" -nueva. También está la opción de hacer en su lugar una Lista blanca, esto es hacer un listado de los sitios webs a los que SI damos permiso para acceder, limitando el acceso a todo el resto de páginas webs que no estén en ese listado.

Para crear la Lista negra indicada en este último apartado tenemos que abrir la aplicación de control parental que usemos (por ejemplo, Family Link, qustodio, en familia) que se ha instalado en nuestro móvil e introducir las páginas a las que no queremos que se tenga acceso.

En family link:

Entramos en el menú “Restricciones de contenido”. Entramos en “Google Chrome”. Seleccionamos “Intentar bloquear sitios con contenido explícito”. Entramos en “Sitios bloqueados”. Introducimos uno a uno los proxies y buscadores que queremos bloquear del siguiente listado:

LISTADO DE SITIOS PARA BLOQUEAR EN LAS APLICACIONES DE CONTROL PARENTAL:

4everproxy

5mins

alltheinternet

animeflv

anoox

aol

archive

ask

baidu

bandsalatmedien

becovi

biglobe

bing

blockaway

brave

croxyproxy

daum

discord

discoverresultsfast

dogpile

dontfilter

dr-gerhard-schmidt

duckduckgo

ecosia

egerin

elastic

elasticsearch

exalead

excite

fireball

free-proxy

free-proxy-list

freejobservices

freeproxyunblockyoutube

futtergold

genmirror

geonode

gibiru

gigablastsearchengine

gmx

goo

hide

hidefrom

hidemyass

hotbot

infinitysearch

k3nko

karmasearch

knaben

kproxy

kurek-remonty

leit

lycos

metacrawler

metager

meyer-cuxhaven

mirrorbay

modnyapartament

mojeek

my-proxy

myiphide

najdi

nate

naver

neo1973-germany

nihilisten-berlin

onion

opensearch

oscobo

panda-search

pc-service-beverstedt

petalsearchengine

pilpilidis

pirate-proxy

piratebay

piratehaven

plainproxies

planschguide

proxfree

proxsei

proxy

proxy-123

proxy-youtube

proxybay.pages.dev

proxyboost

proxyium

proxynova

proxypx

proxysite

qmamu

qwant

rambler

searchencrypt

seznam

skynetcloud

smart-c-a-e-solutions

sogou

startpage

steganos

sup-to-go

super-satelita

swisscows

t-pb

thegpm

thepiratebay

thepiratebaye

tpb

tpb-proxy

tpb-visit

ukpass

unblock-websites

unblockproxy

unblockvideos

unblockyoutube

urban-vpn

vpnbook

vpnproxy

walla

webcrawler

weboproxy

webproxy

webshare

wirtschaftsmedienberatung

yacy

yahoo

yandex

yep

yippysearchengine

yongzin

youdao

IMPORTANTE: **Desde Educación Digital Responsable, entendemos que la opción más óptima para evitar el acceso a contenido inapropiado sería una combinación de los pasos que se indican en este manual, es decir, un filtrado dns en un segundo router (no solo en el router del operador)y una aplicación de control parental donde se añadiría el listado de webs indicado anteriormente a las cuales se les bloquearía su acceso**

NOTA FINAL

Ante cualquier duda pueden mandarnos un mail para resolver cualquier inconveniente que puedan encontrar en la configuración, o dejando algún comentario en nuestra web www.educaciondigitalresponsable.org

EDUCACIÓN DIGITAL
RESPONSABLE

EDUCACIÓN DIGITAL
RESPONSABLE

También pueden encontrar información detallada en de toda esta información en la página web cibertutor.org donde realizan cursos y talleres específicos y gratuitos explicando la configuración de filtrado dns.

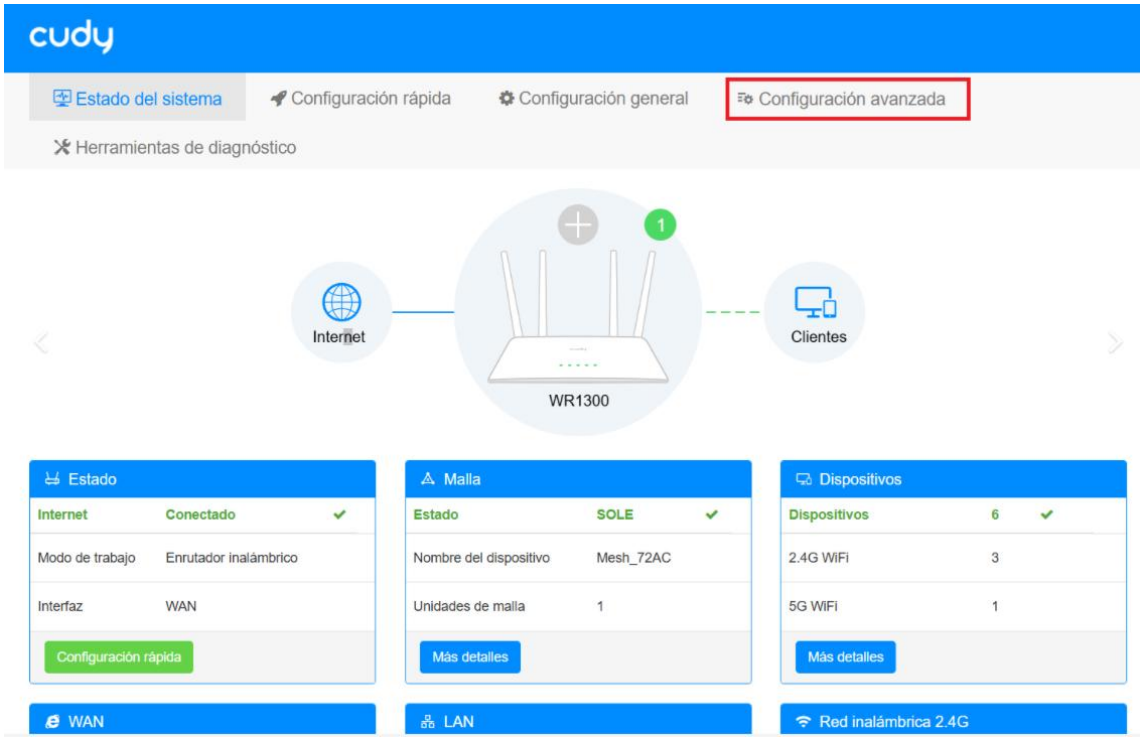
ANEXO1: Configuración de segundo router (en este ejemplo **Cudy WR1200**)

Para evitar que se puedan saltar el filtrado DNS cambiándolas directamente en el dispositivo final (móvil, tablet, pc, etc...) debemos instalar y configurar un segundo router que obligue a todos los dispositivos a usar las DNS que tenga configuradas, es decir, que ofrezca la opción de **FORZAJE DE DNS**. Esto no sucede en los routers de los operadores tradicionales ya que no permiten esa configuración, y por ese motivo que debemos introducir un segundo router.

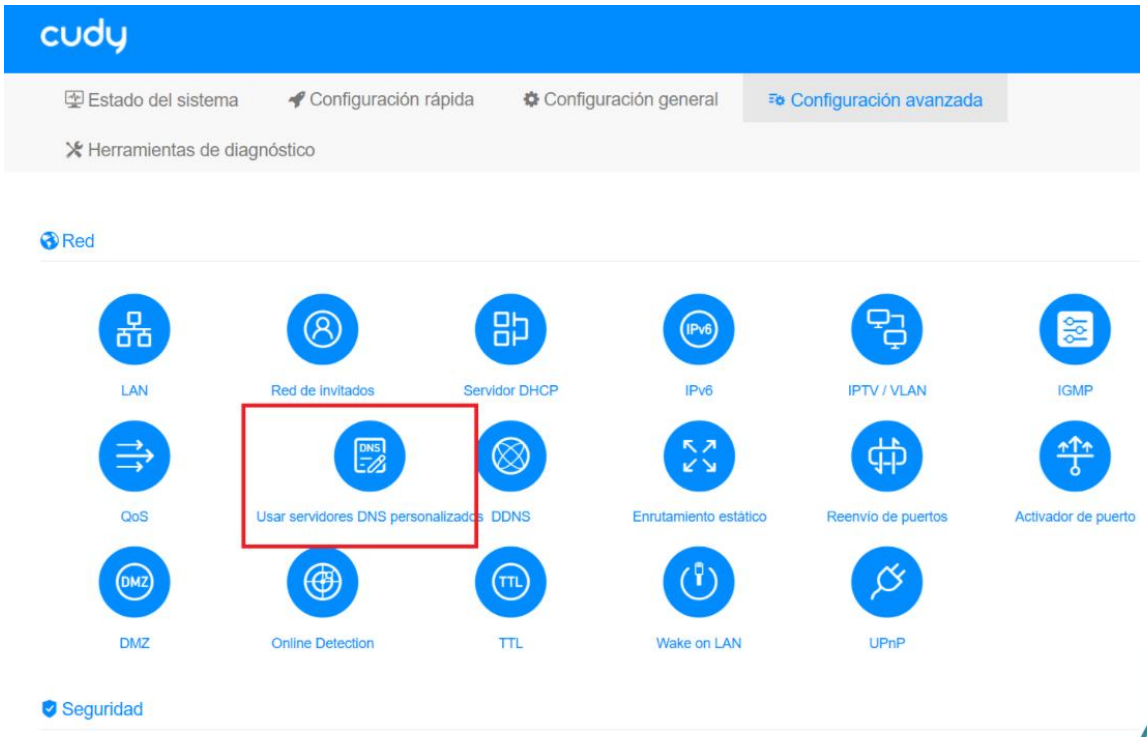
Este segundo router se conectará al de nuestro operador con un cable de red desde una de las tomas ethernet amarillas en el router del ejemplo de Movistar, a una de las tomas ethernet azules en el router Cudy como se muestra en la siguiente imagen (se usa como ejemplo un router del operador Movistar y como segundo router el Cudy WR1200):

Una vez realizada esta conexión el siguiente paso será configurar la wifi y las DNS en el router Cudy.
Para ello accederemos en un navegador web a la siguiente dirección:
http://cudy.net o a la dirección http://192.168.10.1
Usaremos la contraseña **admin** para iniciar la sesión

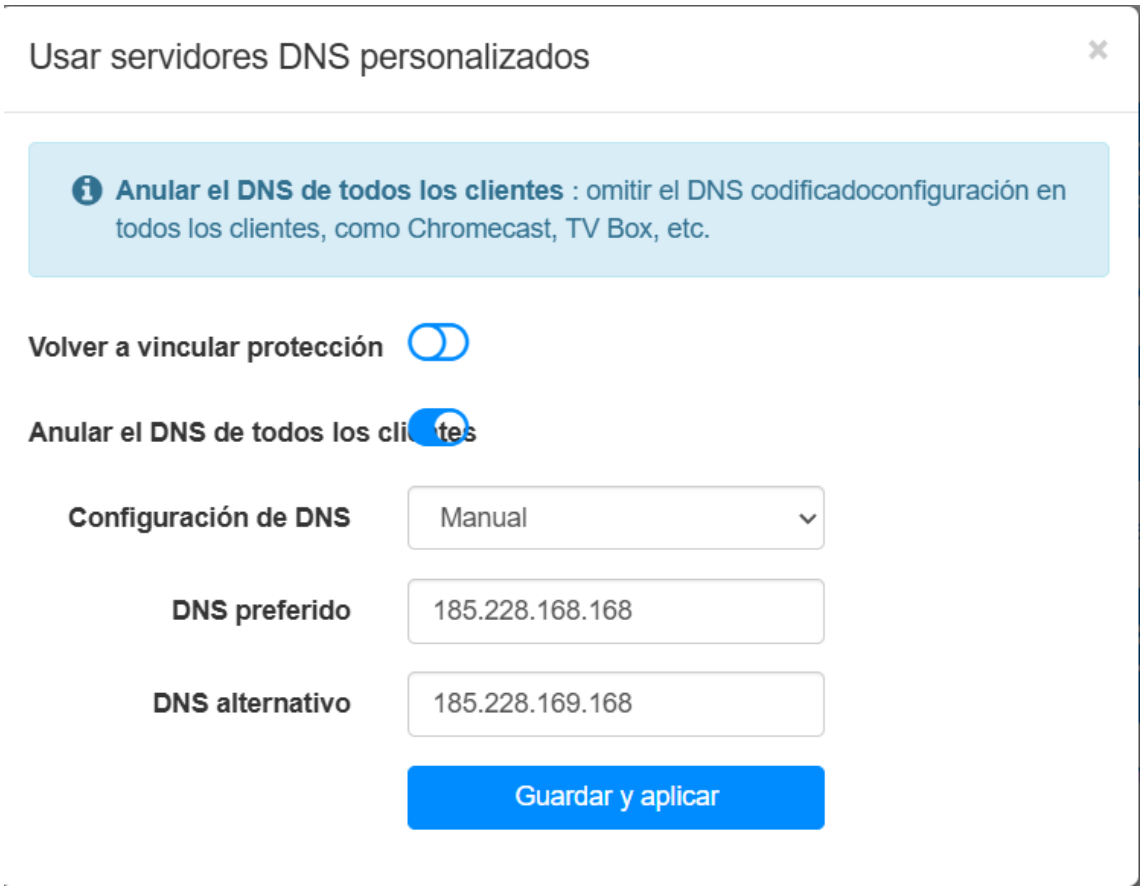
Esto nos permitirá acceder a la pantalla de inicio de configuración del router Cudy



Dentro de esta pantalla accederemos al menú “Configuración avanzada” (marcado en un recuadro rojo)
Esto nos llevará a la siguiente pantalla de configuración donde deberemos seleccionar la opción “usar servidores DNS personalizados” (marcado con un recuadro rojo).



Esto nos abrirá una nueva ventana emergente donde seleccionaremos la opción “anular el DNS de todos los clientes” y donde también introduciremos los servidores DNS seguros, en nuestro caso hemos introducido los de Cleanbrowsing 185.228.168.168 y 185.228.169.168.



Tras esto pulsaremos en “Guardar y aplicar”.

Con esto habremos conseguido configurar unas DNS seguras y además forzaremos a que todos los dispositivos que se conecten a nuestra usen esas DNS seguras, por tanto si a alguno de esos dispositivos alguien les modificase las DNS el router Cudy le obligaría a seguir navegando por internet con las DNS seguras de Cleanbrowsing en este caso.