GUÍA · GUÍA · GUÍA · GUÍA

TU ROUTER

TU CASTILLO

Aprende a ***configurar tu router de forma segura*** paso a paso

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
OSI Oficina de Seguridad del Internauta

Índice

1. El router: La puerta de entrada a Internet

El router es el dispositivo que nos permite conectarnos y navegar por Internet. Configurarlo de manera correcta evitará, en gran medida, que alguien sin permiso utilice nuestra Red e invada nuestra privacidad y seguridad.

Todos los router cuentan con un menú de configuración para modificar los parámetros que vienen por defecto y que, en muchos casos, no son lo suficientemente seguros.

Por tanto, revisar la configuración del router es una de las tareas más importantes que debemos llevar a cabo para proteger nuestros dispositivos, la información que contienen, así como la información que intercambiamos en las distintas comunicaciones que mantenemos con terceros a través de Internet.

Por todo ello, hemos preparado esta guía con la que podremos ponernos manos a la obra y seguir paso a paso las configuraciones más básicas recomendadas.

Si queremos navegar de forma segura, ¡protejamos primero nuestro router!

1.1 Aspectos físicos del router

A continuación, listamos los diferentes componentes externos del router con los que te tienes que familiarizar.

1. Entrada para la corriente: permite al router conectar su fuente de alimentación con la corriente eléctrica. Un fallo aquí significaría que el router no puede encenderse.

2. Interruptor de alimentación: se trata del botón de encendido y apagado. Aunque el router permanece casi siempre encendido, es recomendable apagarlo si no vamos a utilizarlo durante un tiempo, por ejemplo, si nos vamos de vacaciones o de fin de semana.

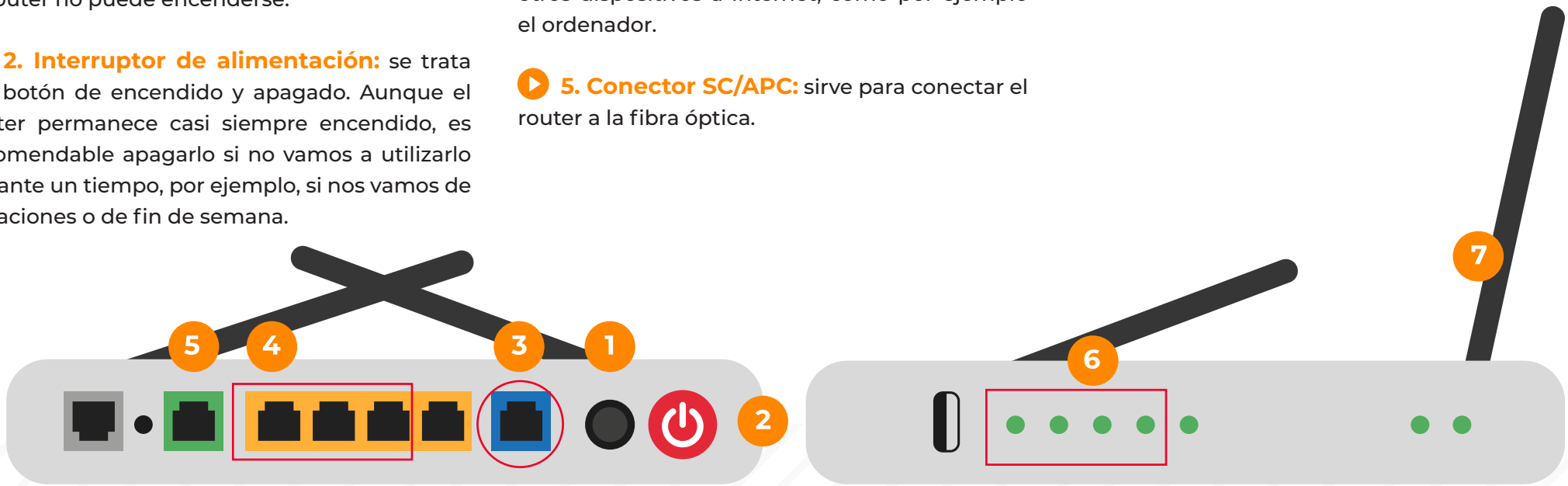
3. Conector WAN: es el acceso en el que conectaremos el cable de nuestro operador de Internet. Suele ser un cable de color amarillo.

4. Conector LAN: suelen venir varios conectores LAN en la parte trasera de nuestro dispositivo. A través de esta entrada, podrás conectar los cables de red con los que conectar otros dispositivos a Internet, como por ejemplo el ordenador.

5. Conector SC/APC: sirve para conectar el router a la fibra óptica.

6. LEDs: luces que sirven como indicadores para saber si la wifi está conectada y verificar que todas sus funcionalidades están correctamente.

7. Antena: muchos routers cuentan con antenas para emitir la red wifi.



Img 01. Aspectos físicos del router

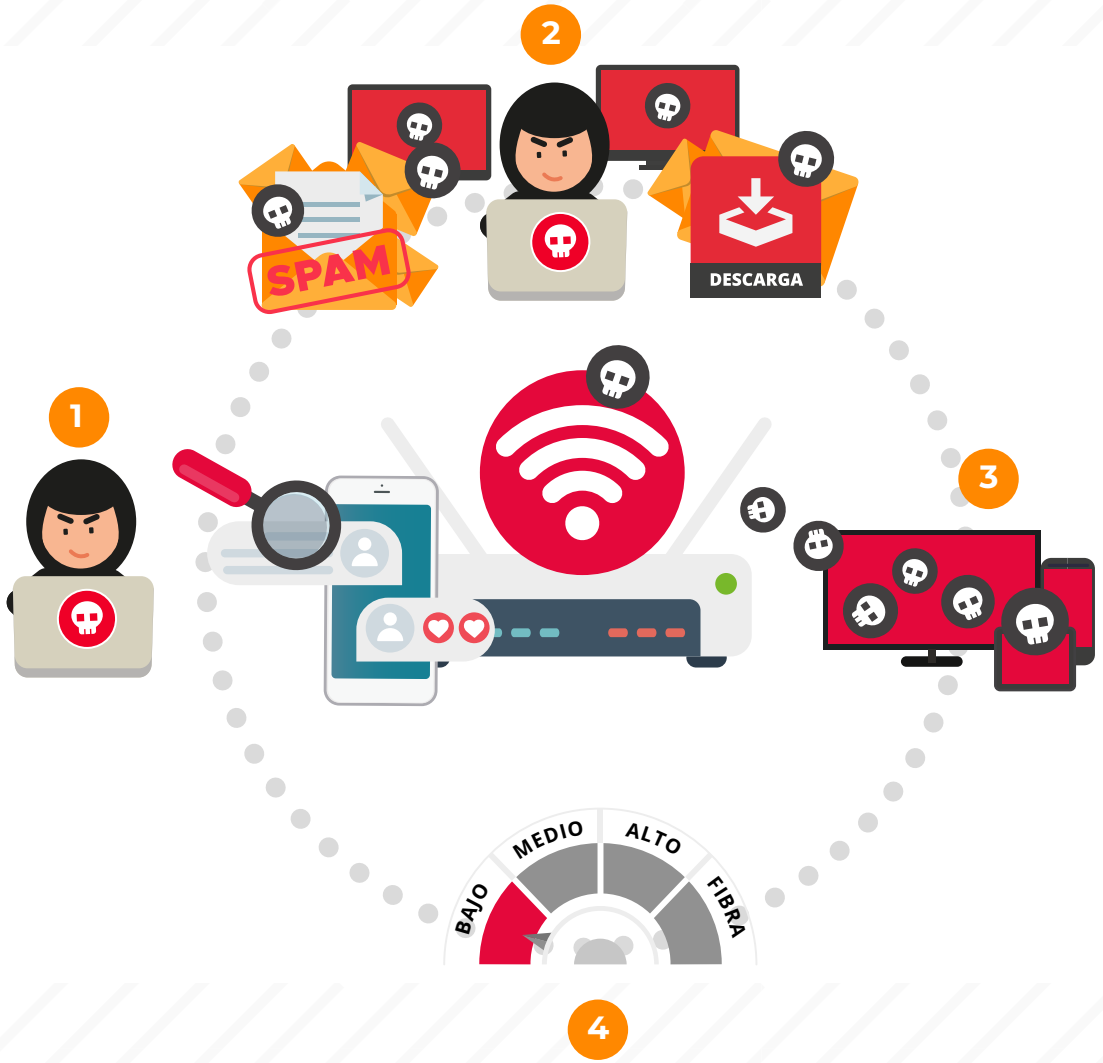
2. Principales amenazas a nuestro router

Un router que no ha sido correctamente configurado podría permitir que terceros se conecten a nuestra red y amenacen nuestra seguridad y privacidad de la siguiente forma:

- **1. Espiando nuestras comunicaciones** (ataque man in the middle).
- **2. Utilizando la red para envío de spam**, realizar ataques DoS (denegación de servicio), descarga de contenido ilegal, etc.
- **3. Infectando los dispositivos conectados** con *malware*.
- **4. Reduciendo el ancho de banda.**

Sabiendo todo lo que un atacante puede hacer desde nuestra red es importante que la protejamos de manera correcta.

¿Comenzamos?



3. Cómo acceder a la configuración de nuestro router

Cada router es un mundo y la interfaz, así como la disposición de sus apartados y opciones de configuración puede cambiar de un modelo a otro.

Por tanto, los pasos que encontraremos a continuación son genéricos y orientativos, si difieren de nuestro router considerablemente o no los encontramos, te recomendamos contactar con el proveedor de servicios de Internet contratado o el fabricante del router.

En cualquier caso, desde **INCIBE** ponemos a tu disposición la ***Línea de Ayuda de Ciberseguridad,*** el número de **teléfono 017,** totalmente gratuito y confidencial.

¡Llámanos si tienes dudas!

TU AYUDA EN
CIBERSEGURIDAD

incibe_

3.1 Conocer nuestra dirección IP

La forma más sencilla de acceder a las opciones de configuración del router es:

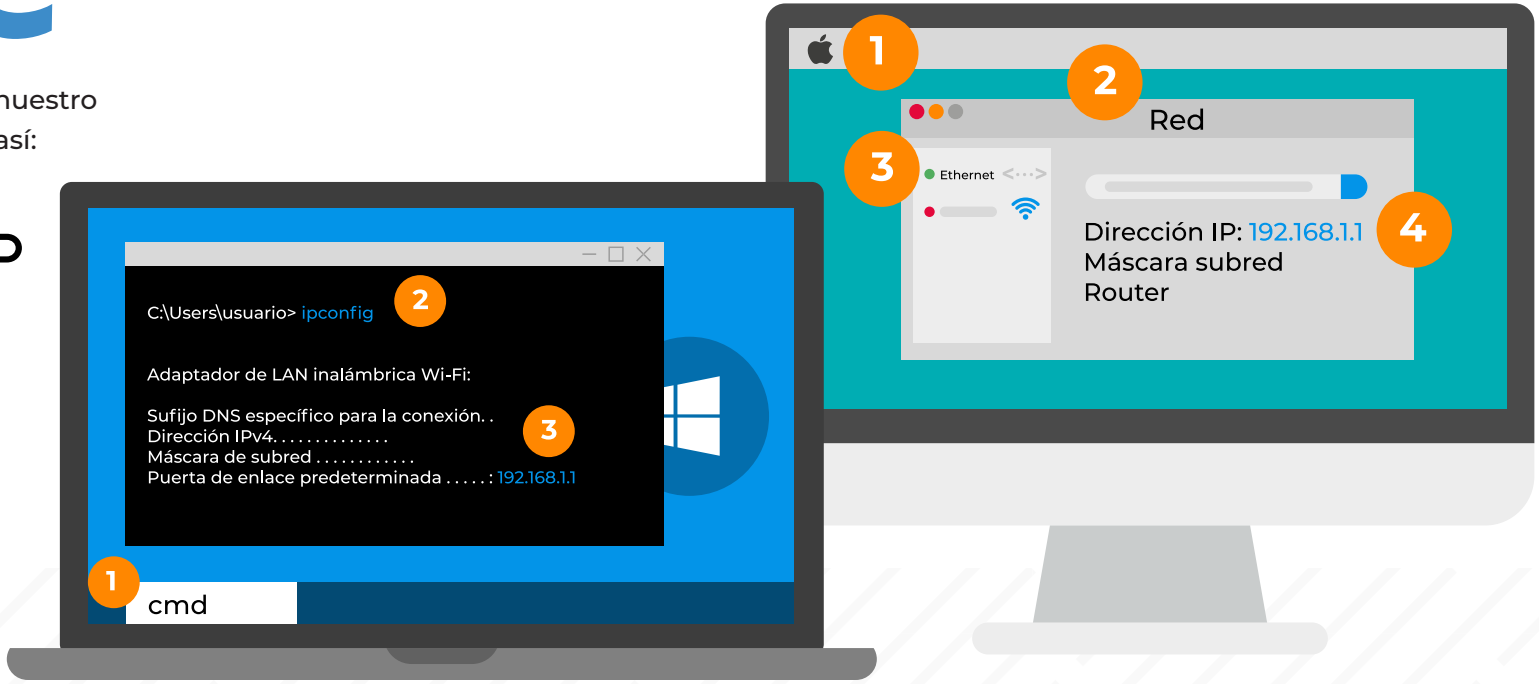
Abrir el navegador.

Introducir la dirección IP de nuestro router. Para conocerla, podemos hacerlo así:

Desde Windows, abriremos una ventana de MS-DOS o escribiremos "***cmd***" en el buscador de Windows *(1)*. A continuación, teclearemos "***ipconfig***" (sin las comillas) *(2)* y buscaremos la dirección que aparece junto a ***Puerta de enlace predeterminada*** *(3)*.

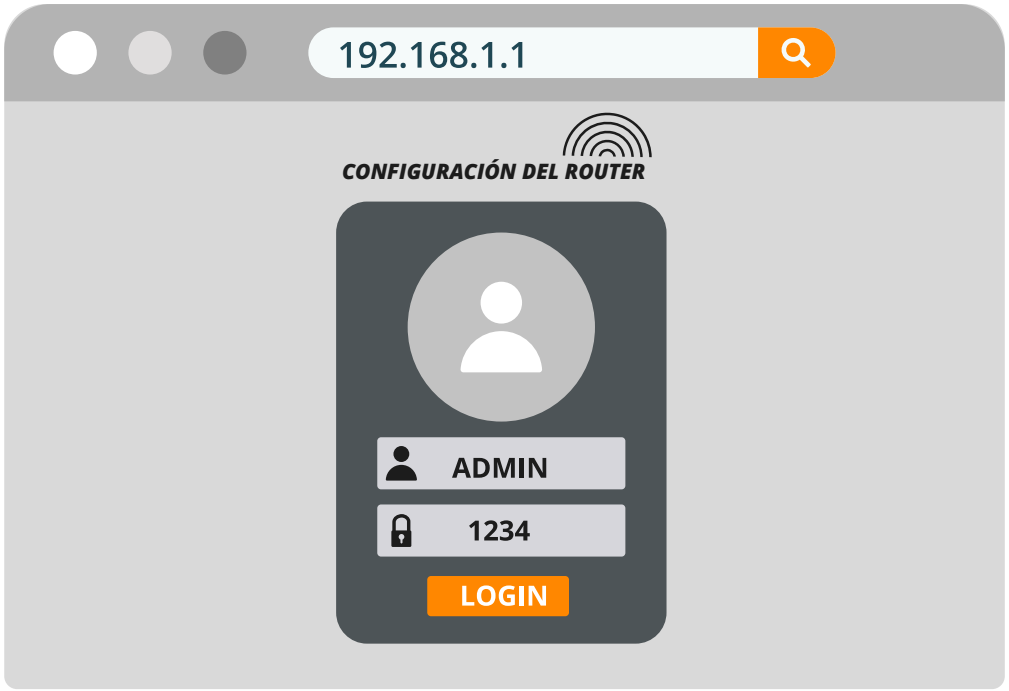
Suele ser: 192.168.1.1

Desde Mac, haremos clic en el icono de Apple *(1)* y seleccionaremos 'Preferencias del sistema'. Luego, iremos a Red *(2)* y seleccionaremos nuestra conexión (AirPort o Ethernet) *(3)*. Junto a ella aparecerá nuestra dirección IP *(4)*.



Img 02. Conoce tu IP en Windows y Mac

Una vez ingresemos nuestra dirección IP en el navegador y pulsemos intro, nos aparecerá una ventana similar a la siguiente.



Img 03. Acceso a la configuración del router

Deberemos ***introducir las credenciales de acceso a nuestro router.*** En ocasiones, suelen venir escritas por defecto en el propio router, otras veces suelen ser genéricas, del tipo ***user: admin / password: admin*** ***user: admin / password: 1234.***

No obstante, podemos ponernos en contacto con nuestro proveedor de servicios de Internet, si tenemos dudas o la desconocemos.

Img 04. Etiqueta de credenciales del router

3.2 | Primer vistazo al menú

Una vez hayamos ingresado nuestras credenciales, veremos la interfaz del menú de configuración de nuestro router.

Aunque los proveedores de servicios de Internet ofrecen un diseño propio y los elementos del menú pueden variar, en líneas generales, contienen opciones y apartados similares.

Mi red local: opción que permite comprobar en tiempo real los dispositivos conectados a Internet a través de nuestro router. También suelen mostrar los dispositivos que se han conectado al router, pero que actualmente están desconectados.

Wifi: este apartado nos proporcionará toda la información relacionada con la red wifi como la red principal, su estado, nombre, clave y protocolo de seguridad.

Información y diagnóstico: nos proporciona información del estado de las distintas funciones y servicios del router como Internet, teléfono, la red wifi, la alimentación, etc. A su vez, podemos comprobar los parámetros del sistema para conocer los datos del tipo de router, su número de serie y otros datos técnicos.

Entre las opciones que podemos configurar, encontramos:

- ***Copia de seguridad:*** para crear una copia de respaldo de la configuración del router.
- ***Reinicio:*** para reiniciar el router y con ello, la conexión a Internet.
- ***Reinicio a valores de fábrica:*** permite borrar todos los parámetros y devolver el aparato al estado inicial de fábrica.
- ***Actualización de software:*** para comprobar si existen nuevas versiones del *firmware* de nuestro router.

Configuración avanzada: este apartado nos permite llevar a cabo configuraciones para distintas funcionalidades de nuestro router:

- ***Configuración de la red:*** configurar el servidor DHCP, DNS, UPnP o DMZ entre otros.
- ***Configuraciones de firewall:*** modificar el nivel de protección de nuestro router. Los distintos niveles ampliarán o disminuirán los requisitos del filtro para descartar determinadas conexiones.
- ***Acceso remoto al router:*** opción que permite acceder de forma remota a la configuración del router mediante el servicio DynDNS y unas credenciales de acceso.
- ***Administración:*** configurar las opciones de administración del router, como son las credenciales de acceso al mismo.
- ***Notificaciones por email:*** configuración del envío de notificaciones a nuestro correo electrónico de determinados eventos que sucedan en nuestro router, como la conexión de

un nuevo equipo o una nueva dirección IP.
Una vez estemos familiarizados con los distintos apartados y secciones de la interfaz, podremos comenzar a realizar las modificaciones en nuestro router. ***Las posibilidades son muchas, pero nos centraremos en aquellas configuraciones que nos ayuden a aumentar la seguridad de nuestro router y de los dispositivos conectados a la red.***

Img 05. Acceso al router

3.3 Actualizaciones

El router es uno de los dispositivos más importantes que tenemos bajo nuestro control.

Sin embargo, apenas le prestamos atención, especialmente en lo que a seguridad se refiere. En muchas ocasiones, dejamos de lado las medidas básicas de seguridad que llevamos a cabo en otros dispositivos, como son las actualizaciones.

Pueden surgir vulnerabilidades o brechas en la seguridad en el *firmware* del router que son resueltas mediante parches o actualizaciones de seguridad. El *firmware* es lo que permite gran parte de las funciones de Internet, es como el sistema operativo del router.

- Comenzaremos desde el ***menú de configuración de nuestro router.***
- Luego, accederemos al apartado de ***Información y diagnóstico > Actualización de software.*** En algunos modelos deberemos buscar la función ***"Actualización o Actualización del firmware",*** en ***Opciones avanzadas*** o ***Información sobre el router.***
- Una vez hagamos clic, se nos informará de si el dispositivo está ya actualizado a la última versión, o nos proporcionará una opción para hacerlo.
- Conviene entrar de vez en cuando a la opción para llevar a cabo esta comprobación y prevenir posibles brechas en la seguridad de nuestra conexión a Internet.

Img 06. Actualizaciones

4. Cambiar la contraseña por defecto

Por norma general, los router vienen protegidos con unas credenciales de acceso para evitar que usuarios no autorizados puedan acceder a nuestro dispositivo y llevar a cabo modificaciones sin nuestro consentimiento.

Del mismo modo, la red wifi también dispone de unas credenciales por defecto que pueden aportar más información de la que quisiéramos a un ciberdelincuente.

Si nunca hemos cambiado las credenciales de acceso, es recomendable que lo hagamos lo antes posible, ya que suelen usarse unas ***contraseñas muy débiles por defecto***.

Ejemplos de contraseñas utilizadas para acceder al router:

- ***admin***
- ***1234***
- ***1234admin***
- ***12341234***
- ***123456***

Si alguna de estas contraseñas coincide con la nuestra, deberemos cambiarla lo antes posible.

4.1 Credenciales por defecto del router

Para cambiar las credenciales de acceso a la configuración de nuestro router, deberemos acceder de nuevo al menú de configuración y buscar las opciones de Administración u Opciones avanzadas.

- En el ejemplo que mostramos, accederemos a ***Configuración Avanzada > Administración.***
- Dentro del apartado, aparecerán los pasos a seguir para ***crear una nueva contraseña.***

Es fundamental que utilicemos una contraseña lo suficientemente robusta para proteger el acceso a la interfaz de configuración de nuestro router:

- ***Entre 8 y 10 dígitos.***
- ***Combinar*** letras, números, mayúsculas, minúsculas y caracteres especiales.
- ***Cambiar*** las credenciales ***cada cierto tiempo*** (3-6 meses).
- ***Utilizar un gestor de contraseñas*** para almacenar todas nuestras credenciales.

Img 07. Cambio credenciales

4.2 Credenciales por defecto de la red wifi

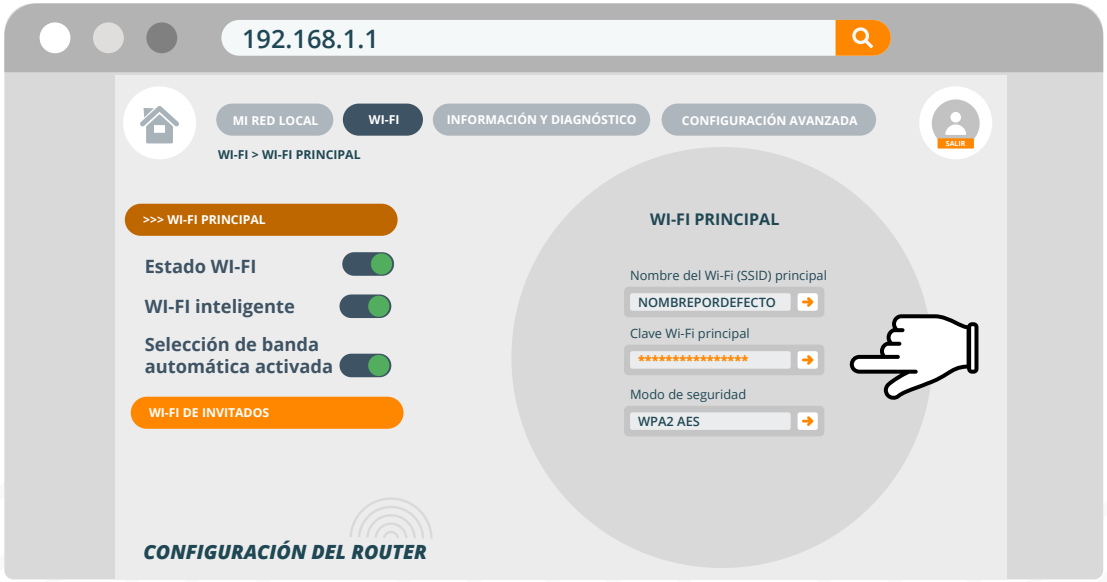
Una vez que conectamos por primera vez nuestro router y comenzamos a emitir una red wifi, esta también viene con un nombre o SSID y una contraseña por defecto.

En concreto, el SSID que viene por defecto (nombre de la red) puede aportar información muy útil a cualquier ciberdelincuente, como quién es nuestro operador o incluso el modelo del router. Por ello, como medida de seguridad adicional, es conveniente que actualicemos esta información, especialmente la contraseña de acceso.

Los pasos para cambiar la contraseña de nuestra red wifi son muy sencillos e intuitivos. De forma general, deberemos buscar el apartado de ***Wifi o Redes*** de nuestro ***menú de configuración***. En nuestro router de ejemplo, deberemos acceder al menú de configuración y seguir los siguientes pasos:

- Buscaremos el apartado de ***Wi-Fi.***
- Una vez dentro, se nos mostrarán todos los ***parámetros y datos de nuestra red wifi***, como su estado, las credenciales, así como el ancho de banda.
- Localizaremos la opción de ***Clave Wi-Fi principal.***
- La sustituiremos por una ***contraseña nueva*** que cumpla con los parámetros de contraseña robusta.
- Una vez cambiado, tendremos que hacer clic en la opción de ***Guardar***.

Es probable que, tras cambiar la contraseña de nuestra red wifi, ***el router necesite reiniciarse y aquellos dispositivos que estaban conectados a la red***, deban reconectarse introduciendo la nueva contraseña como medida de seguridad.

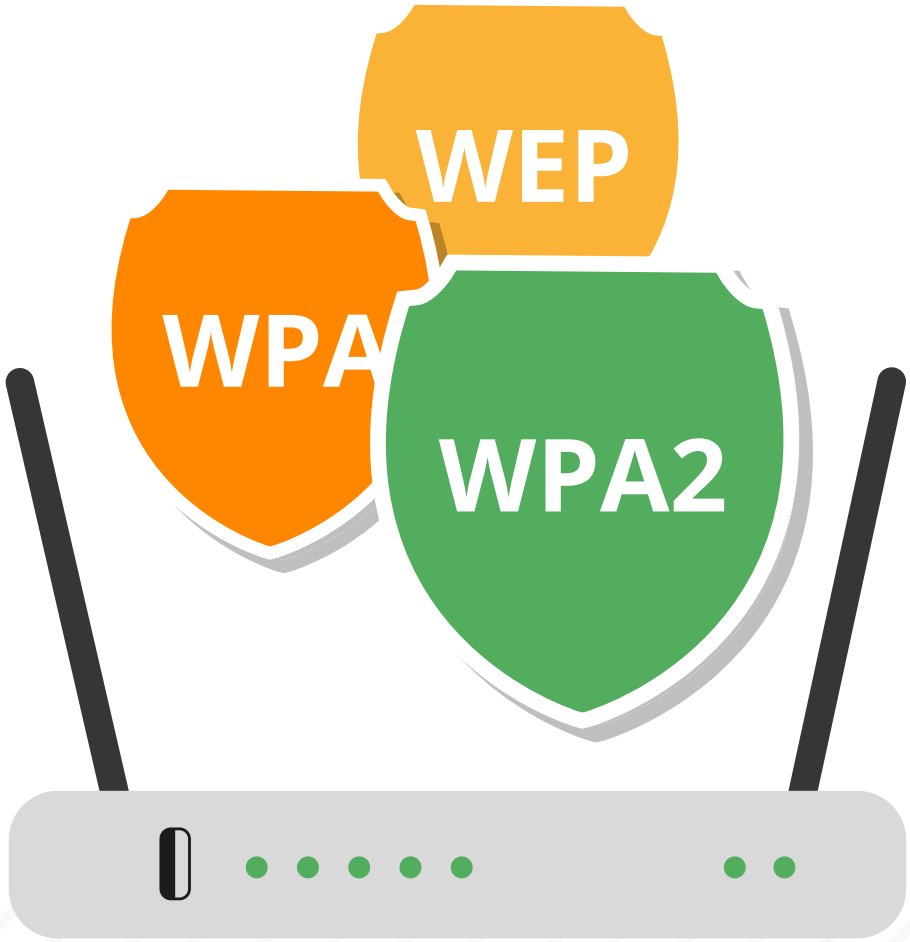


Img 08. Cambio clave Wi-Fi

5. Asignar el mejor protocolo de seguridad

Cuando utilizamos una conexión inalámbrica, como es la red wifi, el cifrado de la información que se envía y recibe a través de esta es algo imprescindible para evitar que terceros puedan llegar a monitorizar nuestra actividad.

Si no contamos con un protocolo avanzado y suficientemente seguro, cualquier ciberdelincuente lo suficientemente hábil podría llegar a interceptar estas comunicaciones y modificar, eliminar o robar la información que desee.



A día de hoy, no existe un protocolo que sea 100% eficaz, sin embargo, si podemos recurrir a algunos tipos que han superado las vulnerabilidades de los modelos más antiguos y que a día de hoy si ofrecen una capa extra de seguridad a nuestras comunicaciones:

Sin cifrado o red wifi abierta: este tipo de redes son comunes en los espacios abiertos y públicos como cafeterías, centros comerciales u hoteles. No ofrece protección ninguna y permite que cualquiera pueda conectarse y capturar los paquetes de datos que intercambien los usuarios de dicha red. Por ello, no es recomendable configurar nuestra red sin cifrado, ni conectarse a una red abierta.

Img 09. Protocolo seguridad

WEP: uno de los primeros protocolos de cifrado diseñados para proteger las comunicaciones de las redes inalámbricas. Actualmente, se trata de un protocolo obsoleto que ofrece una seguridad muy débil y no es recomendable para nuestra red.

WPA: sistema de cifrado que se utilizó después de WEP, pero que también se demostró que es vulnerable y por eso a día de hoy no es recomendable su uso.

WPA2: funciona bajo la misma premisa que el protocolo WPA, pero mejorando algunas vulnerabilidades, haciéndolo más seguro. A día de hoy es la opción más recomendable a utilizar para proteger nuestra red.

Los protocolos WPA y WPA2 pueden llegar a utilizar dos tipos de cifrado diferentes para las contraseñas de acceso a la red. Estos tipos de

cifrado son el TKIP y AES. Si buscamos mejorar la seguridad de nuestra red deberemos elegir el tipo AES. Por tanto, dentro de la configuración de nuestro router, cuando queramos configurar nuestra red wifi seleccionaremos el protocolo de cifrado ***WPA2/AES.***

Finalmente, mencionar que hay un nuevo protocolo de cifrado, pero que aún no está disponible en todos los routers. Se trata del ***WPA3*** y busca resolver los problemas de seguridad que en los últimos años han comenzado a aparecer dentro del WPA2. Si nuestro router dispone de él, lo seleccionaremos.

5.1 Cómo cambiar el protocolo de seguridad

Para llevar a cabo el cambio en el protocolo de cifrado, nos dirigiremos al ***menú de configuración de nuestro router:***

- Buscaremos el apartado de ***Redes wifi o Redes.*** En algunos router estos apartados pueden ser distintos, como Conexiones inalámbricas, *Wireless* o *Network*.
- Seleccionaremos la ***red wifi principal*** y buscaremos entre los parámetros el ***modo de seguridad o protocolo de cifrado.*** En el desplegable, seleccionaremos el protocolo ***WPA2/AES.***

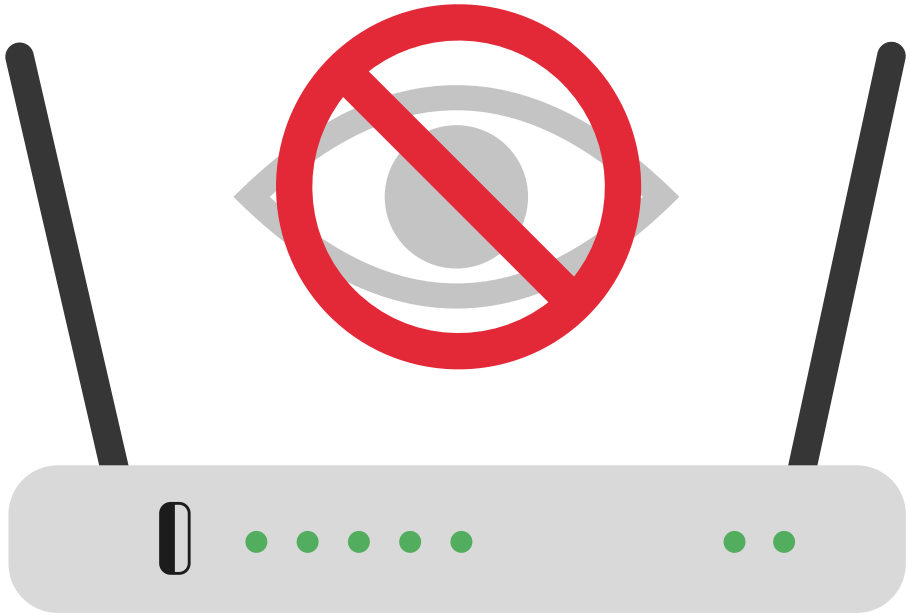
Estos pasos pueden variar de un router a otro, pero las opciones de configuración para el protocolo de seguridad estarán junto a las opciones de nuestra red wifi.

Img 10. Cambio de protocolo

6. Cambiar u ocultar el nombre de la red o SSID

Cuando modificamos las credenciales de acceso a nuestro router o a nuestra red wifi, estamos protegiéndolos de terceros evitando que puedan acceder a ellos. Para aumentar aún más la protección de nuestra red, es recomendable que cambiemos el nombre de nuestra red wifi (SSID).

El problema reside en que los nombres con los que suelen identificarse por primera vez las redes wifi poseen información sobre el proveedor del servicio de Internet.



Un atacante lo suficientemente hábil podría buscar información sobre cómo acceder al panel de administración, credenciales habituales o vulnerabilidades con los que aprovecharse y acceder al dispositivo para luego llevar a cabo las modificaciones que quiera o robar información fácilmente.

Para cambiar el nombre de la red, deberemos:

- Acceder al ***menú de configuración de nuestro router.***
- A continuación, nos dirigimos a la sección Wifi. En algunos modelos puede denominarse ***Wireless o Conexiones.***
- Una vez dentro, buscaremos entre los parámetros de configuración el nombre de la red wifi principal o SSID. Finalmente, ***seleccionaremos un nuevo nombre para la red.***

Una recomendación es utilizar un nombre aleatorio o que no pueda vincularse con nosotros o nuestro proveedor de Internet.

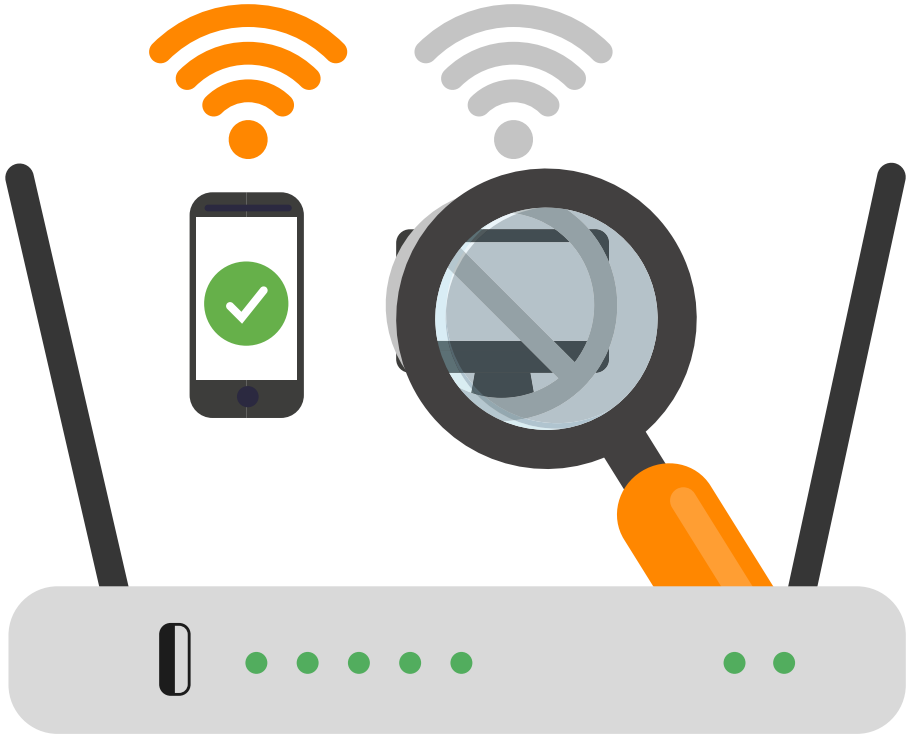
La mayoría de router ofrece una configuración añadida para ***ocultar el nombre de la red wifi.*** Esto es una medida para ***evitar que terceros traten de conectarse a nuestra red.*** Al marcar la opción de ocultar el nombre de la red wifi, ***los programas para detectar redes disponibles no mostrarán nuestra conexión.*** En cualquier caso, no se trata de una medida de seguridad.

Img 11. Cambiar/ocultar SSID

7. Filtrar las direcciones MAC

Una práctica muy útil para mejorar la seguridad de nuestra conexión y protegerla de terceros es revisar eventualmente los dispositivos que están conectados a nuestra red y realizar un filtrado por dirección MAC, que es un identificador único que posee cada dispositivo.

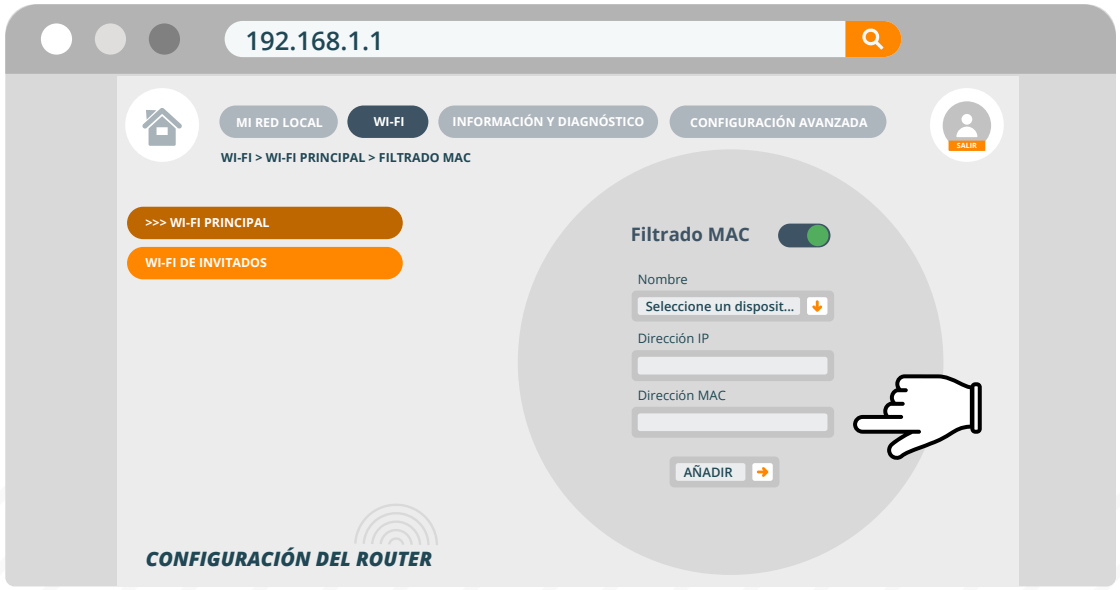
De esta forma, habilitaremos el acceso solo a aquellos dispositivos que conocemos y evitaremos que se conecten dispositivos desconocidos.



Para utilizar esta funcionalidad, deberemos acceder a las opciones de nuestra red wifi. Para ello, entraremos en las ***opciones de configuración*** de nuestro router.

- Buscaremos el apartado de ***redes Wi-Fi o Redes.*** En algunos router estos apartados pueden ser distintos, como ***Conexiones inalámbricas, Wireless o Network.***
- Accederemos a nuestra red wifi principal y ***buscaremos la función de Filtrado MAC.*** Al activarlo, podremos crear un listado de dispositivos a los que permitiremos conectarse a nuestra red. Para ello, ***deberemos introducir sus direcciones MAC en el filtro y hacer clic en guardar.***

Más adelante explicaremos como obtener la dirección MAC de un dispositivo.



Img 12. Filtrado MAC

7.1 Comprobar dispositivos conectados

Existen varias formas de comprobar si tenemos un 'invitado' en nuestra red, y pueden variar dependiendo del modelo de nuestro router. En cualquier caso, prácticamente todos disponen de una opción para visualizar los dispositivos conectados a la red en tiempo real.

En el ejemplo que hemos seleccionado para nuestra guía esta opción está disponible desde el menú principal de ***configuración*** de nuestro router. Sin embargo, en otros modelos es posible que se localice dentro de las ***opciones de nuestra red wifi.***

Debemos realizar una ***comprobación de los dispositivos conectados cada cierto tiempo*** e identificar aquellos que sean de confianza y cuáles son desconocidos, para en este último caso, tomar las acciones que se consideren necesarias, como, por ejemplo, bloquearlos.

Img 13. Comprobar dispositivos conectados

7.2 Cómo obtener direcciones MAC en dispositivos Windows

- Accederemos a un intérprete de comandos ***MS-DOS***, o escribiendo ***"cmd"*** *(1)* en el buscador del sistema operativo.
- A continuación, escribiremos ***"ipconfig /all"*** *(2)* (sin las comillas).
- Una vez aparezcan todos los parámetros, buscaremos en el apartado ***dirección física*** *(3)* la ***dirección MAC de nuestro dispositivo.***

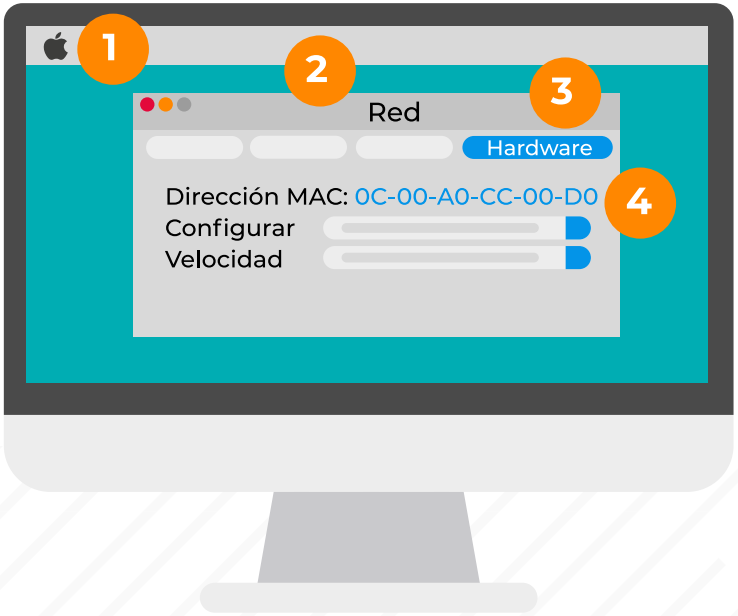
Img 14. Dirección MAC en Windows

7.3 Cómo obtener direcciones MAC en dispositivos macOS

- Abriremos ***Preferencias del sistema*** *(1)* haciendo clic en el icono de la manzana de Apple situada en la esquina superior izquierda de la pantalla.
- Seleccionaremos ***Redes*** *(2)* ***> AirPort o Ethernet*** (según como nos conectemos a Internet).

Si la conexión es Ethernet, haremos clic en el botón de parte inferior ***Avanzado > Hardware*** *(3)*. En la parte superior aparecerá la dirección MAC *(4)*.

Si la conexión es AirPort, haremos clic en el botón de parte inferior ***Avanzado > Hardware*** *(3)*. En la parte superior aparecerá la dirección MAC *(4)*.



Img 15. Dirección MAC en MacOS

7.4 Cómo obtener direcciones MAC en dispositivos Android

- En varios modelos deberemos acceder a ***Ajustes > Acerca del teléfono > Estado.*** Aquí encontramos nuestra dirección MAC.
- En otros, abriremos el menú Configuración o ***Ajustes > Wi-Fi.*** Dentro buscaremos los ***Ajustes avanzados o ajustes adicionales.*** En las propiedades de la wifi aparecerá nuestra dirección MAC.

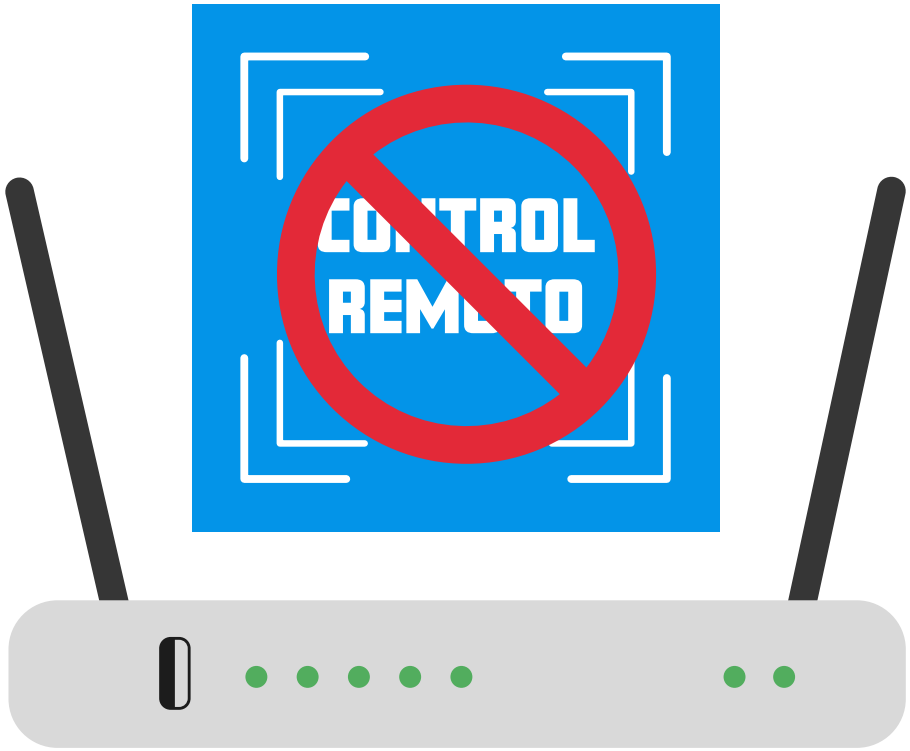
7.2 Cómo obtener direcciones MAC en dispositivos iOS

- Accederemos al ***menú de Ajustes*** de nuestro dispositivo.
- A continuación, ***buscaremos el apartado General,*** y dentro de este la opción de Información.
- En el campo de ***Dirección Wi-Fi*** encontraremos la dirección MAC.

Img 16. Dirección MAC en Android e iOS

8. Desactivar el acceso remoto

Si queremos evitar que se pueda entrar a nuestro router desde el exterior, es decir, desde otra red, tendremos que asegurarnos de que esta funcionalidad está desactivada.



- ***Accederemos a la configuración de nuestro router*** y buscaremos el apartado de ***Configuración avanzada*** (aunque puede variar según el modelo del router).
- ***Buscaremos la opción de Acceso remoto*** al router, aunque en algunos modelos puede estar dentro de los apartados ***Administración o Management Control.***
- Una vez dentro, podremos ***comprobar que la opción de Permitir el acceso remoto del usuario está desactivada.*** Es posible que en algunos modelos debamos buscar y ***deshabilitar la opción de WAN Access o Configuración de acceso remoto.***

Img 17. Acceso remoto

9. Desactivar el WPS o conexión rápida

Los router y sus configuraciones de seguridad han evolucionado mucho a lo largo de los años. La funcionalidad WPS, por ejemplo, es una funcionalidad que, si bien resultaba muy útil a la hora de conectar dispositivos a la red, a día de hoy puede suponer una gran amenaza contra nuestra seguridad y privacidad.

El WPS es un mecanismo creado para facilitar la conexión de dispositivos a nuestra red wifi. Aunque existen diversas formas mediante las cuales un dispositivo puede conectarse a una red inalámbrica utilizando, para ello, dicha funcionalidad, la más extendida de todas sigue siendo mediante una clave PIN.

Para conectarse, el dispositivo debe transmitir un ***código numérico*** (generalmente de 8 dígitos) al router. A cambio, el router le envía los datos necesarios para que el primero pueda conectarse a la red.

Aunque este código PIN suele venir escrito en alguna parte de nuestro router, generalmente en la parte inferior, el principal problema reside en que, al igual que ocurre con muchos otros datos, ***un atacante lo suficientemente hábil podría llegar a averiguarlo.***

Otras formas de conectarnos utilizando la funcionalidad WPS son:

- **NFC**, colocando el dispositivo cerca del router para intercambiar la información.
- **PBC**, pulsando simultáneamente los botones dedicados a esta función en el dispositivo y el router.
- **USB**, de forma física podremos conectar dispositivos a nuestra conexión.

9.1. Riesgos para la seguridad

A pesar de ser una funcionalidad muy útil para conectar un dispositivo de un modo mucho más rápido, no está exento de peligros y riesgos para nuestra seguridad.

El problema reside en ***cómo el router responde ante el ingreso de un PIN incorrecto.*** Una vez que se ha introducido una clave incorrecta, el router devolverá un mensaje indicando si la primera o segunda mitad de la clave es correcta o no. Un atacante podría ***probar distintas combinaciones hasta dar con la correcta fácilmente y en pocos minutos.*** Una vez conectado a nuestra conexión a Internet, no le costaría mucho empezar a interceptar los paquetes de información en nuestra red, por ejemplo.

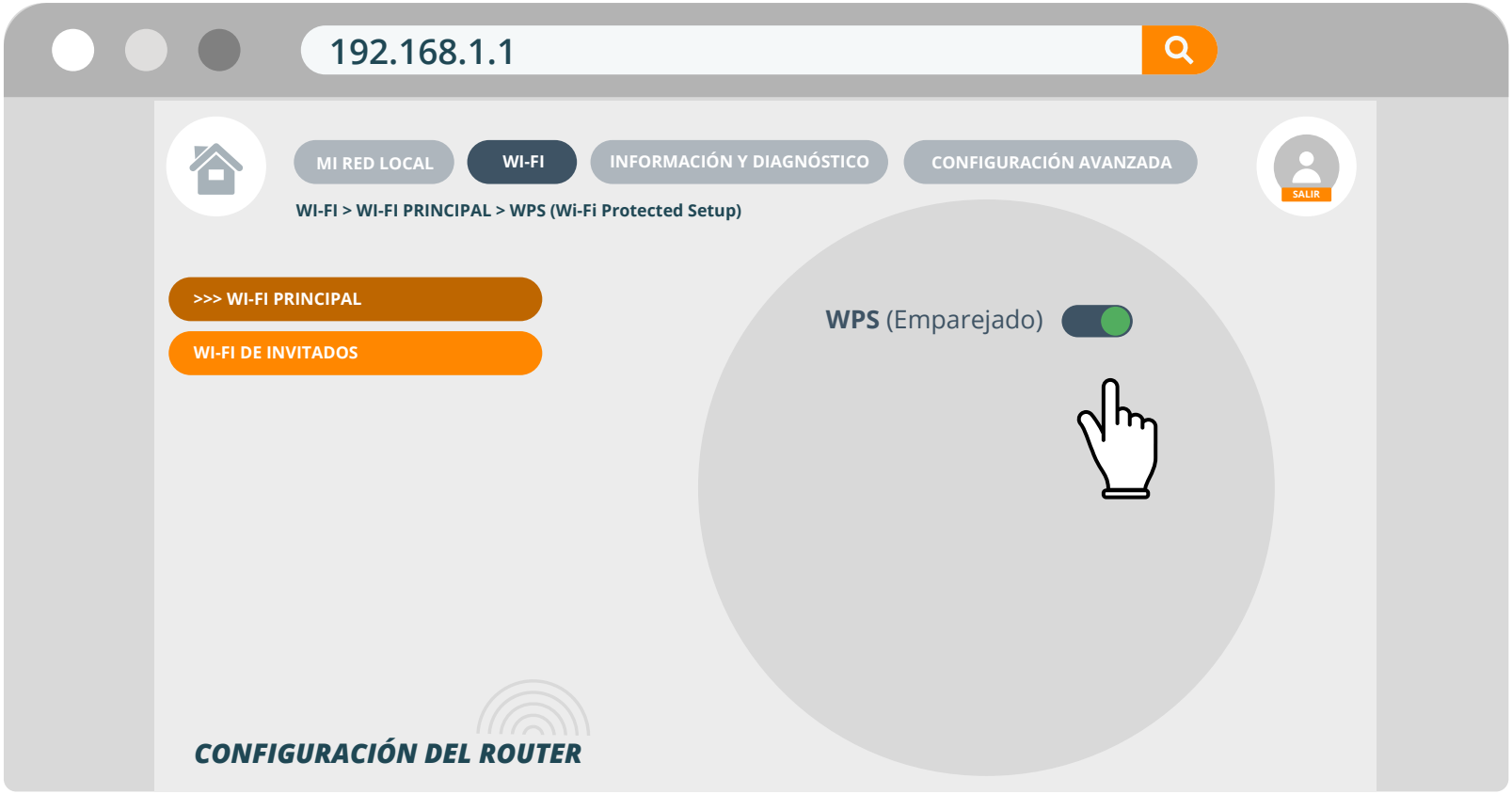
Para mantener nuestra red wifi segura, debemos ***renunciar a la comodidad de conectarnos mediante esta utilidad e introducir la contraseña WPA2 cada vez que queramos conectar un nuevo dispositivo a nuestra red.***

9.2 Cómo desactivar la función WPS

Para desactivar la funcionalidad ***WPS*** lo primero que deberemos hacer es:

- Ir a la ***configuración de nuestro router*** y localizar el ***apartado de Wi-Fi***. Una vez dentro, buscaremos nuestra red wifi principal. En algunos modelos de router deberemos acceder a los apartados de Conexiones inalámbricas, *Wireless* o *Network*.
- A continuación, buscaremos la opción de ***emparejado por WPS*** y haremos clic en ***Desactivar***.

En caso de que nuestro router no disponga de la opción para desactivar esta función, la mejor recomendación es ***evitar utilizarla lo máximo posible.***



Img 18. Desactivar/Activar WPS

10. Puertos del router

Los puertos del router se utilizan como un canal para establecer conexiones de diferentes aplicaciones con los correspondientes servidores remotos para poder funcionar. Nuestro router es el encargado de transmitir la información que entra o sale de los dispositivos conectados a la red y la encamina, a través de router intermedios hasta su destino.

Por ejemplo, el servidor de una red social o los servidores de un juego online al que necesitamos conectarnos para poder acceder al servicio. Si queremos que nuestra conexión funcione bien debemos abrir en nuestro router los puertos que utilice la aplicación que vamos a utilizar vinculando cada puerto a la dirección IP de nuestro ordenador.

Si los router fuesen viviendas, los puertos serían las puertas de las habitaciones, y el interior de estas serían las aplicaciones de Internet que consumimos y disfrutamos. Todos los router tienen ***65.536 puertos numerados del 0 al 65.535.*** De modo que, cuando nos conectamos a una página web, el router del servidor de dicha web tiene abierto el puerto ***80*** o el ***443*** (los puertos por defecto de las comunicaciones HTTP y HTTPS respectivamente).

Por defecto, en la mayoría de router de nuestros hogares, los puertos abiertos son precisamente el ***80*** y el ***443***. Sin embargo, en otros modelos pueden aparecer abiertos el ***8080*** (para el servicio de caché de Internet) y el ***22*** (FTPS/SSH para el intercambio de archivos). Si queremos saber qué puertos tenemos abiertos por tipo de aplicación, podemos acceder al siguiente enlace.

Abrir o cerrar los puertos de nuestro router es una de las acciones más solicitadas por los usuarios, pero no todos saben cómo funciona, ni cuáles son sus implicaciones para nuestra seguridad.

10.1 Riesgos de dejar los puertos abiertos

Los ciberdelincuentes utilizan los puertos para lanzar ataques contra los dispositivos a los que quieren infectar, por lo que mantener esos puertos abiertos les pondría las cosas un poco más fáciles.

Un ataque con éxito contra nuestro router podría ***comprometer todas las comunicaciones de todos los dispositivos de nuestra red***, lo cual podría afectar no solo a nuestra información, sino a la de toda nuestra familia.

Algunas de las ***amenazas más comunes*** contra los router son:

Modificación de la configuración DNS: el protocolo DNS permite relacionar la IP de un servidor (por ejemplo: 195.235.9.101) y el nombre de la web a la que queremos dirigirnos (por ejemplo: osi.es). Un atacante que pudiera modificar esa configuración DNS podría llevarnos hacia una página web falsa que simula ser la web legítima.

Man-in-the-middle: el atacante podría monitorizar y modificar nuestros paquetes de datos desde el propio router. Esto permitiría a los atacantes obtener acceso no autorizado y tener control sobre los datos intercambiados.

Ataque DoS: aunque estos ataques están dirigidos a grandes empresas, el atacante podría secuestrar nuestro router para formar parte de una *botnet* objetivo.

Crear redes falsas: este ataque consiste en crear una réplica de nuestra red para engañar a los usuarios. La red tiene el mismo nombre y usa la misma contraseña de acceso. De esta forma, al conectarse los usuarios a esta red señuelo, podrían ser víctimas de un robo de datos personales.

10.2. Cómo abrir o cerrar puertos

Para configurar los puertos de nuestro router necesitaremos seguir los siguientes pasos:

- Accederemos al menú de configuración de nuestro router y buscaremos el apartado de ***Configuración avanzada.*** En algunos modelos de router deberemos buscar los apartados NAT, *Port Forwarding*, o Puertos.
- Una vez dentro, iremos a las opciones de ***Configuración de la red*** y seleccionaremos la pestaña NAT/PAT.
- Desde aquí, veremos el ***gestor de puertos,*** donde podremos abrir puertos nuevos o cerrar aquellos que no utilicemos.

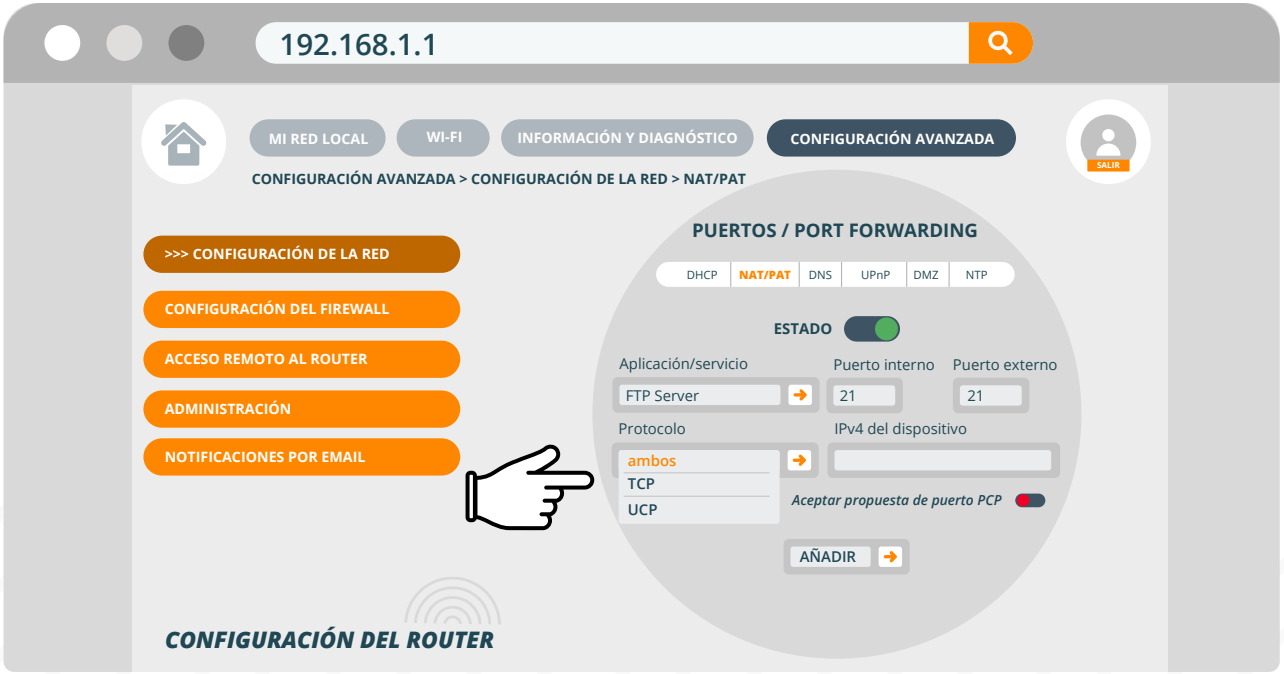
Si queremos ***abrir un puerto***, deberemos rellenar varios campos de información con los datos del puerto que queremos abrir. Algunos de los ***términos más habituales*** que encontraremos son estos:

Nombre: se indica la aplicación que está usando la configuración del puerto que vamos a configurar, a modo informativo.

Dirección IP de LAN: se utiliza para indicar a qué dispositivo de destino debe redirigirse la información que llegue por ese puerto. Introduce la dirección IP del dispositivo en el que se va a ejecutar dicha aplicación.

Dirección IP de WAN: es la dirección desde la que se van a redirigir los datos. Suele corresponder a la dirección IP de nuestro router, por lo que suele venir ya cumplimentado o simplemente en blanco para obviarlo.

Puertos WAN: este campo corresponde al número del puerto o rango que queremos abrir.



Img 19. Abrir y cerrar puertos

Puertos LAN: se utilizan los mismos datos que en la configuración de puertos WAN.

Protocolo UDP/ TCP: este dato debe indicarlo la aplicación o servicios que necesita abrir los puertos. Estos protocolos dan soporte a múltiples protocolos de Internet para asegurar que los datos lleguen correctamente a su destinatario.

Para cerrar un puerto, deberemos seleccionar el puerto en cuestión y hacer clic en ***Borrar / Eliminar.***

Una vez introducidos todos los datos, debemos ***guardar la nueva configuración del router*** y, en algunos casos, incluso es recomendable ***reiniciarlo***.

10.3 Servidor DHCP

Una vez que un dispositivo se conecta a la red wifi de nuestro router, se le provee de todos los elementos necesarios para que pueda navegar por Internet, entre ellos, una dirección IP, la puerta de enlace y los servidores DNS.

El ***servidor DHCP*** es el encargado de asignar estas direcciones según unos rangos específicos a cada red. Dicho de otro modo, la dirección IP asignada a cada dispositivo cambiará cada vez que se conecte a la red wifi.

Desde las ***opciones de configuración de nuestro router***, podemos acceder a las opciones del servidor DHCP y asignar una dirección IP fija a cada dispositivo conectado a nuestra red. Para ello:

- Iremos a ***Configuración avanzada > configuración de la red.*** En otros modelos de router los pasos pueden variar.
- Seleccionaremos la pestaña ***DHCP***. Una vez seleccionada se nos mostrarán las opciones de configuración para asignar una dirección IP a cada dispositivo conectado a nuestra red local.

Img 20. Servidor DHCP

- Rellenar los campos solicitados y hacer clic en ***guardar***.

Puede ser útil si queremos ***asignar a una dirección MAC determinada, una dirección IP fija.*** De este modo tendremos mayor control sobre los dispositivos conectados a nuestra red.

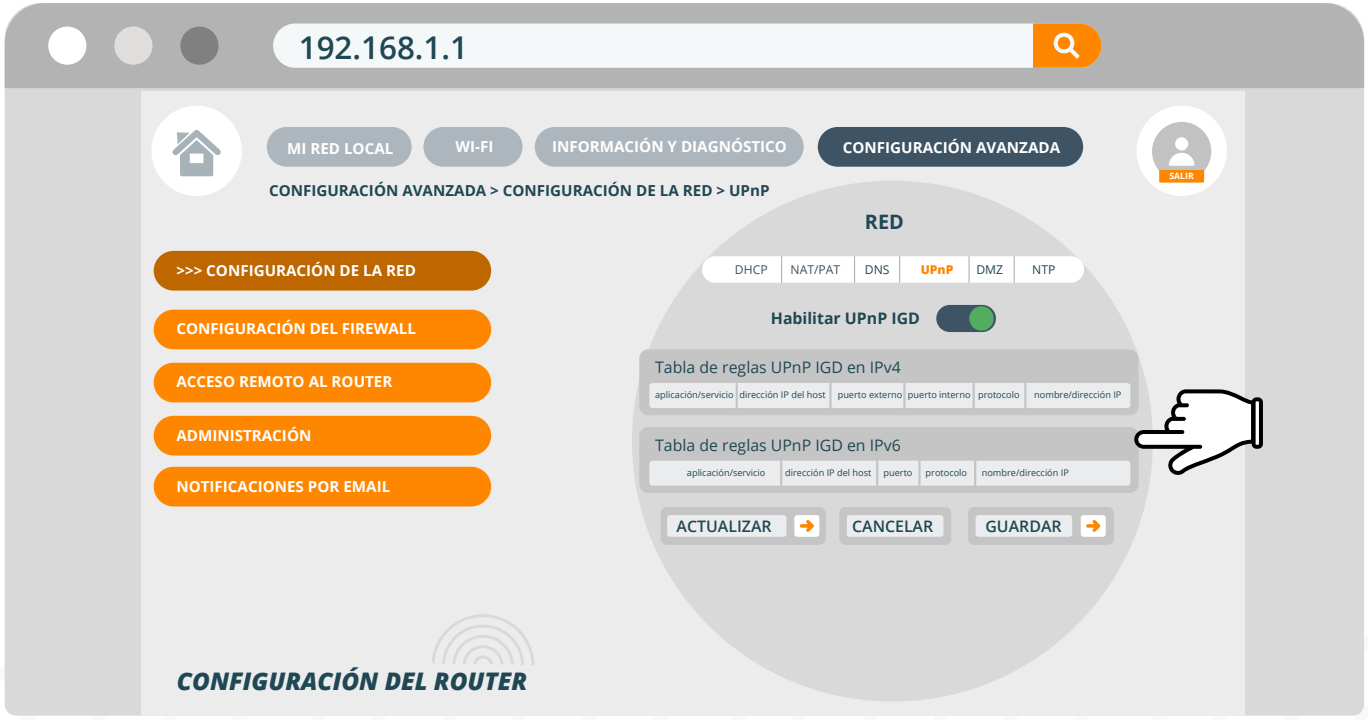
10.4 Servidor UPnP

Algunos modelos de router vienen por defecto con un servidor UPnP, aunque en algunos hay que instalarlo como un añadido, o incluso activarlo.

Este servidor es el ***encargado de que las comunicaciones se llevan a cabo correctamente sin tener que preocuparse de los puertos*** (ya que él se encarga de redirigir el tráfico) ***abriendo las conexiones cuando sea necesario y cerrándolas cuando ya no se necesiten.*** Resulta una función muy útil si queremos despreocuparnos de abrir y cerrar puertos de forma manual.

Para activar esta función, bastará con volver al menú de configuración de nuestro router:

- Iremos a ***Configuración avanzada > configuración de la red.*** En otros modelos de router los pasos pueden variar.
- Seleccionaremos la pestaña ***UPnP***. Una vez dentro de esta opción, solo tendremos que ***habilitar o activar*** la función ***UPnP*** y hacer clic en ***Guardar***.



Img 21. Servidor UPnP

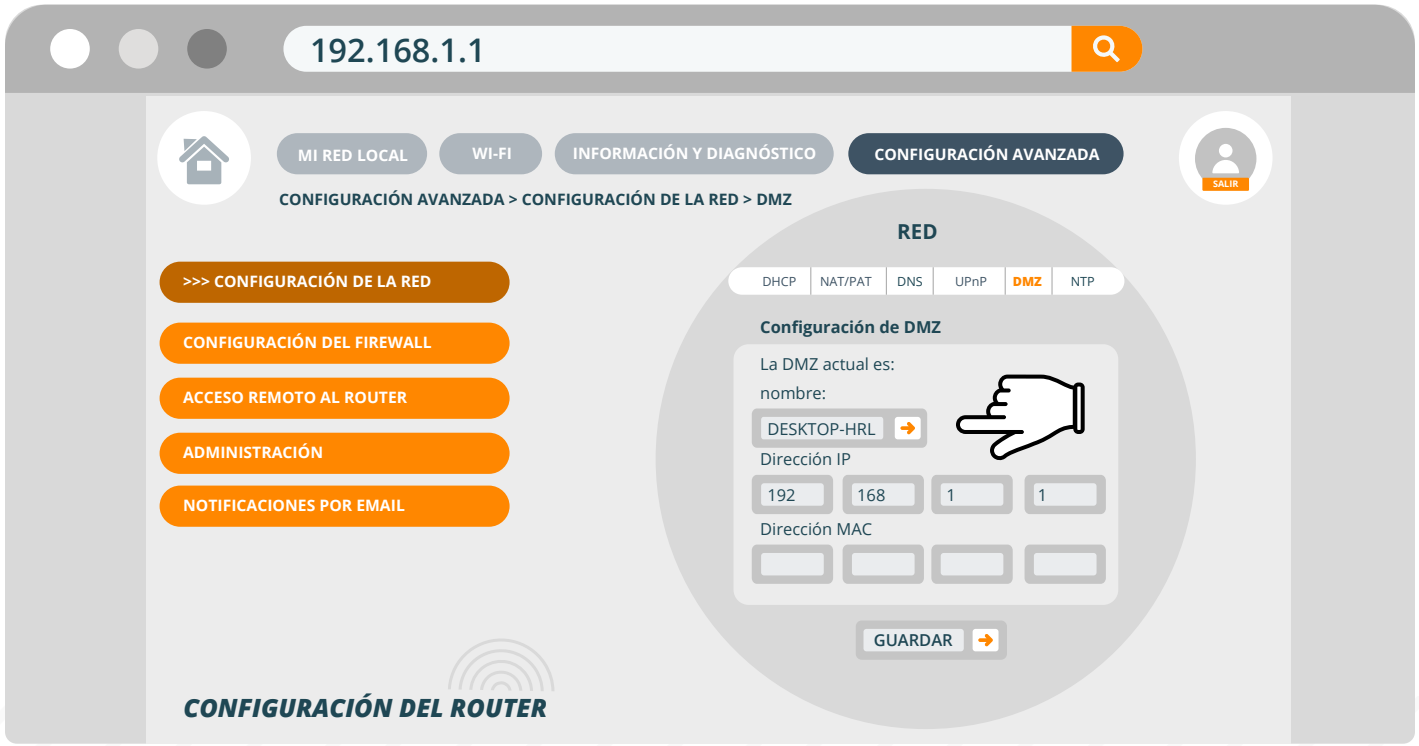
10.5 Servidor DMZ

Esta funcionalidad no está disponible para todos los router. Su función es la de abrir todos los puertos de la red de una dirección IP concreta, dejando la conexión totalmente abierta, sin ningún tipo de restricciones o bloqueos para el usuario.

Sin embargo, activar esta función ***también expone nuestros dispositivos a un gran número de amenazas***, como ciberataques a nuestras conexiones o infección por *malware*, por lo que no es recomendable para usuarios menos avanzados o con pocos conocimientos técnicos.

Para activar esta función, bastará con volver al ***menú de configuración de nuestro router:***

- Iremos a ***Configuración avanzada > configuración de la red.*** En otros modelos de router los pasos pueden variar.
- Seleccionaremos la pestaña ***DMZ***. Una vez ahí, solo tendremos que ***seleccionar el dispositivo*** con el que queremos activar el servidor DMZ. Es necesario que asociemos una ***dirección IP estática*** desde la configuración DHCP sobre el dispositivo para poder activar esta función.
- Una vez seleccionado, haremos clic en ***Guardar***.



Img 22. Servidor DMZ

11. Crear una red para invitados

Una red de invitados tiene como objetivo el permitir que varios dispositivos se conecten a nuestra conexión a Internet, pero permitiéndoles navegar en una red distinta a la de nuestros dispositivos habituales. De este modo, podrán acceder a nuestra conexión a Internet sin comprometer la seguridad de nuestra red principal y, sin que perdamos el control de los accesos.

Por ejemplo, imagina que vienen varios amigos de visita, pero no queremos que tantas personas se conecten a nuestra red principal por seguridad. En estos casos, es muy recomendable disponer de una red para invitados a la que puedan conectarse.

En caso de algún tipo de incidente, nunca se comprometerá nuestra red principal, ni los dispositivos conectados a ella.

Además, ***podremos limitar ciertos parámetros en esta red*** como, por ejemplo, el ancho de banda o el tiempo de conexión.

Dependiendo del modelo del router, es posible que podamos llevar a cabo configuraciones adicionales, como limitar el ***tiempo de conexión*** o el ***ancho de banda***. Se trata de una función que puede encontrarse fácilmente en las ***opciones de nuestro router:***

- Deberemos acceder a la ***configuración de nuestro router*** y buscar las ***Opciones de configuración inalámbrica***. Luego, buscaremos la opción ***Wi-Fi***, aunque puede encontrarse entre los apartados principales como Red para invitados en algunos router.
- Ahora deberemos ***configurar la red de invitados:***

Elegiremos el ***nombre de la red o SSID.***

Crearemos una ***contraseña segura.***

Elegiremos el ***método de autenticación,*** preferiblemente ***WPA2/AES.***

Dependiendo del modelo de router, podremos configurar determinados parámetros, como limitar el ancho de banda, el tiempo de conexión o incluso, un filtrado MAC dentro de la propia red para invitados. También, es posible que podamos escoger el ***tipo de red (2,4GHz o 5GHz)*** que se traducirá en la velocidad a la hora navegar por Internet. Se recomienda escoger la red de ***2,4GHz*** que, aunque es más lenta, es utilizada por la mayoría de los dispositivos móviles.

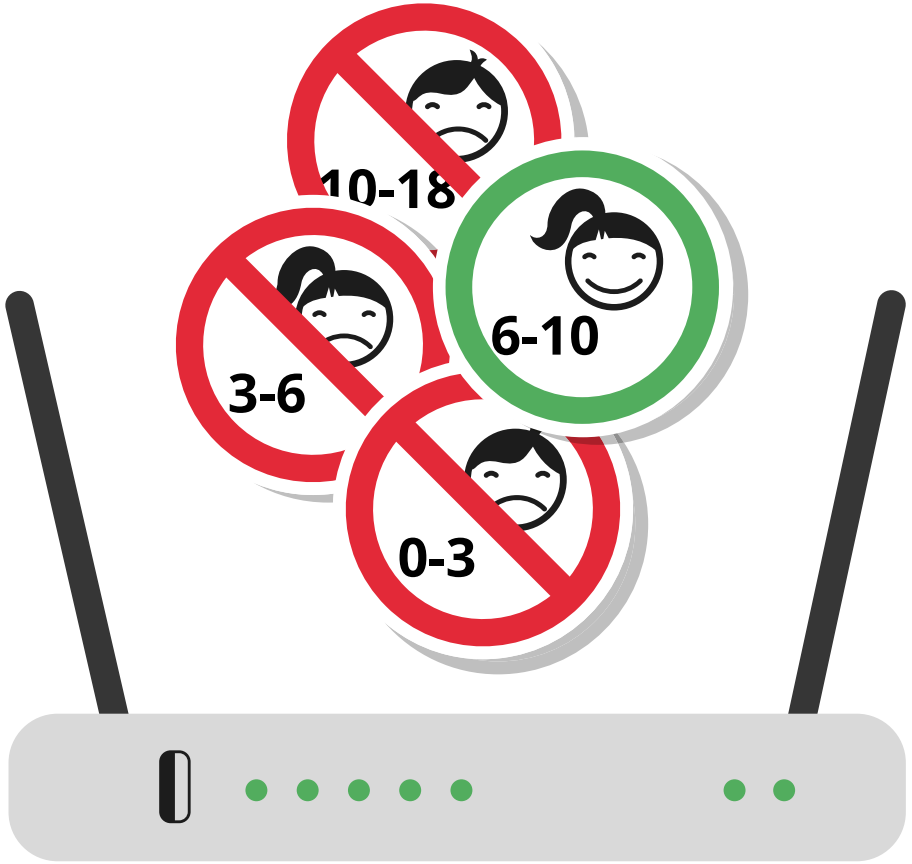
Una vez creada, ***la red se guardará en nuestro router y solo deberemos activarla/desactivarla en función de la situación***. Para evitar riesgos, es recomendable desactivarla siempre que no vayamos a necesitarla.

Img 23. Wi-Fi de invitados

12. Control parental

El control parental permite bloquear ciertas páginas webs que no sean apropiadas para los usuarios más pequeños que se conectan a nuestra red, e incluso, nos permite filtrar ciertas palabras para que, en caso de encontrar una web con dichos contenidos, ésta se bloquee y no lleguemos a acceder a ella.

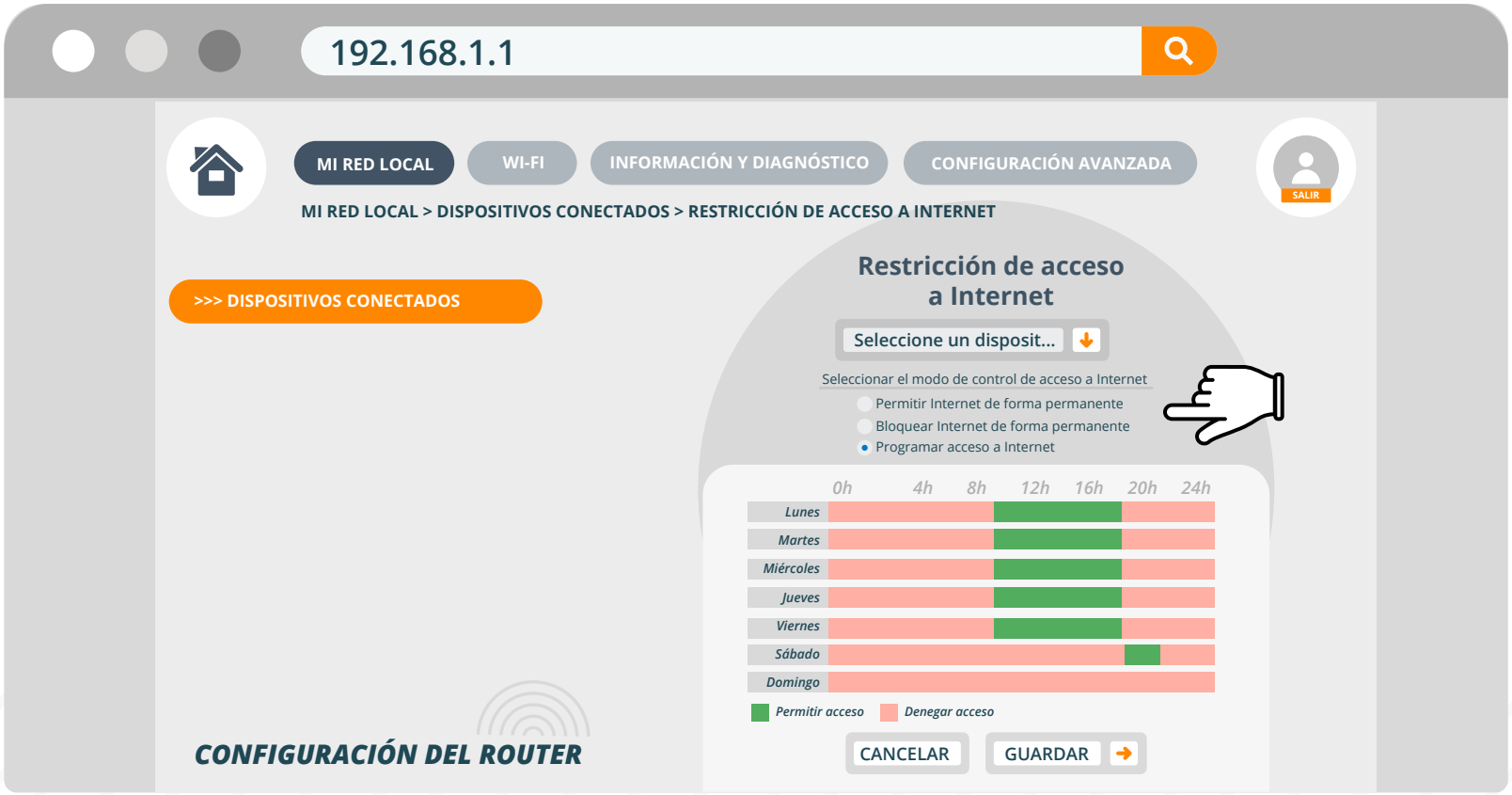
Su función principal es permitir a los padres con menores bajo su responsabilidad, bloquear los contenidos de determinadas web que no se consideren aptas para ellos. Una vez registradas las direcciones IP o URL de las web que queremos bloquear, éstas permanecerán registradas en nuestro router.



Si nuestro router dispone de una opción de control parental, podremos ***incluir las direcciones IP de los servicios y/o páginas web que queramos bloquear.*** En algunos modelos incluso podremos mandar recordatorios, como por ejemplo para avisar al usuario de que lleva demasiado tiempo conectado a Internet, o impedir el acceso a la red a determinadas horas del día.

En algunos modelos, esta opción no está disponible como menú de configuración y en su defecto, tendremos que ***configurar el firewall de nuestro router para bloquear el acceso a determinadas direcciones IP.*** Sin embargo, ***no es una opción recomendada para usuarios no experimentados.***

Otra opción será recurrir a las herramientas de control parental que se pueden instalar directamente en los dispositivos de los menores. Podremos encontrar mucha más información sobre este tipo de aplicativos en la web: www.is4k.es.



Img 24. Control parental

12. Enlaces para ampliar conocimientos

- Protege tu red en 5 sencillos pasos
- Man in the middle. Toda tu actividad al descubierto
- Tu router, tu castillo. Medidas básicas para su protección
- Spoofing o el robo de identidades, ¡qué no te Engañen!
- Pasos para mejorar la seguridad de tu router
- Detectado ataque a routers domésticos que los convierte en bots o Zombies
- Compartir Wifi ¿Si o No?
- Te refrescamos cómo proteger la red wifi de casa
- Descubre las MAC y cómo utilizarlas para que tu red sea más segura
- Descubre y elimina a los intrusos de tu red wifi
- Aprende a asegurar tu WiFi en 7 pasos

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
OSI Oficina de Seguridad del Internauta