Recomendaciones de seguridad en

Redes caseras *de cara al teletrabajo*

Carlos Guerra, marzo 2020.

Este informe fue realizado por Derechos Digitales.

Editado por Alex Argüelles.
Diseño y diagramación por Constanza Figueroa.
Corrección de estilo por Rocío Consales.

Marzo 2020.

Frente a la necesidad de trabajar remotamente que ha impuesto la crisis sanitaria producto de la explosiva propagación del COVID-19, hemos redactado una guía básica para asegurar redes residenciales, pensando en aquellas personas que manipulan información sensible y desean mayor seguridad en sus comunicaciones.

Para desarrollar estas recomendaciones asumimos que queremos proteger una red casera compuesta de un router y múltiples dispositivos conectados a él, especialmente de forma inalámbrica. Haremos mucho énfasis en la protección del router, ya que este equipo es la puerta de entrada y salida a internet, y muchas de las vulnerabilidades posibles de seguridad se pueden resolver en este.

Primero lo primero: asegurarse de que la red tenga contraseña

Cuando una red Wi-Fi no tiene contraseña no solamente es susceptible a que cualquiera pueda conectarse y consumir el ancho de banda, sino que también permite a terceros acceder a: los equipos dentro de la red, los recursos compartidos como carpetas en red, impresoras, etc.

No tener contraseña de acceso a tu red Wi-Fi también abre la posibilidad de explotar las vulnerabilidades que los sistemas operativos de los dispositivos conectados pudieran tener, especialmente si no se encuentran actualizados. Recomendamos como primer paso establecer una buena contraseña para la red, teniendo en cuenta algunas limitaciones -que discutiremos más adelante- para personalizar estas contraseñas.

Sobre la seguridad del router en nuestra red

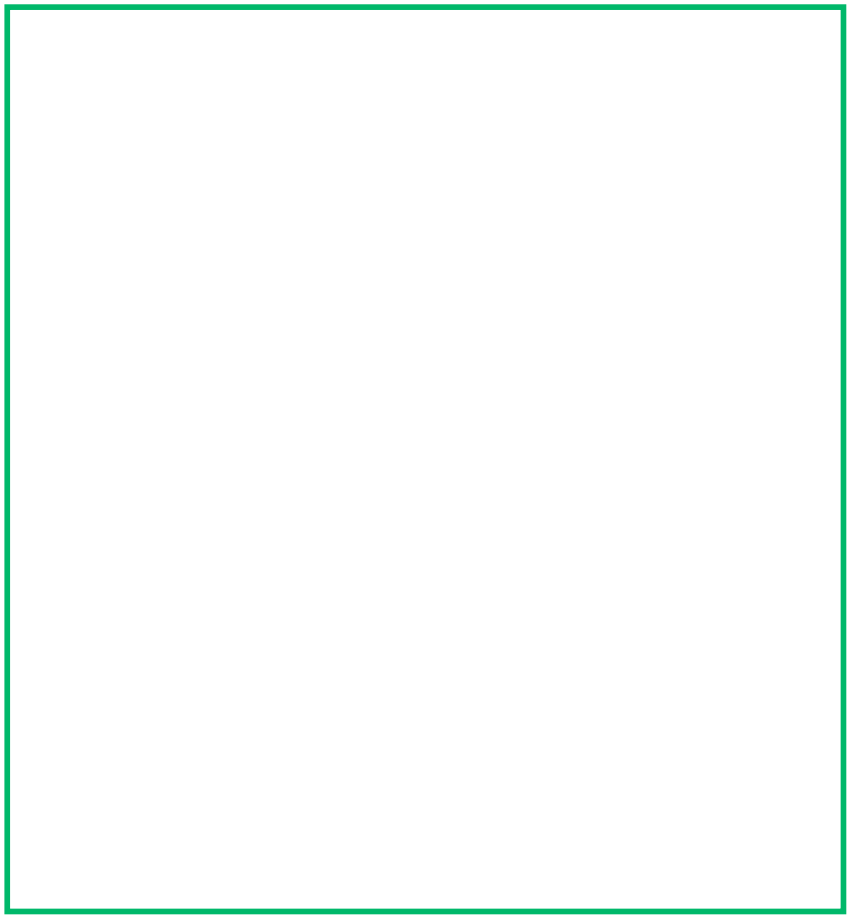
Revisar si el router puede ser administrado por cualquier persona no autorizada dentro de la red

Generalmente en nuestro router podemos ajustar muchas características de funcionamiento que permiten optimizar el uso que hacemos de la red (inalámbrica y cableada), sin embargo estas posibilidades también pueden ser abusadas para violar nuestra seguridad. Algunas cosas que un atacante puede hacer son: enviar el tráfico a equipos específicos, cambiar la contraseña y dejar a las propietarias de la red fuera de esta, acceder a equipos dentro de la red y explotar vulnerabilidades de seguridad para tomar control de ellos, y otras actividades maliciosas que dependan de las características del router.

Para mitigar estas amenazas, debemos asegurar mejor nuestra red, de forma que se restrinja el acceso a personas indeseadas que potencialmente tengan acceso a nuestra red inalámbrica. Recomendamos realizar estos pasos:

1. Encontrar la dirección IP de nuestro router: en redes residenciales suele ser 192.168.0.1 o 192.168.1.1, sin embargo, dependiendo de múltiples factores puede ser diferente. A continuación algunos métodos para ubicarla según tu sistema operativo:

a. En Windows:
    i. Iniciar, seleccionar el símbolo del sistema (o escribir “cmd”).
    ii. Escribir el comando ipconfig y ubicar la dirección IP de la “Puerta de enlace predeterminada”.

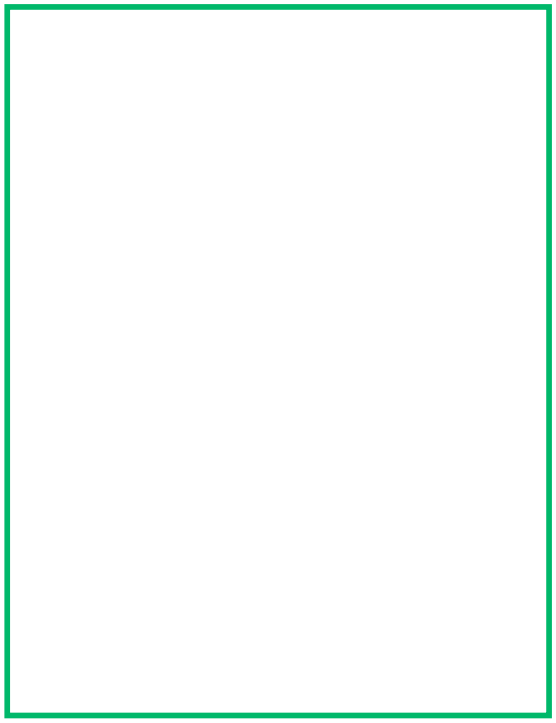


Ejemplo para Windows.

b. En Mac:
   i. Abrir Terminal e ingresar el comando “netstat -nr | grep default”.
   ii. Ubicar el dato de la dirección correspondiente al router.

Ejemplo para Mac.

c. En Android:
   i. Ajustes, Wi-Fi, buscar nuestra red, opciones, detalles, puerta de enlace.



Ejemplo para Android.

b. En Linux: dependerá de qué distribución utilices, sin embargo algunas opciones que funcionan en la mayoría son:
   i. En un terminal colocar “ifconfig”linux y ubicar el IP de la puerta de enlace o gateway (que corresponderá al router).
   ii. Si la función anterior no resulta se puede escribir “ip r”.
   iii. En las propiedades de red (algunos entornos de escritorio).

Ejemplo para Gnome Shell.

2. Ingresar la dirección IP obtenida en un navegador web (como Chrome, Firefox, etc.)
3. Ver qué ventana aparece, muy probablemente una pidiendo un usuario y contraseña. Dependiendo de la marca, modelo y compañía proveedora podemos averiguar las credenciales por defecto:
   a. Ir a https://www.routerpasswords.com/
   b. Buscando en Google marca, modelo, proveedor y contraseñas por defecto, por ejemplo “DLink dir 600 contraseña por defecto”, “TP-Link N300 default password” (En inglés quizás aparezcan más resultados) o “Movistar router fibra contraseña por defecto”.
4. Ingresar en los campos de usuario y contraseña las credenciales encontradas.
   a. ¿Pudiste ingresar al administrador siguiendo los pasos anteriores?: El router tiene una contraseña insegura, sugerimos cambiar la contraseña de administración por una mejor. Más adelante daremos recomendaciones para crear contraseñas fuertes.
   b. ¿No funcionaron los pasos anteriores? En este caso un tercero configuró una contraseña propia. Recomendamos ubicar esta contraseña (en ocasiones anotada debajo o detrás del propio router) o hacer una restauración de fábrica, usando un botón

que suele estar detrás del router y generalmente solo se puede presionar con un alfiler.

OJO: Al hacer una restauración de fábrica se perderá la configuración actual del router y habría que volver a configurar el nombre de la red y su seguridad como mínimo.

5. Una vez en el administrador del router, hay que tener presente la seguridad de la red inalámbrica. Más adelante cubriremos algunas configuraciones básicas.

Revisar si nuestro router puede ser administrado desde internet

En muchos casos, de forma inadvertida, poseemos una dirección IP Pública (a la que se puede llegar desde cualquier lugar en Internet) y cuando accedemos a ella llegamos a la misma página de administración del router que acabamos de revisar. Esto puede ser bastante inseguro, sobretodo si -como vimos- tenemos un usuario y contraseña de administración de fábrica.

Esta situación permite a miles de personas escanear toda la internet de forma automatizada, en búsqueda de este tipo de errores para intentar controlar dispositivos e incluirlos en botnets, infectarlos con ransomware o extraer información sensible como datos bancarios, íntimos o información confidencial empresarial. Para chequear y atender este problema recomendamos estos pasos:

1. Conseguir nuestra dirección IP pública, en muchos casos corresponderá a la dirección de nuestro router. Se pueden usar sitios como https://myip.es/

OJO: Nuestra dirección IP pública es diferente a la dirección IP privada que conseguimos en la sección anterior, la privada únicamente es visible estando dentro de nuestra red.

2. Ingresar la dirección obtenida en un navegador web.
3. Ver si aparece lo mismo que aparece cuando ponemos la dirección interna de nuestro router.
4. ¿No se puede acceder al administrador del router a través de internet? En el caso en que no se vea algo o aparezca algún tipo de error al intentar ver el administrador de nuestro router en el navegador, entonces estamos protegidos ante cualquier amenaza externa en internet que quiera vigilar nuestras comunicaciones a través del router. Puedes saltar a la siguiente sección sin problemas.
5. ¿Se puede acceder al administrador del router a través de internet? Se recomienda muy enfáticamente buscar una forma de deshabilitar este acceso, algunas opciones son:

    a. Ver si hay opciones para deshabilitar esa interface hacia internet: Dependiendo del modelo puede haber una opción diseñada directamente para esto. Prueba buscando en algún apartado de seguridad cosas como “deshabilitar acceso al administrador desde Internet/WAN” (o “Disable admin access from internet/WAN” en inglés).

    b. Hacer un reenvío de puertos o “Port forwarding”: Esto sirve para enviar cualquier solicitud desde internet a la interfaz administrativa del router a un dispositivo y/o servicio que no exista. Aunque este es un tema un poco más avanzado, compartimos algunas referencias para encontrar más información. Lo importante es configurar el reenvío del puerto 80 a algún otro puerto no usado de un equipo no conectado en la red (por ejemplo a una dirección IP que ningún equipo esté usando). Aprende más en: ¿Cómo configurar Port Forwarding?

    c. ¿No podemos hacer ninguna de las configuraciones planteadas arriba? Consideraremos entonces nuestra red como insegura. En este caso, para mantener nuestras comunicaciones completamente privadas ante cualquier persona que puede estar espiando nuestra red a través de internet -y un acceso simple al nuestro router- recomendamos el uso de un cliente de VPN o Tor.

Sobre la seguridad de la red inalámbrica

Ahora que el acceso al router está más asegurado, después de seguir los pasos anteriores, es un buen momento para revisar y ajustar algunas configuraciones que mantendrán más segura la conexión para nosotros y los demás usuarios que utilizan nuestra red Wi-Fi.

Deshabilitar WPS

WPS es un protocolo de conexión que sirve para agregar nuevos equipos a la red Wi-Fi con solo presionar un botón en el router y luego en el dispositivo. Aunque este método resulta muy conveniente, tiene un problema clave de seguridad: habilita una segunda contraseña para acceder a la red Wi-Fi de 8 números, la cual es muy fácil de conseguir ya que permite intentar muchas veces en poco tiempo todas las combinaciones posibles; de hecho, algunos programas permiten “crackear” la clave del Wi-Fi de redes con WPS habilitado en unas pocas horas.

Al deshabilitar este protocolo nuestra seguridad se verá mucho más fortalecida, sin embargo perderemos la opción de incluir equipos a la red de forma automática.

Desactivar los protocolos de seguridad WEP y WPA

Las redes Wi-Fi pueden usar varios protocolos de seguridad a través de contraseñas. Los protocolos también ayudan a cifrar las comunicaciones, esto quiere decir que si un tercero logra interceptar los paquetes de datos (que literal viajan en el aire) no podrá entenderlos/descifrarlos. Históricamente los protocolos de seguridad más comunes son WEP, WPA y WPA2. Los dos primeros se consideran antiguos e inseguros, ya que se han descubierto formas de interceptar las comunicaciones cifradas con estos protocolos y descifrarlas con facilidad.

Recomendamos revisar que ni WEP ni WPA estén activados como protocolo de seguridad de la red Wi-Fi. En caso de tener esos protocolos activados, sugerimos cambiarlos por WPA2 o WPA3 (si está disponible).

También es posible elegir el tipo de cifrado que usará el protocolo elegido, las dos opciones más comunes son TKIP y AES. De la misma forma en que WEP y WPA se consideran protocolos inseguros, TKIP no se recomienda ya que es antiguo y se puede vulnerar con facilidad. Recomendamos habilitar cifrado AES, sin embargo -en caso de que esta opción no aparezca- es probable que estemos usando un router más moderno que solo maneje cifrado AES por defecto.

Deshabilitar UPnP

Una de las funciones que incluyen muchos routers desde hace tiempo es llamada Universal Plug and Play o UPnP, que ayuda a automatizar configuraciones de reenvío de puertos (que abordaremos más adelante). Esta función puede ser explotada, con grandes consecuencias de seguridad. Recomendamos su desactivación desde la configuración del router. En caso de no tener acceso a esta configuración probablemente signifique que la función UPnP no está disponible.

Evaluar la seguridad de las contraseñas de red

Al habilitar WPA2 como protocolo de seguridad para nuestra red Wi-Fi también tenemos la ventaja de usar contraseñas de hasta 63 caracteres, esto nos permite usar contraseñas realmente seguras para nuestra red.

Aunque existen diversos criterios sobre la creación de contraseñas seguras, los principales son:

- *Una contraseña de 8 caracteres es muy corta: las recomendaciones de una longitud aceptable van desde 12 hasta 20 como mínimo. Incluso, recomendamos frases de contraseña que pueden pasar los 30 caracteres.*
- *Usar varios tipos de caracteres (mayúsculas, minúsculas, números y símbolos) ayuda a hacer las contraseñas más seguras, pero puede dificultarnos recordarlas. Como regla general: mientras más larga sea la contraseña, más segura será, independientemente de la diversidad de sus caracteres.*
- *Las contraseñas más fáciles de adivinar son aquellas que tienen algo que ver con sus propietarias: números de identificación, fechas de cumpleaños, direcciones, números de teléfono, etc. Ya que estos datos podrían ser fáciles de obtener para un tercero malintencionado, se recomienda usar contraseñas que no tengan relación aparente con las personas que las crean. Se recomienda usar algo "muy fácil de recordar para nosotros pero muy difícil de adivinar para otros".*

Otra observación relevante respecto a las contraseñas es que los routers más recientes tienen la posibilidad de operar en bandas de 2.4GHz y 5GHz. Esto permite que las redes que operan en ambas bandas tengan nombres,

contraseñas y protocolos diferentes. Recomendamos revisar que al menos los protocolos de seguridad y las contraseñas de ambas redes sigan los lineamientos que hemos descrito en este manual.

Habilitar una red para invitados

Algunos routers tienen la posibilidad de habilitar una red de invitados aislada virtualmente del resto de la red. Esto puede ayudar a quienes reciban muchas visitas o compartan internet con vecinos, y quieran reducir las posibilidades de que estos terceros puedan ejecutar alguna actividad maliciosa sobre los equipos y comunicaciones propios. Si necesitas compartir tu red con terceros y tu router permite esta funcionalidad, recomendamos activarla.

Sobre los dispositivos que están conectados a la red

Generalmente, los dispositivos que están conectados a la red de nuestras casas son dispositivos conocidos que conectamos a propósito a la red. Estos dispositivos pueden ser teléfonos celulares, computadoras e incluso equipos de "Internet de las cosas" o IoT como lavadoras, cámaras de seguridad, iluminación inteligente, etc.

Cuando revisamos la seguridad de nuestra red es importante confirmar que no existen equipos extraños que puedan estar consumiendo ancho de banda y comprometiendo la calidad de descargas y llamadas por internet, o incluso ejecutando vigilancia mediante técnicas invasivas como captura de tráfico de red.

Algunos métodos para revisar qué equipos están conectados a nuestra red son:

Usar la página de administración del router

https://es.wikihow.com/sacar-a-alguien-de-tu-red

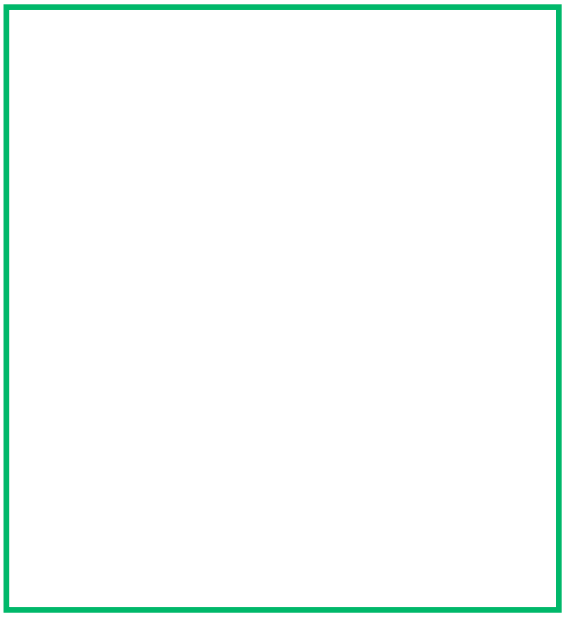
Aplicaciones de mapeo de red

Algunas aplicaciones se especializan en este tipo de análisis de red, algunas aplicaciones son :

Ping Tools (Android)

Fing - Network Scanner (iOS)

Nmap (Computadoras, más avanzado)



Ejemplo para Ping Tools en Android.

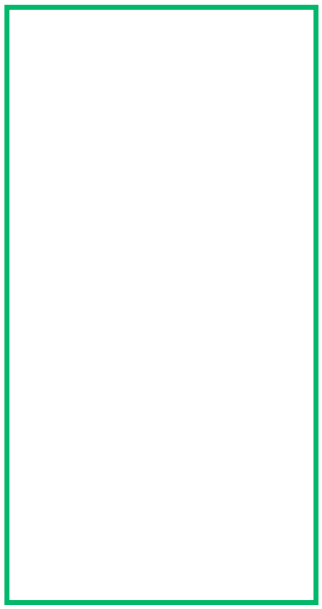
En el caso en que todos los dispositivos sean conocidos y de confianza, no hay motivo de alarma; pero si vemos equipos sospechosos o evidentemente maliciosos, recomendamos:

a. Comprobar que no sea un equipo nuestro que olvidamos o que funciona en red, como algunos decodificadores de televisión por cable, una cafetera inteligente o una computadora vieja que se encuentre encendida sin saberlo.
b. En caso de verificar que es un dispositivo sospechoso, desconectarlo en la interfaz del router.
c. Cambiar la contraseña de la red. Más arriba conversamos sobre algunas buenas prácticas.
d. Revisar que no sea un dispositivo conectado a un cable o punto de red, en ese caso desconectarlo.
e. Reunir toda la evidencia y documentación posible si se desea iniciar una investigación técnica o judicial.

En caso de no poder desconectar al equipo sospechoso de la red, recomendamos el uso de VPNs o Tor para manejar información sensible.

Algunos consejos generales

- Mantener todos los equipos de la red actualizados.
- Mantener el firmware del router también actualizado (avanzado).
- Evitar descargar e instalar programas sospechosos.
- Tener software antivirus instalado, actualizado y activado.
- En aquellos casos en donde tengamos velocidades de conexión bajas:
    a. Evaluar la conexión por cable al router en caso de señales inalámbricas débiles.
    b. Usar los equipos más cercanos al router para una mejor estabilidad de la señal.
    c. Evitar poner el router cerca de equipos que emitan señales de radio en frecuencias parecidas a las usadas por Wi-Fi, como microondas y teléfonos tradicionales inalámbricos.
- Usar aplicaciones como Wifi Analyzer para detectar en qué canal está transmitiendo nuestro router su señal y ver si este canal está muy saturado. Los routers pueden operar en varios lugares del espectro radioeléctrico y para mejorar su funcionamiento es recomendado que en una misma área geográfica se distribuyan las redes existentes en los diferentes canales disponibles. Esta configuración se realiza en la interfaz administrativa del router que ya usamos en las secciones anteriores.



Ejemplo de gráfico de canales para Wifi Analyzer.


DERECHOS
DIGITALES
América Latina