ASOCIACIÓN NACIONAL DE UNIVERSIDADES
E INSTITUCIONES DE EDUCACIÓN SUPERIOR

Dirección General de Administración
Dirección de Tecnologías de la Información y Comunicación

Manual de seguridad para redes inalámbricas

Contenido

Redes Inalámbricas

En los primeros días de la Web, la mayoría de los hogares no necesitaban una red de conexión entre aparatos.

Una familia solo tenía un ordenador, que se usaba para revisar el correo electrónico o navegar por la Web, pero todo esto ha cambiado mucho.

Ordenadores, portátiles, tablets, Smartphone, juegos, televisores, decodificadores, coches e incluso aparatos de cocina, todos necesitan conectarse a Internet y entre sí.

Hoy en día, una red de cualquier tipo que sea capaz de conectar muchos aparatos se ha convertido en una necesidad, y para esto, las redes inalámbricas se han convertido en las más utilizadas y se están volviendo cada vez más populares debido a su fácil configuración y que no requiere cableado.

¿Qué es una Red Inalámbrica?

Una red inalámbrica es una red configurada para utilizar una señal de radio (onda), a una determinada frecuencia, para comunicarse entre varios dispositivos que tengan acceso a la red y sin necesidad de utilizar cables.

Son redes que utilizan radiofrecuencia o infrarrojos para transmitir la información. También pueden utilizar ondas de microondas, pero no es lo más habitual.

En las Redes Inalámbricas no hay una conexión física por cable entre el remitente y el receptor de la información, sino que la red está conectada por ondas de radio o de microondas para mantener las comunicaciones.

Básicamente están compuestas por un AP (punto de acceso inalámbrico) al que se conectan todos los demás dispositivos inalámbricos de la red. El AP suele ser un **router**.

Funcionamiento de Una Red Inalámbrica

Podemos explicar el funcionamiento de una red inalámbrica para conectar varios ordenadores de la siguiente forma.

El ordenador utiliza datos binarios, es decir información codificada con 2 dígitos, ceros y unos. Estos datos binarios se codificarán (transformarán) a la frecuencia de una onda de radio y se transmitirán a través de una antena.

La conversión de los datos binarios a datos en forma de señal de radio la realiza una tarjeta llamada Tarjeta Ethernet, tarjeta que ya llevan incorporados casi todos los ordenadores modernos.

En un puerto de la tarjeta Ethernet se conecta la antena para el envío de la información.

Una vez enviado los datos como una señal de radio por la antena, el ordenador receptor los recogerá con su antena y su tarjeta Ethernet decodificará la señal a datos binarios de nuevo para que el ordenador receptor los entienda.

Tanto el ordenador que envía la información, como los ordenadores que la reciban, deban tener una antena receptora de la información y una tarjeta Ethernet para la descodificación de señal de radio a datos binarios.

También necesitamos tener en los ordenadores instalado un programa que gestione el envío y recibo de información por la red.

Ya tenemos nuestra red inalámbrica operativa para enviar y recibir información por el aire, sin necesidad de cables.

Si queremos conectar nuestra red u otra red, por ejemplo, a Internet, necesitaremos un aparato llamado Router Inalámbrico.

El router debe estar conectado a la nueva red con la que queremos conectar. Imaginemos que es Internet. Puede ser conexión inalámbrica o por cable.

Si queremos enviar información a otro aparato de la otra red, la información le llegará al router desde nuestra red, y lo que hace el router es recibir la información

en forma de ondas de radio por su antena y la codifica en otros datos que sean capaces de navegar por la red de unión entre las dos redes. Esta unión puedes ser por cable o incluso también inalámbrica.

Si la otra red es Internet, codifica los datos de la señal de radio que le llegan procedentes de nuestra red, en datos que sean capaces de viajar por el cableado de Internet y los envía a la dirección de la otra red especificada por nosotros con el programa de envío de datos.

Además, el router inalámbrico también es capaz de recibir información de Internet (la otra red) y convertirlos en señales de radio (codifica) para enviarla a la antena de uno de los ordenadores de nuestra red.

El router es capaz de codificar la información que le llega de nuestra red y descodificar los datos que le llegan de la otra red (internet), además de saber a qué ordenador o aparato le tiene que enviar la información, y por supuesto enviársela.

En las redes inalámbricas basadas en Wi-Fi, todos los dispositivos se conectan a un solo enrutador, en lugar de estar directamente conectados uno con otro.

Los ordenadores, tablets y otros dispositivos se conectan a un solo router, llamado «punto de acceso inalámbrico» que trabaja como un conmutador, ya que lo que hace es enviar la información recibida desde uno de los aparatos de nuestra red, hacia el dispositivo concreto de nuestra red que los tiene que recibir. Muchas veces este tipo de router se llama switch inalámbrico (interruptor en inglés).

Como ves, los router conectan los dispositivos de la red y además tienen la capacidad de conectar la propia red a otra red, como ya vimos.

Un dispositivo solo podrá conectarse a la red inalámbrica cuando está dentro del alcance de las señales (ondas) que emite el router inalámbrico u otro dispositivo que emita la señal.

Además, si se tiene habilitada la seguridad inalámbrica en la red, deberás ingresar la contraseña de la red en cada dispositivo que desee conectar a esa red.

Para entender mejor el funcionamiento de las redes inalámbricas se recomienda ver el siguiente video que toma menos de 5 min:
https://www.youtube.com/watch?v=_K9M0A9ukMU&t=159s

Riesgos asociados a las redes inalámbricas

La llegada del Wi-Fi a los lugares públicos marcó un antes y un después en el día a día de los usuarios interconectados, ya que nos permitió aprovechar el servicio de Internet cuando nos sentamos en algún café, ya sea que tengamos que pedir la contraseña o que directamente esté abierta para cualquiera que desee conectarse.

Pero si tan solo nos detuviéramos unos minutos para pensar en qué tan seguras son estas conexiones, rápidamente encontraríamos varios motivos para dar una respuesta negativa. Si al visitar un lugar público no dejamos nuestras pertenencias en cualquier sitio, porque conocemos los riesgos de hacerlo, ¿por qué lo haríamos con la información almacenada en nuestros dispositivos?

Es por ello que antes de usar estos accesos de internet gratuito, se deben considerar algunos cuidados y recomendaciones para evitar ser víctima de ataques cibernéticos y hackeos. Sin importar el lugar o proveedor, todas las redes públicas gratuitas tienen cierto grado de riesgo.

Ser víctima de un ataque "*Man in the Middle*"

Como su nombre lo indica, los de ataques "Man in the Middle", que traducido sería "hombre en el medio", asociados a conexiones a redes Wi-Fi públicas suelen estar relacionados con la presencia de un intermediario entre la víctima y el sitio que ésta visita, pudiendo el cibercriminal acceder a los datos mientras viajan.

No solo se trata de ataques altamente efectivos, sino que, además, también motivo de su efectividad, son muy difíciles de detectar, dado que la información es interceptada a mitad de camino cuando viaja entre el dispositivo de usuario y el router, sin que sea percibido.

Robo de datos personales, información confidencial y/o credenciales

Por supuesto, si la red Wi-Fi a la que te conectas no es lo suficientemente segura, los datos que guardas en tu computadora o teléfono (archivos personales o contraseñas) pueden quedar expuestos al robo. ¿Cómo? Por ejemplo, si un criminal se aprovecha de la falta de mecanismos de seguridad en una red Wi-Fí pública podría interceptar el tráfico mediante un ataque Man in the Middle. Esto podría tener consecuencias aún peores si te conectas a esta red desde tu equipo de trabajo, donde probablemente haya información confidencial.

Cuidado al realizar una transacción en línea

Puedes pensar que no es necesario decirlo, pero son muchos los usuarios que siguen realizando compras y transferencias online o ingresando a *Homebanking* conectados a la red Wi-Fi de algún café, hotel o aeropuerto. Sin importar desde qué dispositivos te conectes, el uso de una red pública siempre representará un riesgo para realizar cualquier acción que involucre algún dato privado, porque como vimos anteriormente, no sabemos si alguien está interceptando el tráfico.

Falsos puntos de acceso se presentan como redes sin clave

Cada vez es más común encontrarnos con redes Wi-Fi en lugares públicos sin ningún tipo de seguridad. Si se trata de un café, por ejemplo, es normal ver que el nombre del lugar figura también como nombre una red y que ésta no tuviera clave alguna.

En estos casos, es importante tener presente dos cosas:

En primer lugar, si bien nunca es recomendable conectarse a redes sin clave, si vas a hacerlo es aconsejable consultar cuál es el nombre de la red de ese lugar para comprobar que efectivamente sea el que ves en tu pantalla.

Por otro lado, es posible (y sencillo) que un atacante aproveche estas conexiones para clonarlas (montando una red con el mismo nombre) para utilizarla como un señuelo a la espera de que los usuarios se conecten y enlacen sus dispositivos a la antena del atacante. Si esto ocurre, todos los paquetes de conexión que entren y salgan pasarán por el equipo atacante, quien podrá ver y modificar todo a voluntad.

Router vulnerado

Sí, así como los computadores y smartphones pueden infectarse, también existen vulnerabilidades presentes en otros dispositivos conectados, como los routers. Tal vez el ataque se trate de un simple secuestro del ancho de banda, o podría incluso escalar hasta convertir a los dispositivos infectados en partes de una botnet. La realidad es que, sin una mínima protección básica, como la modificación de la contraseña predeterminada, el router puede convertirse en la puerta de entrada para que un atacante logre acceder a cualquier dispositivo que esté conectado a él.

Consejos de seguridad inalámbrica para mantener la seguridad en redes Wi-Fi públicas

Los usuarios de redes Wi-Fi están en peligro frente a los hackers, pero afortunadamente existe protección frente a ellos. La reciente ampliación de las redes Wi-Fi públicas y gratuitas ha supuesto un gran beneficio para los profesionales. Desde que estos puntos de acceso gratuito están disponibles en restaurantes, hoteles, aeropuertos, bibliotecas e incluso en algunos locales de venta al público, rara vez tienes que desplazarte a gran distancia para tener acceso a la red y a tu trabajo. Aunque esta libertad tiene un precio, y muy pocas personas entienden realmente los riesgos asociados de una red Wi-Fi pública con estas conexiones. Si aprendes a protegerte, te asegurarás de que los datos importantes de tu empresa permanecen seguros.

- **Recuerda que cualquier dispositivo puede correr peligro**
  Portátiles, smartphones y tablets... Todos los dispositivos pueden verse afectados por los riesgos asociados a la seguridad inalámbrica.
- **Sospecha de todos los enlaces Wi-Fi**
  No asumas sin más que el enlace Wi-Fi es legítimo. Podría ser un enlace falso configurado por un cibercriminal que está tratando de capturar información

personal valiosa de usuarios ingenuos. Duda de todo y no te conectes a un punto de acceso inalámbrico desconocido o no reconocido.

- **Intenta verificar si se trata de una conexión inalámbrica legítima**
  Algunos enlaces falsos (configurados por usuarios maliciosos) tendrán un nombre de conexión que, de forma intencionada, será similar al de la cafetería, el hotel o el local que ofrece Wi-Fi gratuito. Si puedes hablar con un empleado del lugar que ofrece la conexión Wi-Fi pública, pide información sobre su punto de acceso Wi-Fi legítimo, como el nombre y la dirección IP de la conexión.

- **Utiliza una VPN (red privada virtual, del inglés "virtual private network")**
  Si utilizas una VPN al conectarte a una red Wi-Fi pública, estarás utilizando un "túnel privado" que cifra todos los datos que pasan por la red. Esta opción puede ayudar a evitar que los cibercriminales que acechan la red intercepten tus datos.

- **Evita utilizar tipos específicos de sitios web**
  Intenta evitar iniciar sesión en sitios web en los que los cibercriminales puedan capturar tu identidad, contraseñas o información personal, como los sitios de redes sociales, servicios de banca online o cualquier sitio web que almacene la información de tu tarjeta de crédito.

- **Plantéate la posibilidad de utilizar tu teléfono móvil**
  Si necesitas acceder a sitios web que almacenan o requieren la introducción de información confidencial (incluidos los sitios de redes sociales, compras online y banca online), puede que merezca la pena utilizar la red de tu teléfono móvil en lugar de la conexión Wi-Fi pública.

- **Protege tus dispositivos de ciberataques**
  Asegúrate de que todos tus dispositivos están protegidos mediante una solución antimalware y de seguridad eficaz, y asegúrate de actualizarlos con la máxima frecuencia posible.

Protección de las redes inalámbricas

A continuación, se incluyen varios pasos sencillos que puedes seguir para proteger tu red y routers inalámbricos:

- **Evita la utilización de la contraseña predeterminada**
  Es muy fácil para un hacker descubrir cuál es la contraseña predeterminada del fabricante de tu router inalámbrico y utilizarla para acceder a la red inalámbrica. Por lo tanto, es conveniente que cambies la contraseña de administrador de tu router inalámbrico. A la hora de establecer la contraseña nueva, trata de elegir una serie compleja de números y letras, e intenta evitar la utilización de una contraseña que pueda adivinarse fácilmente.
- **No permitas que el dispositivo inalámbrico indique su presencia**
  Desactiva la difusión del identificador de red SSID (Service Set Identifier) para evitar que el dispositivo inalámbrico anuncie su presencia al mundo que te rodea.
- **Cambia el nombre SSID del dispositivo**
  Al igual que antes, es muy fácil para un hacker descubrir cuál es el nombre SSID predeterminado del fabricante del dispositivo y utilizarlo para localizar la red inalámbrica. Cambia el nombre SSID predeterminado del dispositivo e intenta evitar la utilización de un nombre que pueda adivinarse fácilmente.
- **Cifra los datos**
  En la configuración de la conexión, asegúrate de que activas el cifrado. Si el dispositivo es compatible con el cifrado WPA, utilízalo; en caso contrario, utiliza el cifrado WEP.
- **Protección contra los ataques de malware e Internet**
  Asegúrate de que instalas un programa antimalware eficaz en todos los ordenadores y demás dispositivos. Con el fin de mantener actualizada la protección antimalware, selecciona la opción de actualización automática en el producto.

Medidas para la protección del router

El router es la puerta de entrada desde Internet hacia nuestra red privada por lo que configurarlo de manera correcta evitará, en la mayoría de las ocasiones, que alguien sin permiso se pueda "colar" e invada nuestra privacidad y seguridad.

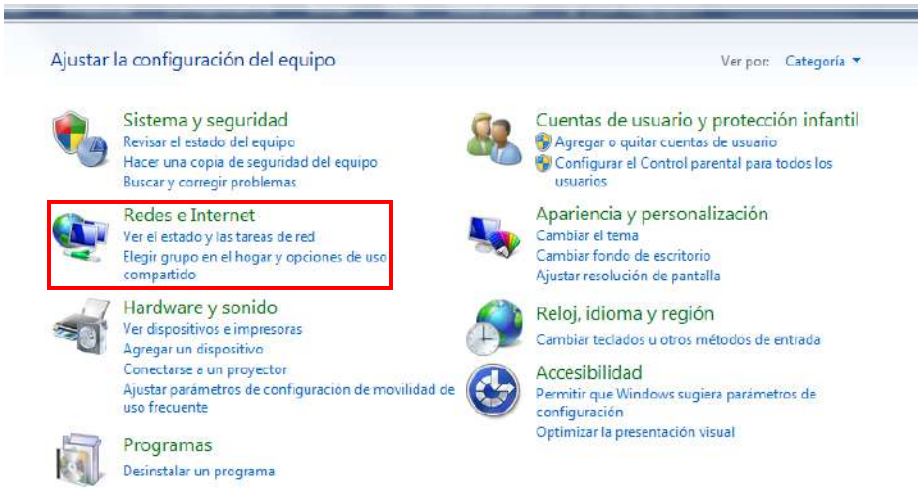
Todos los routers cuentan con una configuración de parámetros por defecto que en la mayoría de los casos no son las más apropiadas

A continuación, te mostraremos como configurar de manera segura nuestros routers.

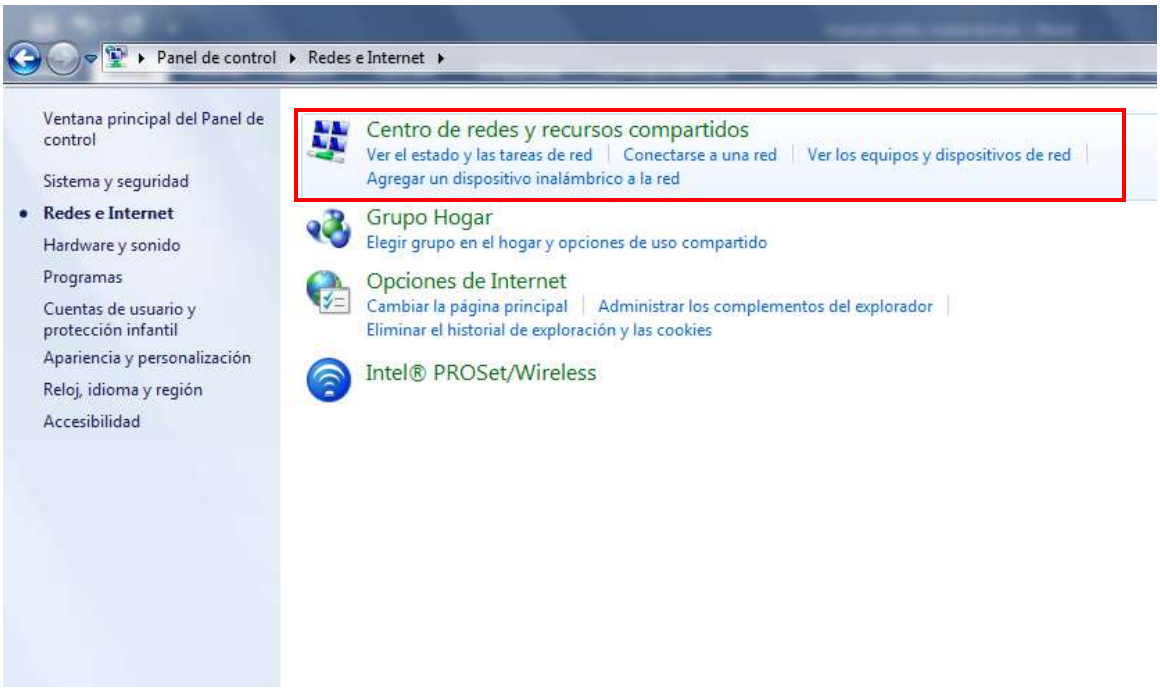
¿Cómo acceder a la configuración del router?

Para acceder a la configuración del router lo primero que hay que hacer es conocer cuál es la IP que nos permitirá acceder, normalmente coincide con lo que se denomina "Puerta de enlace". La puerta de enlace es una dirección IP que utilizan los dispositivos de nuestra red privada como pasarela para acceder a Internet.

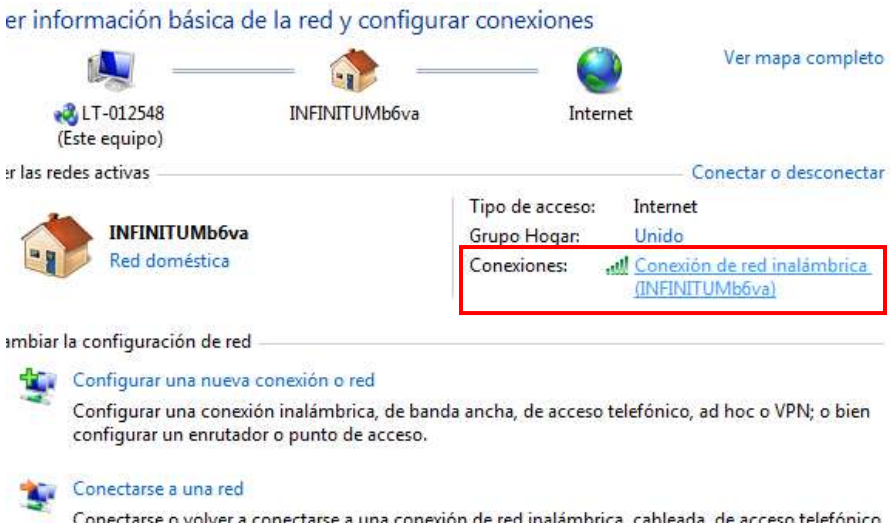
Para saber qué puerta de enlace utilizamos en Windows, independientemente de que utilicemos Windows 7, 8 ó 10, accedemos al **"Panel de control" > "Redes e Internet"**.



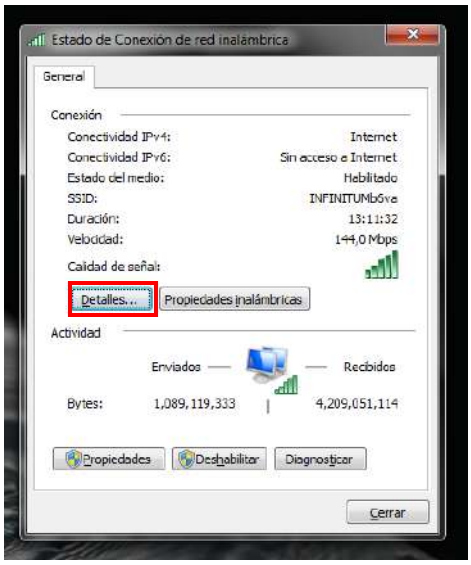
En la nueva ventana que se abrirá seleccionamos **“Centro de redes y recursos compartidos”**.



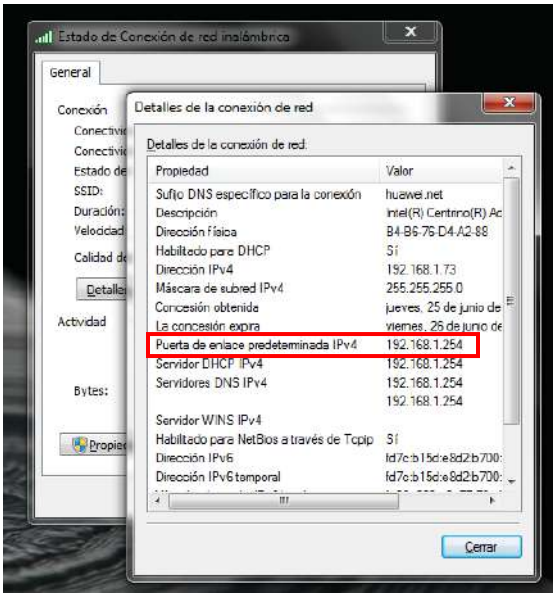
A continuación, seleccionamos el enlace de **“Conexiones”**.



En esta nueva ventana seleccionamos el botón **“Detalles”**.



En la nueva ventana que se abrirá se encuentra la propiedad **"Puerta de enlace predeterminada IPv4"** y a su derecha un valor que será nuestra puerta de enlace.



Una vez que sabemos cuál es nuestra puerta de enlace abrimos un navegador web y la escribimos en la barra de direcciones. Se abrirá una ventana en la que se nos solicita el usuario y la contraseña para acceder a la configuración del router. Estas credenciales, si no han sido modificadas, suelen estar en una pegatina en el propio router o en el manual de usuario. Al introducir la información correcta accederemos a la configuración de nuestro dispositivo.

Fuentes

redes inalambricas. (s. f.). *redesinalambricas.es*. https://www.redesinalambricas.es/#Ventajas_e_Inconvenientes_de_las_Redes_Inalambricas

Seguridad para redes Wi-Fi públicas. (s. f.). kaspersky.es. https://www.kaspersky.es/resource-center/preemptive-safety/public-wifi

Protección de las redes inalámbricas. (s. f.). kaspersky.es. https://www.kaspersky.es/resource-center/preemptive-safety/protecting-wireless-networks

Riesgos asociados a las redes Wi-Fi públicas. (2019, 5 febrero). welivesecurity. https://www.welivesecurity.com/la-es/2019/02/05/riesgos-asociados-redes-wi-fi-publicas/

Tu router, tu castillo. (2016, 3 noviembre). Oficina de Seguridad del Internauta. https://www.osi.es/es/actualidad/blog/2016/11/03/tu-router-tu-castillo-medidas-basicas-para-su-proteccion