# Introducción a redes informáticas

## ¿Qué es una red informática?

Una red consiste en un conjunto de dispositivos inteligentes (PCs, Notebooks, Tablets, Smartphones, TVs, etc.) conectados entre sí, mediante un medio físico (cables) o inalámbrico, capaces de compartir información, periféricos como Impresoras, Cámaras, y hasta una conexión a Internet. A manera de ejemplo, una red podría consistir en tan sólo tres PCs conectadas en el salón de clases o incluso una PC conectada a Internet.

Cuando conectás tu PC a Internet, estás conectándola a una red (en este caso, la denominada Red de Redes, World Wide Web o internet).

Muchas personas tienen en casa varios equipos conectados entre sí mediante una red, por lo tanto tienen el poder de intercambiar archivos (música, videos, documentos, etc) y periféricos tanto en el interior (red local) como al exterior si están conectados a Internet.

En las empresas, actualmente, es inevitable instalar una red porque es la manera más sencilla de compartir datos, recursos, sistemas de gestión y administración, video vigilancia, acceso a internet, difusión, venta online, etc.

Las redes informáticas permiten utilizar de forma fácil y eficaz **herramientas de comunicación** como los emails, mensajería instantánea, líneas telefónicas, videoconferencia.

Favorecen la **optimización del tiempo** en cuanto al intercambio de archivos y datos informáticos.

Permiten **centralizar la información y mantenerla organizada**, lo cual facilita y asegura su acceso.

Fortalecen y optimizan el **trabajo en equipo**.

Reducen **gastos** logísticos, productivos y administrativos.

Actúan como medio de difusión, venta y colaboración entre productores y consumidores.

Sólo citamos algunas de las muchas ventajas que nos ofrecen las redes informáticas actuales.

# Componentes que integran una red

Como en todo proceso de comunicación para que una red sea posible necesita dispositivos que envíen y reciban información, un medio de transmisión (cableado o inalámbrico) para transportar la información entre el dispositivo emisor y el receptor; reglas (*protocolos*) que formen un lenguaje común y permitan el entendimiento de la información intercambiada, y programas que procesen dicha información.

Cuando hablamos de informática necesariamente nos referimos a la interacción entre los componentes que podemos ver y tocar, *hardware*, y los que no tienen un componente físico ya que sólo existen a través de los circuitos de los dispositivos, el *software*.

La interacción entre el software y el hardware hace operativa una red, una PC o cualquier dispositivo informático.

## Dispositivos

*Dispositivos de usuario final y dispositivos de red.*

Los dispositivos de usuario final incluyen las computadoras, impresoras, cámaras, y demás elementos que brindan servicios directamente al usuario, y los segundos son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación, por ejemplo, módem, router, switch, access point.

Los dispositivos que utilizan la red pueden cumplir dos roles (clasificación de redes por relación funcional): servidor, en donde el dispositivo brinda un servicio para todo aquel que quiera consumirlo; o cliente, en donde el dispositivo consume uno o varios servicios de uno o varios servidores. Este tipo de arquitectura de red se denomina cliente/ servidor.

Por otro lado, cuando todos los dispositivos de una red pueden ser clientes y servidores al mismo tiempo y se hace imposible distinguir los roles, estamos en presencia de una arquitectura punto a punto o peer to peer (p2p). En Internet coexisten estos diferentes tipos de arquitecturas.

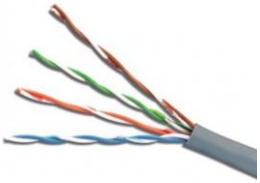
## Medio

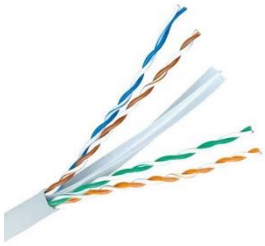
El medio hace posible que los dispositivos se relacionen entre sí. Los medios de comunicación pueden clasificarse por tipo de conexión como físicos, en donde se encuentran: el cable coaxial, el cable de par trenzado o UTP y la fibra óptica; e inalámbricos, en donde se encuentran las ondas de radio (Wi-Fi y Bluetooth), las infrarrojas, etc.

*Cable UTP o Par trenzado:* Es un tipo de cable cuya función consiste en trasladar bits (datos) de un punto a otro. Está compuesto de 8 conductores de cobre aislados por papel o plástico y trenzados en pares, lo que ayuda a disminuir el ruido y la interferencia. Las velocidades de una red cableada dependen de la categoría de sus componentes (cables, conectores, switchs, etc).

Existen varias categorías de cables, los más utilizados hoy son:

Categoría 5e (capaces de transferir 100Mb por segundo) y Categoría 6a (1000 Mb por segundo).





*Cable Coaxial*: Los cables coaxiales presentan una estructura diferente a los cables UTP. Existe una variedad muy amplia de este tipo de cables coaxiales (más de 200 tipos diferentes) cada una con una aplicación específica. Algunas observaciones sobre los cables coaxiales son:

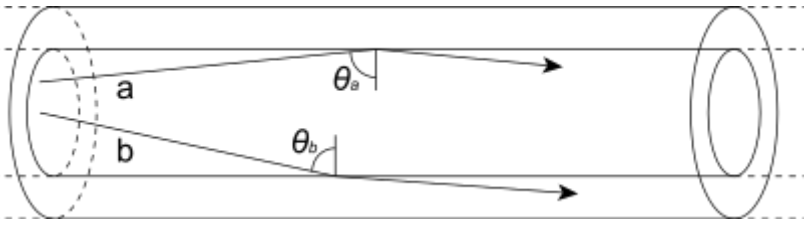
Se pueden instalar en topología de bus, estrella y árbol. Tienen coberturas de hasta 185mts. Es hasta cierto punto inmune a radiaciones electromagnéticas. Ancho de banda de 10Mbps.

*Fibra Óptica:* Una fibra óptica es una fibra flexible, transparente hecha al embutir o extruir vidrio (sílice) o plástico en un diámetro ligeramente más grueso que el de un pelo humano. Las fibras ópticas se utilizan más comúnmente como un medio para transmitir luz entre dos puntas de una fibra y tienen un amplio uso en las comunicaciones por fibra óptica, donde permiten la transmisión en distancias y en un ancho de banda (velocidad de datos) más grandes que los cables eléctricos. Se usan fibras en vez de alambres de metal porque las señales viajan a través de ellas con menos pérdida; además, las fibras son inmunes a la interferencia electromagnética, un problema del cual los cables de metal sufren ampliamente. Las fibras también se usan para la iluminación e imaginería, y normalmente se envuelven en paquetes para poder ser usados para introducir o sacar luz de espacios reducidos, como en el caso de un fibroscopio. Algunas fibras diseñadas de manera especial se usan también para una amplia variedad de aplicaciones diversas, algunas de ellas son los sensores de fibra óptica y los láseres de fibra.

Típicamente, las fibras ópticas tienen un núcleo rodeado de un material de revestimiento transparente con un índice de refracción más bajo. La luz se mantiene en el núcleo debido al fenómeno de reflexión interna total que causa que la fibra actúe como una guía de ondas. Las fibras que permiten muchos caminos de propagación o modos transversales se llaman fibras multimodo (MM), mientras que aquellas que permiten solo un modo se llaman fibras monomodo (SM). Las fibras multimodo tienen generalmente un diámetro de núcleo más grande6 y se usan para enlaces de comunicación de distancia corta y para aplicaciones donde se requiere transmitir alta potencia. Las fibras monomodo se utilizan para enlaces de comunicación más grandes que 1000 metros.

Los principios básicos de su funcionamiento se justifican aplicando las leyes de la óptica geométrica, principalmente, la ley de la refracción (principio de reflexión interna total) y la ley de Snell.

Su funcionamiento se basa en transmitir por el núcleo de la fibra un haz de luz, tal que este no atraviese el revestimiento, sino que se refleje y se siga propagando. Esto se consigue si el índice de refracción del núcleo es mayor al índice de refracción del revestimiento, y también si el ángulo de incidencia es superior al ángulo límite.




Representación de dos rayos de luz propagándose dentro de una fibra óptica. En esta imagen se percibe el fenómeno de reflexión total en el haz de luz "a".

El proceso de comunicación mediante fibra óptica implica los siguientes pasos:

Creación de la señal óptica mediante el uso de un transmisor;

Transmisión de la señal a lo largo de la fibra, garantizando que la señal no sea demasiado débil ni distorsionada;

Recepción de la señal, lo que consiste en la conversión de ésta en una señal eléctrica.

*Wifi:* Wifi es una tecnología que permite la interconexión inalámbrica de dispositivos electrónicos. Los dispositivos habilitados con wifi (tales como computadoras, teléfonos, televisores, videoconsolas, reproductores de música...) pueden conectarse entre sí o a internet a través de un punto de acceso de red inalámbrica.

Wi-Fi es una marca de la Alianza Wi-Fi, la organización comercial que adopta, prueba y certifica que los equipos cumplen con los estándares 802.11 relacionados con redes inalámbricas de área local.

Esta nueva tecnología surgió por la necesidad de establecer un mecanismo de conexión inalámbrica que fuese compatible entre distintos dispositivos. Buscando esa compatibilidad, en 1999 las empresas 3Com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies se unieron para crear la *Wireless Ethernet Compatibility Alliance*, o WECA, actualmente llamada Alianza Wi-Fi. El objetivo de la misma fue designar una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos.

Existen diversos tipos de wifi, basado cada uno de ellos en un estándar IEEE 802.11. Son los siguientes:

Los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n disfrutan de una aceptación internacional debido a que la banda de 2,4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbit/s, 54 Mbit/s y 300 Mbit/s, respectivamente.

En la actualidad ya se maneja también el estándar IEEE 802.11ac, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios. La banda de 5 GHz ha sido recientemente habilitada y, al no existir otras tecnologías (Bluetooth, microondas) que la utilicen, se producen muy pocas interferencias. Su alcance es algo menor que el de los estándares que trabajan a 2,4 GHz (aproximadamente un 10 %), debido a que la frecuencia es mayor (a mayor frecuencia, menor alcance).

Existen otras tecnologías inalámbricas como Bluetooth que también funcionan a una frecuencia de 2,4 GHz, por lo que puede presentar interferencias con la tecnología wifi. Debido a esto, en la versión 1.2 del estándar Bluetooth por ejemplo se actualizó su especificación para que no existieran interferencias con la utilización simultánea de ambas tecnologías, además se necesita tener 40 Mbit/s.

Uno de los problemas a los cuales se enfrenta actualmente la tecnología wifi es la progresiva saturación del espectro radioeléctrico, debido a la masificación de usuarios; esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). En realidad el estándar wifi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias.

Un elevado porcentaje de redes se instalan sin tener en consideración la seguridad, convirtiéndose así en redes abiertas (completamente accesible a terceras personas), sin proteger la información que por ellas circulan. De hecho, la configuración por defecto de muchos dispositivos wifi es muy insegura (routers, por ejemplo) dado que a partir del identificador del dispositivo se puede conocer la contraseña de acceso de éste y, por tanto,se puede conseguir fácilmente acceder y controlar el dispositivo.

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares wifi como el WEP, el WPA, o el WPA2 que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos. La mayoría de las formas son las siguientes:

WEP, cifra los datos en su red de forma que solo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una “clave” de cifrado antes de enviarlo al aire. Este tipo de cifrado no está recomendado debido a las grandes vulnerabilidades que presenta ya que cualquier cracker puede conseguir sacar la clave, incluso aunque esté bien configurado y la clave utilizada sea compleja.

WPA: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como dígitos alfanuméricos.

IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.

Filtrado de MAC, de manera que solo se permite acceso a la red a aquellos dispositivos autorizados. Es lo más recomendable si solo se va a usar con los mismos equipos y si son pocos.

Ocultación del punto de acceso: se puede ocultar el punto de acceso (router) de manera que sea invisible a otros usuarios.

El protocolo de seguridad llamado WPA2 (estándar 802.11i), que es una mejora relativa a WPA. En principio es el protocolo de seguridad más seguro para Wi-Fi en este momento. Sin embargo, requieren hardware y software compatibles, ya que los antiguos no lo son.

## Protocolos de red

Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores.

También se define como un conjunto de normas que permite la comunicación entre dispositivos, estableciendo la forma de identificación de estos en la red, la forma de transmisión de los datos y la forma en que la información debe procesarse.

Existen tantos protocolos en redes que llegan a ser más de cien diferentes, entre ellos se encuentran:

**ARP:** protocolo de resolución de direcciones, para encontrar la dirección física (MAC) correspondiente a una determinada IP.

**FTP:** protocolo de transferencia de archivos, popular en la transferencia de archivos.

**HTTP:** protocolo de transferencia de hipertexto, que es popular porque se utiliza para acceder a las páginas web.

**POP:** protocolo de oficina de correo, para correo electrónico.

**SMTP:** protocolo para transferencia simple de correo, para el correo electrónico.

**Telnet** (*Telecommunication Network*), para acceder a equipos remotos.

**DHCP** (Dynamic Host Configuration Protocol – Protocolo de Configuración de Anfitrión Dinámico) es la sigla que define un protocolo de configuración dinámica de direcciones, que trabaja sobre TCP/IP. Su función es asignar direcciones IP, de forma automática, a un grupo de computadoras que estén en red. La IP es como un número de documento que posee cada equipo conectado a una red, para poder identificarlo. Este mecanismo de asignación se basa en dos estándares necesarios para trabajar: un cliente y un servidor. Un servidor DHCP puede ser una PC/Servidor o un módem/router que tenga activado este servicio.

Y los dos protocolos más utilizados

**TCP:** protocolo de control de transmisión.

Muchos programas dentro de una red de datos compuesta por redes de dispositivos, pueden usar TCP para crear "conexiones" entre sí a través de las cuales puede enviarse un flujo de datos (que conforman un archivo). El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

**IP:** protocolo de internet.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas. En IP no se necesita ningún intercambio de información de control previa a la carga de datos, como sí que ocurre, por ejemplo, con TCP. El diseño del protocolo **IP** se realizó presuponiendo que la entrega de los paquetes de datos sería no confiable. Por ello, **IP** tratará de realizarla del mejor modo posible, mediante técnicas de enrutamiento, sin garantías de alcanzar el destino final pero tratando de buscar la mejor ruta entre las conocidas por la máquina que esté usando **IP**.

## Tipos de Redes

Por su medio de transmisión estableceremos dos grandes grupos, redes inalámbricas y redes cableadas.

*Inalámbricas:* En casa, conectamos desde una pc hasta un Smartphone, y estos pueden compartir desde datos, como música, videos y documentos hasta una impresora o cámara, todo mediante una conexión inalámbrica (en la mayoría de los casos). Es que las empresas que ofrecen acceso a internet, por lo menos aquí en Argentina, instalan en nuestros domicilios un Módem-Router-Wifi (más adelante veremos cómo funciona) que permite la conexión de dispositivos a

través de un enlace de radio (Wifi) y a su vez darles una puerta de salida (Gateway) a internet mediante un cable coaxil, telefónico o fibra óptica.

*Cableadas:* En la oficina, en la fábrica, en el trabajo, es más probable encontrar redes cableadas que son mucho más estables y veloces. Las redes cableadas necesitan un medio físico para transportar información de un dispositivo a otro.

Por su tamaño estableceremos 3 tipos de redes. De mayor a menor, WAN, MAN y LAN.

*WAN*: Una red de área amplia, o WAN (Wide Area Network en inglés), es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física. Muchas WAN son construidas por organizaciones o empresas para su uso privado, otras son instaladas por los proveedores de internet (ISP) para proveer conexión a sus clientes.

*MAN*: Redes de área metropolitana. Básicamente son una versión más grande de una LAN. Puede ser pública o privada.

*LAN*: Red de computadoras y/o dispositivos que abarca un área reducida a una casa, un departamento o un edificio.

Ya tenemos una noción básica sobre las ventajas de una red informática, los dispositivos, medios de transmisión y protocolos que la hacen posible, también de sus denominaciones según el medio que utilizan y el tamaño.

Profundizaremos algunos conceptos con la ayuda del siguiente ejercicio.

Nuestra primera Red

Veamos los aspectos a tener en cuenta si necesitamos armar nuestra propia red desde cero.

1- La cantidad de dispositivos que necesitamos conectar tanto ahora como en el futuro.
2- El espacio físico que queremos abarcar.
3- Tipo de Red: ¿cableada, inalámbrica, o una mezcla de ambas?
4- Hardware de red necesario.
5- Configurar y asegurar.

**Router (también conocido como enrutador):** es el dispositivo central de una red del hogar, en el que puedes conectar un extremo de un cable de red. El otro extremo del cable se coloca en el dispositivo de red que tiene un puerto de red. Si deseas agregar más dispositivos a su *router*, necesitarás más cables y más puertos en el dispositivo. Estos puertos, tanto en el router como en los dispositivos finales, se llaman puertos de Red de Área Local (LAN, por sus siglas en inglés). También se conocen como puertos RJ45. Cuando conectas un dispositivo a un *router*, ya tienes una red conectada. Los dispositivos de red que vienen con un puerto de red RJ45 se conocen como dispositivos preparados para Ethernet.


**Puertos LAN:** un router para el hogar generalmente tiene cuatro puertos LAN, lo que significa que, tal como viene de fábrica, puede albergar una red de hasta cuatro dispositivos conectados. Si deseas tener una red más grande, deberás recurrir a un conmutador (o un concentrador), que agrega más puertos LAN al router. En general, un router para casas puede administrar hasta 250 dispositivos en red, y la mayoría de los hogares y las empresas pequeñas no necesitan más que eso. En la actualidad, hay dos estándares de velocidad importantes para los puertos LAN: Ethernet (Cat. 5e), que alcanza una velocidad de 100 Mbps (o unos 13 MBps) y Gigabit Ethernet (Cat. 6ª), que alcanza 1 Gbps (o unos 125 MBps). En otras palabras, lleva alrededor de un minuto transferir los datos que caben en un CD (unos 700 MB o unas

250 canciones digitales) mediante una conexión de Ethernet. Con Gigabit Ethernet, la misma tarea lleva solo unos cinco segundos. La velocidad real de una conexión de red depende de muchos factores, como los dispositivos finales, la calidad del cable, la cantidad de tráfico, etc.

Recordemos que: *la velocidad de una conexión de red está determinada por la velocidad más baja de cualquiera de las partes involucradas*. Por ejemplo, para tener una conexión Gigabit Ethernet por cable entre dos computadoras, ambas computadoras, el router al que están conectadas y los cables usados para unirlas necesitan ser compatibles con Gigabit Ethernet. Si enchufas un dispositivo Gigabit Ethernet y un dispositivo Ethernet a un router, la conexión entre ambos tendrá una velocidad máxima igual a la velocidad de Ethernet, es decir, 100 Mbps.

En resumen, los puertos LAN de un router permiten que dispositivos preparados para Ethernet se conecten entre sí y compartan datos. Para que puedan también acceder a Internet, el router tiene que tener un puerto de Red de Área Amplia (WAN).

**Puerto WAN:** en general, un router tiene solo un puerto WAN. (Algunos routers empresariales vienen con doble puerto WAN, para que uno pueda usar dos servicios distintos de Internet al mismo tiempo). En cualquier router, el puerto WAN siempre está separado de los puertos LAN y a menudo viene en otro color para que se pueda distinguir. Un puerto WAN es exactamente lo mismo que un puerto LAN, pero con un uso distinto: para conectarse a una fuente de Internet, como un módem de banda ancha. El WAN le permite al router conectarse a Internet y compartir esa conexión con todos los dispositivos preparados para Ethernet conectados a él.

**Hub vs. Switch:** un hub y un switch agregan más puertos LAN a una red existente. Ayudan a aumentar la cantidad de clientes para Ethernet que una red puede albergar. La diferencia principal entre hub y un switch es que un hub usa un canal compartido para todos sus puertos, mientras que un switch tiene un canal dedicado para cada uno de sus puertos. Esto significa que mientras más clientes conectas a un hub, más lento se vuelve el rango de datos; mientras que con un switch la velocidad no cambia según la cantidad de clientes conectados. Por este motivo, los hubs son mucho más baratos que los switchs con la misma cantidad de puertos.

El precio de un switch suele variar en base a su categoría (Cat. 5e o Gigabit Cat. 6a, este último es más caro) y a la cantidad de puertos (más puertos, más caro).

**Módem de banda ancha:** un módem de banda ancha, a menudo llamado módem DSL o módem por cable, es un dispositivo que une la conexión de Internet de un proveedor de servicio con una computadora o router para que los clientes dispongan de Internet. En general, un módem tiene un puerto LAN (para conectarlo al puerto WAN de un router o a un dispositivo preparado para Ethernet) y un puerto relacionado con el servicio, como un puerto de teléfono (módems DSL) o un puerto coaxial (módems por cable), que se conecta a la línea de servicio. Si solo tienes el módem, solo podrás conectar a Internet un dispositivo preparado para Ethernet, como una computadora. Para conectar más de un dispositivo a Internet, necesitarás un router. Algunos proveedores ofrecen un dispositivo en combo, que es una combinación de un módem y un router, o router inalámbrico, todo en uno.

**Punto de acceso:** un punto de acceso (AP) es un dispositivo central que emite la señal Wi-Fi para que los clientes Wi-Fi se conecten a ella. En general, cada red inalámbrica, como aquellas

que ves que aparecen en la pantalla de su teléfono inteligente mientras paseas por una ciudad grande, pertenece a un punto de acceso. Puedes comprar un AP por separado y conectarlo a un router o a un conmutador para agregar apoyo Wi-Fi a una red cableada, pero en general, es preferible comprar un router inalámbrico, que es un router normal (un puerto WAN, cuatro puertos LAN, etc.) con un punto de acceso integrado. Algunos routers incluso vienen con más de un punto de acceso (vea el router de doble banda a continuación).

Cliente Wi-Fi: un cliente Wi-Fi o un cliente WLAN es un dispositivo que puede detectar la señal emitida por un punto de acceso, conectarse a ella y mantener la conexión. (Este tipo de conexión Wi-Fi se establece en el modo Infraestructura, pero no necesita saber eso). Prácticamente todas las computadoras portátiles, teléfonos inteligentes y tabletas del mercado vienen con capacidad Wi-Fi integrada. Aquellos que no la traen, pueden actualizarse mediante USB o adaptador de Wi-Fi PCIe. Piensa en un cliente Wi-Fi como un dispositivo con un puerto de red y un cable de red invisibles. El cable metafórico es tan largo como el rango de una señal de Wi-Fi.

**Rango de Wi-Fi:** este es el radio que un punto de acceso de señal de Wi-Fi puede alcanzar. Generalmente, una red Wi-Fi es más viable dentro de los 45 m del punto de acceso. La distancia, sin embargo, cambia dependiendo de los dispositivos involucrados, el entorno y, lo más importante, el estándar de Wi-Fi. Un buen punto de acceso Wireless-N puede ofrecer un rango de hasta unos 90 m o aun mayor. El estándar de Wi-Fi también determina cuán rápida puede ser una conexión inalámbrica y es el motivo por el que el Wi-Fi se vuelve complicado y confuso, especialmente cuando se mencionan las bandas de frecuencia, lo cual acabo de hacer.

**Bandas de frecuencia:** estas bandas son las frecuencias de radio que usan los estándares de Wi-Fi: 2.4 GHz, 5 GHz y 60 GHz. La banda de 2.4 GHz es actualmente la más popular, es decir, la usan la mayoría de los dispositivos de red existentes. Eso, más el hecho de que los electrodomésticos del hogar, como los teléfonos inalámbricos, también usen esta banda, hace que la calidad de su señal sea generalmente peor que la de la banda de 5 Ghz, debido a la saturación e interferencia. Solo el estándar 802.11ad usa la banda de 60 GHz.

Según el estándar, algunos dispositivos Wi-Fi usan una de las dos bandas de 2.4 GHz y 5 GHz, mientras que otros usan las dos y se los conoce como "dispositivos de doble banda". Pocos dispositivos también soportan bandas de 60 GHz y son "dispositivos tribanda". A continuación, están los estándares de Wi-Fi, comenzando por el más viejo:

802.11b: este fue el primer estándar inalámbrico que se comercializó. Ofrece una velocidad máxima de 11 Mbps y funciona solo en la banda de frecuencia de 2.4 GHz. El estándar se lanzó en 1999 y ahora es totalmente obsoleto; los clientes de 802.11b, sin embargo, funcionan con puntos de acceso de estándares de Wi-Fi posteriores.

802.11a: similar al 802.11b en términos antigüedad, el 802.11a ofrece una capacidad de velocidad de 54 Mbps a costa de un rango mucho más corto, y usa la banda de 5 GHz. También es obsoleto ahora, a pesar de que aún funciona con puntos de acceso de estándares posteriores.

802.11g: introducido en 2003, con el estándar 802.11g se empleó por primera vez el término Wi-Fi para referirse a las redes inalámbricas. El estándar ofrece una velocidad máxima de

54 Mbps pero funciona en la banda de 2.4 GHz, ofreciendo, por ende, mejor rango que el estándar 802.11a. Este estándar funciona con puntos de acceso de estándares posteriores.

802.11n o Wireless-N: disponible desde 2009, el 802.11n ha sido el estándar de Wi-Fi más popular, con muchas mejoras respecto de los previos, como hacer al rango de la banda de 5 GHz comparable con el de la banda de 2.4 GHz. El estándar funciona en las bandas de 2.4 GHz y 5 GHz y comenzó una nueva era de routers de doble banda, aquellos que vienen con dos puntos de acceso, uno para cada banda. Hay dos tipos de routers de doble banda: routers de doble banda seleccionable, que pueden funcionar en una banda a la vez, y routers de doble banda real, que ofrecen de manera simultánea señales de Wi-Fi en ambas bandas.

En cada banda, el estándar Wireless-N está disponible en tres configuraciones, según la cantidad de flujos espaciales que se usen: un flujo, dos flujos y tres flujos, que ofrecen velocidades límite de 150, 300 y 450 Mbps, respectivamente. Esto, a cambio, crea tres tipos de routers de doble banda real: N600 (cada una de las bandas ofrece un límite de velocidad de 300 Mbps), N750 (una banda tiene un límite de velocidad de 300 Mbps y la otra, de 450 Mbps) y N900 (cada una de las bandas ofrece una velocidad límite de 450 Mbps).

## Dirección IP

La dirección IP es un número que identifica, de manera lógica y jerárquica, a una placa de red de un dispositivo (computadora, tableta, portátil, smartphone) que utilice el protocolo IP o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP. La dirección IP no debe confundirse con la *dirección MAC*, que es un identificador de 48 bits expresado en código hexadecimal, para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado en la red.

La dirección IP puede cambiar muy a menudo debido a cambios en la red, o porque el dispositivo encargado dentro de la red de asignar las direcciones IP, decida asignar otra IP (por ejemplo, con el protocolo DHCP). A esta forma de asignación de dirección IP se le denomina también dirección IP dinámica (normalmente abreviado como IP dinámica).

Los dispositivos se conectan entre sí mediante sus respectivas direcciones IP.

IP son las siglas de "**Internet Protocol**» que, si lo traducimos al español, significa «**Protocolo de Internet**". Este protocolo, al igual que otros muchos como HTTP, TCP, UDP, etc., se encarga de establecer las comunicaciones en la mayoría de nuestras redes. Para ello, asigna una **dirección única e irrepetible a cada dispositivo** que trata de comunicarse en una red.

No existe dispositivo en el mundo que pueda comunicarse con otro sin tener una IP. Las direcciones IP son los nombres numéricos que se asignan a un dispositivo a modo de «patente» para que pueda ser llamado por otros dispositivos. Existen dos tipos de IP: las direcciones IP públicas y las direcciones IP privadas.

Tanto las direcciones IP públicas como las privadas están construidas en cuatro bloques numéricos, cuatro octetos (8 bits cada uno). Cada bloque es un número del 0 al 255 y está separado por un punto («.»). Por ejemplo, una dirección IP pública podría ser 63.45.12.34 y una dirección IP privada, 192.168.0.11

Una dirección *IP Privada* se utiliza para identificar equipos o dispositivos dentro de una red doméstica o privada. Pueden ser dinámicas (asignadas por un servidor DHCP que puede ser un Router o una PC Servidor) o fijas asignadas manualmente en las propiedades de la placa de red de los dispositivos.

Se utilizan para IP Privadas 3 rangos de direcciones:

Clase A: 10.0.0.0 a 10.255.255.255

Clase B: 172.16.0.0 a 172.31.255.255

Clase C: 192.168.0.0 a 192.168.255.255

CLASE A: Usada para las redes gigantescas, como las de las empresas internacionales. El primer bloque de la dirección es usado para identificar la red, mientras los otros tres bloques son usados para identificar a los dispositivos (xxx.yyy.yyy.yyy). Esto nos permite crear hasta 126 redes distintas y tener un máximo de 16.777.214 equipos conectados por red.

CLASE B: Usadas por redes de tamaño mediano, como puede ser una universidad o instituciones de similar envergadura. Utiliza los dos primeros bloques para identificar la red, mientras que los dos restantes son utilizados para identificar a los dispositivos conectados (xxx.xxx.yyy.yyy). Esto nos permite crear un mayor número de redes, pero menos equipos conectados por red (16.384 redes y 65.534 equipos).

CLASE C: Las que el 99% de la población usamos. Son reservadas para pequeñas redes domésticas. Los tres primeros bloques son usados para identificar la red y el último como identificador de equipo (xxx.xxx.xxx.yyy). Esto nos hace tener más redes distintas aún, pero menor número de equipos por red (2.097.152 redes y 254 equipos por red).

En una red, las direcciones IP Privadas deberán ser únicas para cada dispositivo o al duplicarlas surgirán problemas.

La *IP pública* es el identificador de nuestra red desde el exterior, es decir, la de nuestro router en casa u oficina, que es el que es visible desde fuera, mientras que la privada es la que identifica a cada uno de los dispositivos conectados a nuestra red, por lo tanto, cada una de las direcciones IP que el router (a través del servicio DHCP) asigna a cada dispositivo conectado a nuestra red. Por lo tanto, todos los dispositivos conectados a un mismo router tienen distintas direcciones IP privadas, pero la misma IP pública, ya que es la del router, que actúa como puerta de enlace a internet.

Normalmente estas direcciones IP suelen ser rotadas por tu ISP (proveedor de internet) cada vez que reinicias el router o cada cierto tiempo. A estas direcciones IP se las conoce como direcciones IP dinámicas. Si por algún motivo necesitamos tener una dirección IP estática o fija para un dispositivo, debemos ponernos en contacto con el ISP y solicitar que nos asignen una IP fija asociada a la dirección MAC de nuestro Router.

Cuando nació Internet existían muy pocos servidores y **la única forma de acceder a ellos era saber su dirección IP pública**. Si una persona quería acceder a un recurso determinado no alcanzaba con escribir, por ejemplo, **diariociudadano.com** (porque aún no existían los nombres de dominio), sino que tenía que conocer la dirección IP del servidor donde estaba alojado ese recurso. **Imaginemos que la dirección IP de ese servidor fuera: 156.87.234.176**.

No es útil, eficiente ni fácil recordar todos esos números. Los centros de datos seguían creciendo y cada vez albergaban más servidores con más información diferente. ¡Sería una locura tener que recordar cada dirección IP para cada recurso! **Por eso nacieron los** nombres de dominio.

Actualmente, usamos los famosos *DNS (Domain Name Servers)* para **suplantar con un nombre de dominio a una dirección IP**. Ahora, para acceder a un material de **diariociudadano.com** ya no hay que poner la IP 156.87.234.176 sino indicar **diariociudadano.com**. Usar nombres de dominio tiene una lista de ventajas enorme frente a usar direcciones IP:

Son más fáciles de recordar que una dirección IP

Son más cortos

Son más fáciles de escribir

Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.2

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio Google es 216.58.210.163, la mayoría de la gente llega a este equipo especificando www.google.com y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable.3 La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre del sitio web. Incluso, en el caso de que una página web utilice una red de distribución de contenidos (Content delivery network o CDN, por sus siglas en inglés) por medio del DNS el usuario recibirá la dirección IP del servidor más cercano según su localización geográfica (cada CDN a su vez tiene sus propios servidores DNS).

Los usuarios generalmente no se comunican directamente con el servidor DNS: la resolución de nombres se hace de forma transparente por las aplicaciones del cliente (por

ejemplo, navegadores, clientes de correo y otras aplicaciones que usan Internet). Al realizar una petición que requiere una búsqueda de DNS, la petición se envía al servidor DNS local del sistema operativo. El sistema operativo, antes de establecer alguna comunicación, comprueba si la respuesta se encuentra en la memoria caché (memoria temporal). En el caso de que no se encuentre, la petición se enviará a uno o más servidores DNS, el usuario puede utilizar los servidores propios de su ISP, puede usar un servicio gratuito de resolución de dominios, por ejemplo: OpenDNS 208.67.220.220 / 208.67.222.222, Google 8.8.8.8 / 8.8.4.4, o contratar un servicio avanzado de pago que por lo general son servicios contratados por empresas por su rapidez y la seguridad que estos ofrecen.

## Redes de Grupo de Trabajo

Los grupos de trabajo son una de las posibles formas de organizar los equipos dentro de una red local.

La totalidad de equipos pertenecientes a un mismo grupo de trabajo podrán verse y comunicarse entre ellos. Este hecho proporcionará las siguientes ventajas:

Los equipos pertenecientes a un mismo grupo podrán compartir archivos y directorios entre ellos de forma extremadamente sencilla.

Los equipos pertenecientes a un mismo grupo podrán compartir recursos como por ejemplo impresoras, etc.

En ningún momento los grupos de trabajo sirven para centralizar o gestionar permisos de equipos. La administración de usuarios y privilegios se hará de forma individual en cada uno de los equipos que forman parte del grupo de trabajo. Cada uno de los equipos pertenecientes a un grupo de trabajo tienen una relación de igual a igual entre ellos y se administran de forma local.

Los grupos de trabajo son útiles para ser usados en redes locales pequeñas. Por lo tanto, los grupos de trabajo son una buena solución para usarlos en nuestro hogar. En ambientes corporativos es más recomendable usar dominios.

### *PROPIEDADES DE LOS GRUPOS DE TRABAJO*

Las características básicas de los equipos que forman parte de grupos de trabajo son las siguientes:

La relación entre todos los equipos de un grupo de trabajo es de igual a igual. Por lo tanto, ningún ordenador perteneciente al grupo tiene control sobre el otro.

El número de equipos que forma un grupo de trabajo acostumbra a ser bajo. Si disponemos de un grupo de trabajo con más de 20 equipos deberíamos plantearnos migrar a un dominio.

Para que los usuarios de un grupo de trabajo puedan verse entre ellos deben encontrarse en la misma red local.

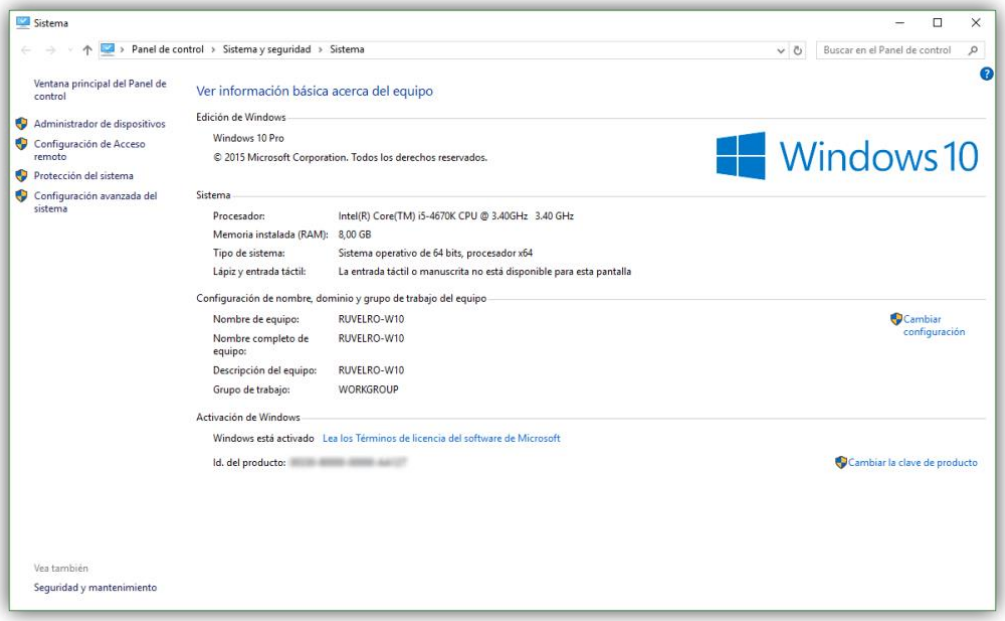
Cada equipo perteneciente al grupo de trabajo debe disponer de su cuenta de usuario local. Por lo tanto, para iniciar la sesión en un equipo perteneciente a un grupo de trabajo debemos disponer de una cuenta de usuario en este equipo.

Todos los usuarios de una red local pueden pertenecer a un grupo de trabajo sin necesidad de pedir permiso ni introducir ninguna contraseña. Por lo tanto, cuando compartimos una carpeta hay que configurar de forma adecuada los permisos y los usuarios que tendrán acceso a nuestra carpeta compartida.

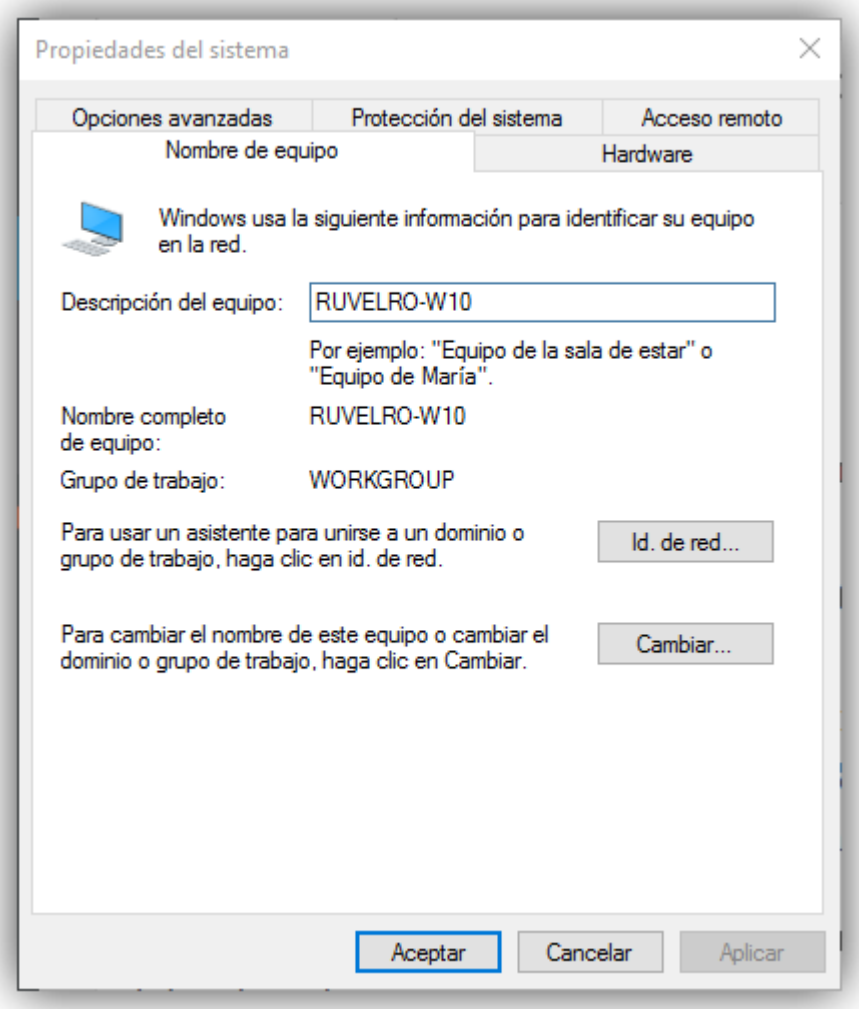
### *Cómo configurar los nombres de los equipos y el grupo de trabajo*

Lo primero que debemos hacer es asignar a cada PC un nombre de equipo (con el cual se identificarán en la red) y un grupo de trabajo por donde compartirán la información. Si queremos que dos o más PCs se conecten entre sí, entonces cada uno debe tener un nombre diferente pero todos ellos pertenecer al mismo grupo de trabajo.

Para ello, desde nuestro escritorio de Windows, hacemos clic con el botón derecho sobre “Este equipo” y abrimos la ventana de propiedades del ordenador. Otra manera es abriendo el Explorador de archivos y hacer click derecho sobre “Equipo” a la izquierda de la ventana.

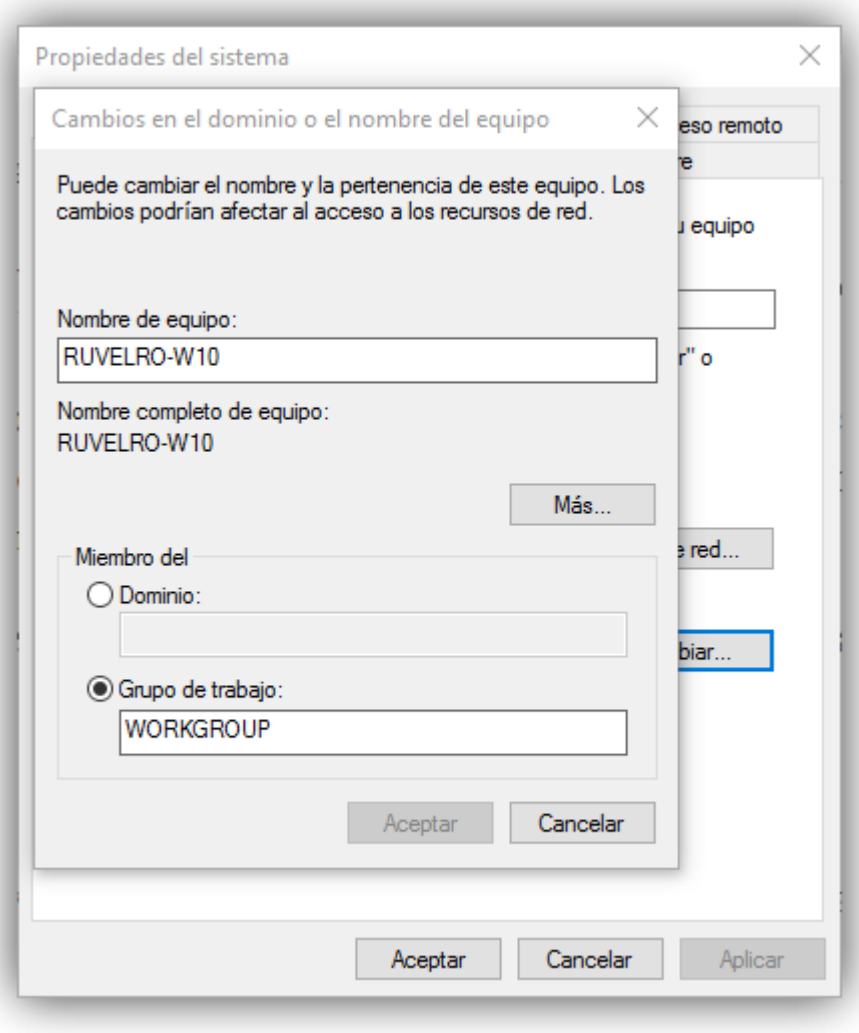


Aquí, en el apartado “Configuración de nombre, dominio y grupo de trabajo” pulsamos sobre el botón “Cambiar configuración”. Se nos abrirá una nueva ventana similar a la siguiente.




Aquí veremos un apartado llamado “Descripción”, donde podemos añadir, solo a nivel informativo, una pequeña descripción sobre el ordenador.

Para cambiar tanto el nombre del equipo como el grupo de trabajo debemos hacer clic sobre el botón “Cambiar”. Veremos una nueva ventana como la siguiente.




Desde aquí sí que vamos a poder cambiar la configuración del equipo. Lo primero que haremos será darle al equipo un nombre único en la red de trabajo. También asignaremos un nuevo grupo. Por defecto, Windows suele asignar “Workgroup” como grupo de trabajo, sin embargo, podemos poner lo que queramos, siempre y cuando en todos los equipos sea lo mismo.

Una vez realizados los cambios reiniciamos el equipo para que estos se apliquen correctamente. Cuando nos volvamos a conectar ya lo haremos dentro del nuevo grupo y con el nuevo nombre de cara a la red.

# Seguridad

Entendemos por seguridad informática el conjunto de acciones, herramientas y dispositivos cuyo objetivo es dotar a un sistema informático de integridad, confidencialidad y disponibilidad. Tenemos que ser conscientes de que las pérdidas de información no pueden venir sólo de ataques externos sino que pueden producirse por errores nuestros o por accidentes o averías en los equipos. El elemento clave de un sistema de información son los datos y hay dos principales amenazas externas al software y a los datos: 2.1 Código malicioso (malware)2.2 Ingeniería social2.1 Código malicioso (malware)El código malicioso o malware, es un programa que tiene como objetivo introducirse y hacer daño en un ordenador sin que el usuario lo note. Entre sus objetivos podemos señalar:- Robar información, datos personales, claves, números de cuenta.- Crear redes de ordenadores zombis, denominadas también botnet, para ser utilizadas en el envío masivo de spam, phishing, realización de ataques de denegación de servicio.- Cifrar el contenido de determinados archivos para solicitar el pago de una cantidad para solucionarlo. Hay diferentes tipos de malware entre los que podemos destacar los siguientes:

*Virus* Es un código malicioso que tiene como objetivos alterar el funcionamiento de un ordenador sin el nocimiento del usuario. Por lo general incorporan código infectado en archivos ejecutables activándose los virus cuando se ejecuta este archivo. En ese momento el virus se aloja en la memoria RAM y se apodera de los servicios básicos del sistema operativo. Cuando el usuario ejecuta otro archivo ejecutable, el virus alojado en la RAM lo infecta también para ir de esta manera replicándose.

*Gusanos* Es un tipo de virus. La principal diferencia entre gusano y virus es que el gusano no necesita la intervención humana para ser propagado, lo hace automáticamente, no necesita alojarse en el código anfitrión, se propaga de modo autónomo, sin intervención de una persona que ejecute el archivo infectado. Suelen apropiarse de los servicios de transmisión de datos para controlarlo. Por lo general los gusanos consumen mucha memoria provocando que los equipos no funcionen adecuadamente. Uno de los sistemas que utiliza el gusano para propagarse es enviarse a sí mismo mediante correo electrónico a los contactos que se encuentran en el ordenador infectado.

*Troyanos* Son programas aparentemente inofensivos que tienen una función no deseada. Son realmente un programa dañino con apariencia de software útil que puede acabar siendo una gran amenaza contra el sistema informático. Ejemplos de virus que se pueden identificar como troyanos serían: *Puertas traseras (backdoors):* Modifican el sistema para permitir una puerta oculta de acceso al mismo de modo que el servidor toma posesión del equipo como si fuese propio lo que permite tener acceso a todos los recursos, programas, contraseñas, correo electrónico, unas veces en modo de vigilancia y otras para modificar la información y utilizarla con fines no licítos.

*Keyloggers:* Almacenan todas las pulsaciones del teclado que realiza el usuario. Se utilizan normalmente para robar contraseñas.

*Spyware:* Envía información del sistema el exterior de forma automática. Es un código malicioso que, para instalarse en un ordenador, necesita la participación de un virus o troyano, aún que también puede estar oculto en los archivos de instalación de un programa normal. Su cometido es obtener información de los usuarios que utilizan ese ordenador. E objetivo más leve y más comunes aportar los datos a determinadas empresas de marketing online que, con posterioridad y por diferentes medios, correo electrónico, pop-ups, enviarán publicidad al usuario sobre los temas que detectaron que les podían interesar. Estos programas espía pueden indagar en toda la información existente en el equipo, como listas de contactos, información recibida, enviada, por ejemplo el dni, números de tarjetas de crédito, cuentas bancarias, domicilios, teléfonos, software que tiene instalado, direcciones ip, servidores de internet que utiliza, páginas web que visita, tiempo de permanencia en un sitio web, etc. Por otra parte, el spyware puede servir como sistema de detección de delitos cometidos a través de internet, es muy representativa la utilización por la Policía española de código malicioso incorporado a fotos de menores que permite identificar casos de corrupción de menores y pederastia.

*Adware:* Programas de publicidad que muestran anuncios, generalmente mediante ventanas emergentes o páginas del navegador. Los equipos se pueden infectar si ejecutan algún programa no adecuado, con código maligno, generalmente recibido por correo electrónico como adjunto al mismo o bien descargado de internet. A veces también es posible que sea instalado directamente en el equipo por una persona con acceso físico al mismo.

*Bot malicioso* También son conocidos como robot web, bot es la simplificación de robot, se trata de un programa que pretende emular el comportamiento humano. Hay bots con fines lúdicos, que buscan mantener un chat con una persona, ser contrincante en un juego o de rastreo como los que usan los buscadores google o yahoo que tienen como finalidad detectar el movimiento que se produce en los sitios webs a los que enlazan y ofrecen las novedades en las búsquedas de los usuarios. Los bots maliciosos son realmente troyanos de puerta trasera, con la particularidad de que se instalan en los equipos vulnerables mediante el sistema de rastreo en internet. Una vez infectado el equipo envía una señal a su creador y pasa a formar parte de una botnet o red de bots.

A los bots se les denomina zombis, pues cumplen las órdenes de los ciberdelincuentes que los crearon. Así pueden reenviar spam y virus, robar información confidencial o privada, enviar órdenes de denegación de servicio en internet o hacer clic automáticamente en anuncios publicitarios en la página web del ciber delincuente que pagan por clic efectuado

*Virus de macro* También se denominan macro virus, son un subtipo de virus que es creado en macros inscritas en documentos, páginas web, presentaciones, ... Si el ordenador de la víctima abre un documento infectado la macro pasa a la biblioteca de macros de la aplicación que ejecuta, con lo que la macro acabará ejecutándose en los diferentes documentos que se abran con esta aplicación. Los resutados de ejecución de este virus son muy variados, desde auto-enviar un documento por correo electrónico a una dirección definida en la macro hasta realizar cálculos matemáticos erróneos.

*Ingeniería social* Es la manipulación inteligente de la tendencia natural de la gente a confiar. Consiste en obtener información a través de las personas que la utilizan. No es necesario

recurrir a programas complejos, código malicioso o estrategias para entrar en sistemas informáticos utilizando puertas traseras aprovechando la vulnerabilidad del software o del sistema operativo. Utiliza los más antiguos métodos de engaño y timo, pero utilizados a nivel informático con la máxima de que el ser humano es el eslabón más débil de la cadena, cuando nos referimos a seguridad de los sistemas de información. El método principal es el correo electrónico, las cadenas de correos buscan obtener direcciones de correo electrónico para poder enviarles spam, un correo de este tipo se multiplica de forma exponencial con lo que más tarde o más temprano lo vuelve a recibir pero averiguando cientos de direcciones de email. A veces pueden buscar colapsar los servidores de correo o los correos millonarios como la lotería de los nigerianos que se comprometían a entregarte una gran cantidad de dinero si le proporcionabas una cuenta para meter la cantidad ganadora. Dentro de la ingeniería social está el método conocido como phishing, palabra parecida al término inglés de pescar phishing pero con la p de password. Puede llegar a través de un correo electrónico de gente desconocida o de sitios webs de poca confianza pero en ocasiones parece que proviene de contactos conocidos, bancos o organismos oficiales. Por tratarse de correos de fuentes de confianza, aumentan las posibilidades de que la víctima llegue a caer en la trampa. Un ejemplo típico es el de que la víctima recibe un correo electrónico de su director de su oficina bancaria en el que se le comunica que el nuevo método de acceder a banca electrónica es pulsando sobre un enlace que le envía realmente a una web fraudulenta con apariencia similar a la real. El objetivo es hacerse con el nombre de usuario y la contraseña real para poder operar con ellas en su nombre. Ejemplos de phishing.

## Problemas comunes y/o recurrentes en redes Lan

Muchas veces, al enfrentarnos a estas situaciones pensamos que hay un complejo problema que afecta nuestra red, suele no ser así y muchas veces se puede lograr una mejora significativa sólo con revisar las cosas más básicas.

*"No tengo internet, no funciona por cable, tampoco por wifi"*

Ningún dispositivo de la red tiene salida a internet, de ninguna manera.

Soluciones posibles: Primero comprobar que el problema sea la red lan o el proveedor de internet llamando al soporte del proveedor (ISP: Internet Service Provider) y realizar las pruebas solicitadas, entre ellas, seguramente, reiniciar el módem/router para liberar cache.

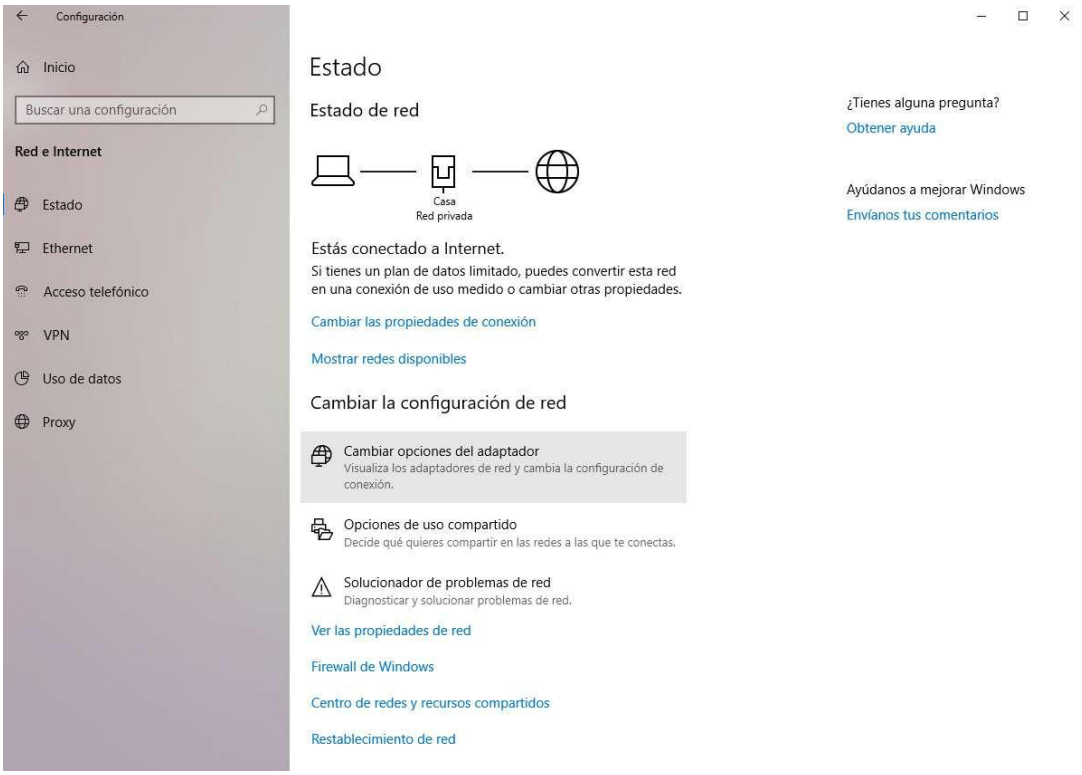
En el caso de disponer de un Router propio conectado al módem de nuestro proveedor, comprobar la conexión física, el cable de red que los conecta, controlando que las luces indicadoras de conexión para la boca de red usada WAN o INTERNET este encendida y/o parpadeando. Acceder a la configuración de nuestro Router y comprobar que tenemos asignada una dirección IP WAN y que tenemos habilitado el servicio DHCP.

### *Conflictos con direcciones IP*

Los servidores DHCP, en general, poseen sistemas que les ayuda a prevenir que asignen una IP repetida a un equipo en la red, sin embargo puede ocurrir que 2 equipos tengan la misma IP dentro de la misma red lan, ya que uno de ellos puede estar configurado con una IP estática de manera manual. Esto se conoce como IP Duplicada en la red. Solución: Identificar las direcciones de IP asignadas por el servidor DHCP y la del equipo con problemas. Cambiar la dirección IP del equipo con dirección IP estática por una que no esté siendo utilizada o, mejor aún, configurarlo para que reciba una dirección IP automáticamente del servidor DHCP evitando futuros nuevos conflictos. Recuerden siempre la utilidad de CMD: IPCONFIG /ALL

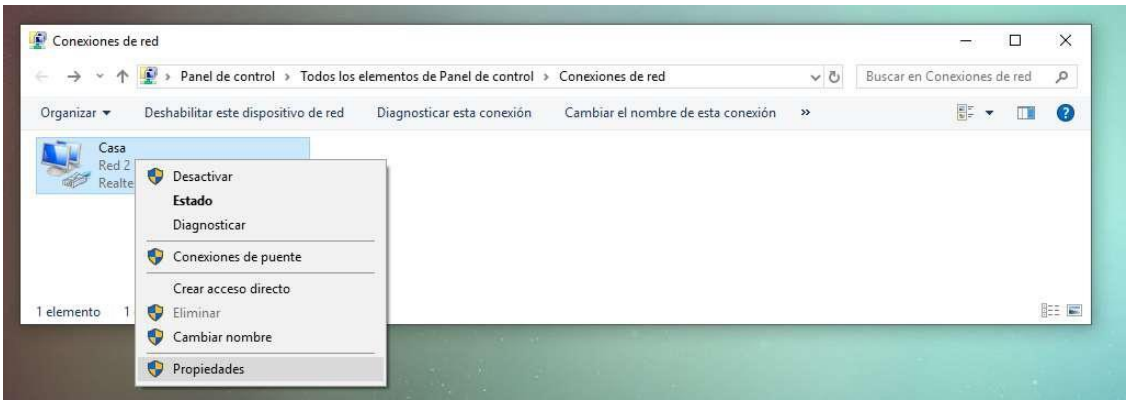
Para cambiar una dirección IP en nuestra placa de red o configurarla para obtenerla automáticamente vamos a acceder al **menú de configuración de Windows 10**. Esto puede hacerse desde el icono de la rueda dentada del menú de inicio, desde el panel de notificaciones pulsando en “todas las configuraciones” o escribiendo Configuración en el buscador.


Una vez en “Configuración de Windows” tendremos que abrir el menú de “Red e Internet” y buscaremos la opción “Cambiar opciones del adaptador”.

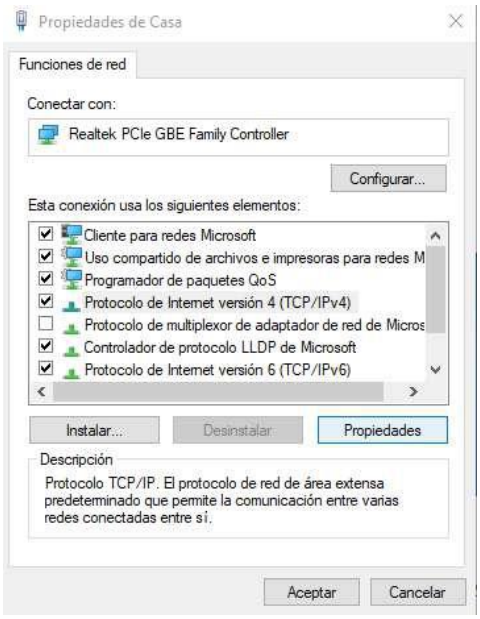



Eso nos abrirá el Panel de Control clásico en su opción de Conexiones de Red ya que esta función todavía no está migrada al nuevo menú de configuración de Windows 10**. Por eso, en Windows 7 y 8.1 podemos llegar a este punto sin tener que hacer todo lo anterior con sólo abrir el Panel de Control.**

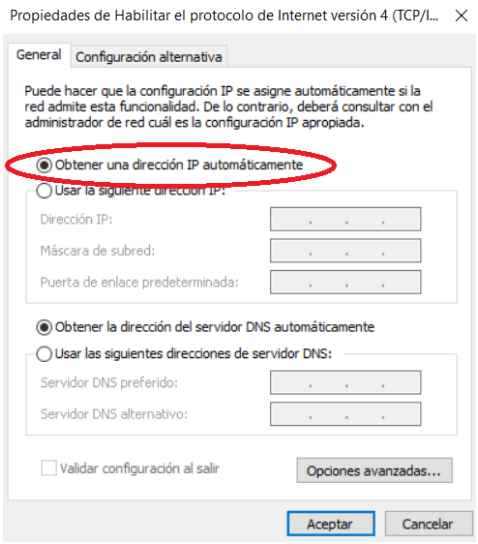

Ahora tendremos que localizar la conexión que queremos configurar, ya sea Red Cableada o Red Inalámbrica.




Pulsaremos con el botón derecho del ratón sobre el adaptador de red y pincharemos en Propiedades. Dentro de la pestaña Funciones de Red buscaremos el elemento Protocolo de Internet versión 4 (TCP/IPv4) que marcaremos y pulsaremos en el botón Propiedades de la parte inferior.




Eso nos abrirá el menú de configuración de la IP en el que tendremos que realizar los cambios deseados, modificar la ip estática actual o pulsar sobre la opción Obtener una dirección IP automáticamente.




Faltará marcar la casilla “Validar configuración al salir” y pulsar en Aceptar para que todo quede. Para comprobar que los cambios se han aplicado correctamente, abriremos CMD o símbolo de sistema y escribiremos ipconfig /all.

### *Falla en los servidores DNS*

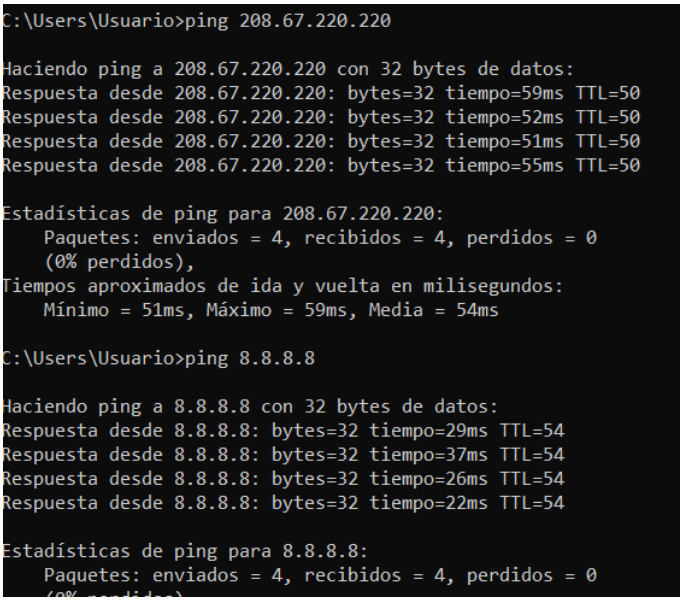
Este tipo de falla se manifiesta cuando al intentar navegar cualquier sitio web a través de cualquier navegador recibimos una página de error, por ejemplo “No se puede cargar la página NAME NOT RESOLVED”. Sin embargo nuestro ícono de red, ya sea cableada o inalámbrica, figuran con conexión, y hasta podemos otros servicios como el cliente de correo (Outlook, Thunderbird, etc) sin problemas.

Estamos, muy probablemente ante un problema con nuestros servidores DNS (Domain Name Server). Solución: Identificar cuáles son los servidores DNS que estamos utilizando (CMD IPCONFIG /ALL).

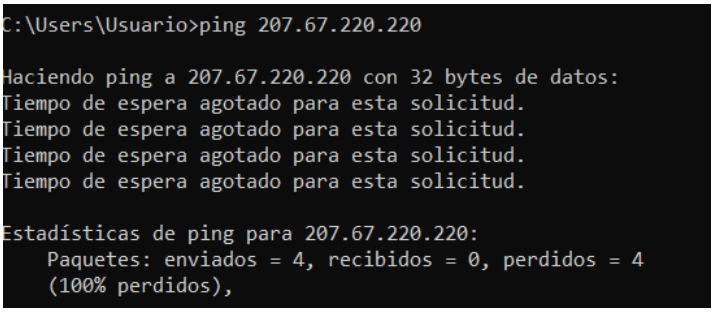
```
Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Adaptador de red 802.11n Broadcom
   Dirección física. . . . . . . . . . . . . : 08-ED-B9-85-AD-45
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local. . . : fe80::6916:7999:4b2e:5d1e%9(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.8(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Concesión obtenida. . . . . . . . . . . . : lunes, 3 de junio de 2019 20:17:53
   La concesión expira . . . . . . . . . . . : lunes, 3 de junio de 2019 22:07:20
   Puerta de enlace predeterminada . . . . . : 192.168.0.1
   Servidor DHCP . . . . . . . . . . . . . . : 192.168.0.1
   IAID DHCPv6 . . . . . . . . . . . . . . . : 168357305
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-23-EC-25-F9-E0-DB-55-97-C6-F7
   Servidores DNS. . . . . . . . . . . . . . : 208.67.220.220
                                               8.8.8.8
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

Hacer PING a cada uno de esos servidores y verificar si responden, como en la siguiente imagen.




O no responden como en la siguiente.




Si este fuera el caso procederemos a cambiar los servidores DNS que estamos utilizando de las siguientes maneras, pero antes vamos a asegurarnos de utilizar servidores DNS abiertos y funcionales, por ejemplo:

208.67.220.220 / 208.67.222.222 OPENDNS

8.8.8.8 / 8.8.4.4 GOOGLE

209.244.0.3 / 209.244.0.4 Level3

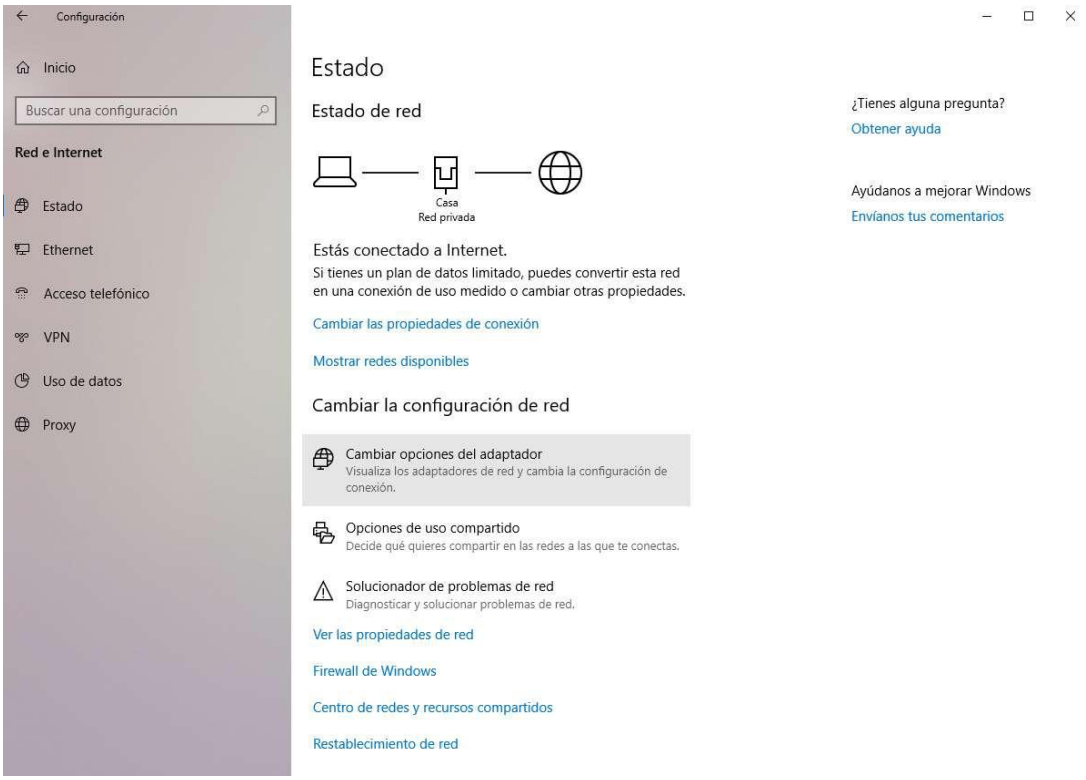
9.9.9.9 IBM Quad9

Ahora que sabemos que DNS utilizar lo primero es acceder al **menú de configuración de Windows 10**.

Verán que repetiremos algunos pasos siempre que querramos modificar configuraciones sobre los adaptadores de red en Windows.

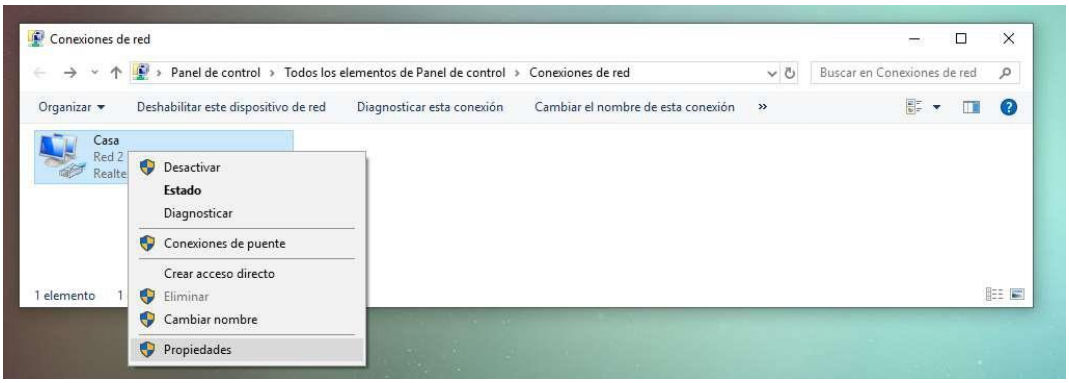
Esto puede hacerse desde el icono de la rueda dentada del menú de inicio, desde el panel de notificaciones pulsando en “todas las configuraciones” o escribiendo Configuración en el buscador.


Una vez en “Configuración de Windows” tendremos que abrir el menú de “Red e Internet”. Dentro de ese menú podemos ver el estado de la red, del acceso telefónico, de la VPN, el uso de datos o los proxy. Nosotros nos quedaremos en la pantalla inicial y buscaremos la opción “Cambiar opciones del adaptador”.

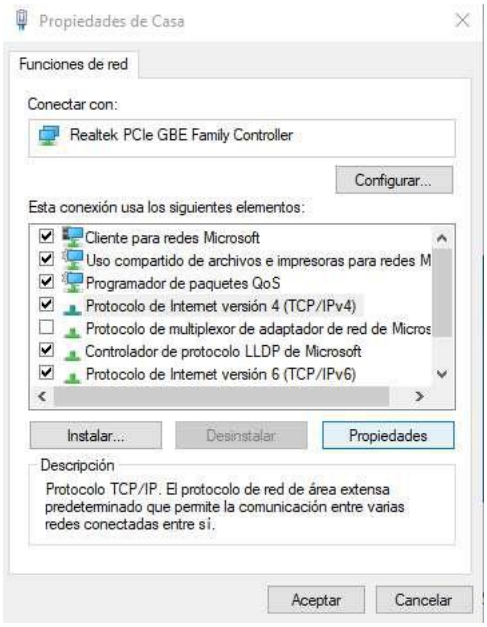



Eso nos abrirá el Panel de Control clásico en su opción de Conexiones de Red ya que esta función todavía no está migrada al nuevo menú de configuración de Windows 10**. Por eso, en Windows 7 y 8.1 podemos llegar a este punto sin tener que hacer todo lo anterior con sólo abrir el Panel de Control.**

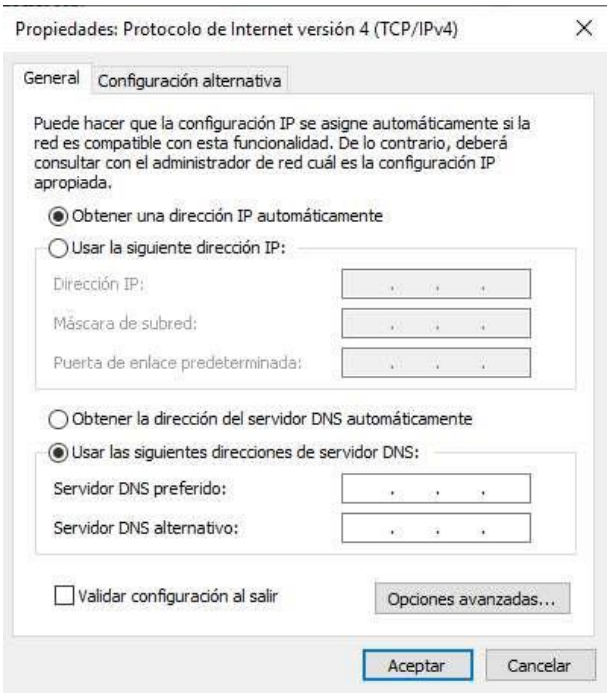

Ahora tendremos que localizar la conexión sobre la que queremos cambiar las DNS. Para asegurarnos, podemos cambiar las DNS en todos los adaptadores.




Pulsaremos con el botón derecho del ratón sobre el adaptador de red y pincharemos en Propiedades. Dentro de la pestaña Funciones de Red buscaremos el elemento Protocolo de Internet versión 4 (TCP/IPv4) que marcaremos y pulsaremos en el botón Propiedades de la parte inferior.




Eso nos abrirá el menú de configuración de la IP en el que tendremos que fijarnos en la parte inferior y marcar “Usar las siguientes direcciones de servidor DNS”. Al activar esa opción, podremos pasar a rellenar “Servidor DNS preferido” y “Servidor DNS Alternativo” dónde introduciremos alguno de los recomendados más arriba.




Marcar la casilla “Validar configuración al salir” y pulsar en Aceptar para que todo quede guardado. Para comprobar que los cambios se han aplicado correctamente, abriremos CMD o símbolo de sistema y escribiremos ipconfig /all.

### *Infección con malware*

Otra de las razones que le restan desempeño a nuestra red es que uno o más dispositivos estén infectados. Los virus y malware suelen utilizar la conexión a la red, por lo que muchas veces son la causa de que esta sea lenta.

Medidas preventivas:

Mantenerse atento. Uno de los medios más populares para propagar malware es el correo electrónico, en el que el malware se puede disfrazar como un mensaje procedente de una empresa conocida, como un banco o un mensaje personal de un amigo. Ten cuidado con los correos electrónicos que te solicitan contraseñas, así como con los correos que parecen provenir de amigos, pero contienen mensajes del tipo "¡Visita este interesante sitio web!" seguido por un enlace. Permanecer atento es la primera capa de protección contra el malware, pero no basta con tener cuidado.

Utilizar un software antivirus actualizado. Les recomiendo utilizar el que viene integrado en Windows, Defender, siempre actualizado. Otras alternativas gratuitas invaden el equipo con procesos que no usamos y consumen recursos que podemos aprovechar para otras tareas.

Periódicamente comprobar la existencia de malware a través de herramientas ejecutables (no instalables) antimalware como por ejemplo ADWCLEANER.

*Sobrecarga de extensiones (deseadas o no) en los navegadores.*

Una extensión de navegador es un complemento que añade ciertas funcionalidades y características. Las extensiones pueden modificar la interfaz del usuario o añadir el servicio de alguna web a tu navegador.

Por ejemplo, algunas extensiones se usan para bloquear anuncios en las páginas web, traducir el texto de un idioma a otro o almacenar contenido de las páginas que visitas en blocs de notas como Evernote o Pocket. Hay miles de aplicaciones para mejorar la productividad, personalizar, comprar o jugar.

Casi todos los navegadores más populares tienen extensiones, como Chrome, Firefox y Edge. Hay muchas extensiones y algunas son muy útiles, por lo que la mayoría acabamos usando unas cuantas. Pero las extensiones pueden ser tan útiles como peligrosas.

Primero, las extensiones pueden ser maliciosas. Esto sucede sobre todo con extensiones que provienen de sitios web de terceros, pero a veces el *malware* se cuela en tiendas oficiales, como es el caso de Android y Google Play.

Por ejemplo, unos investigadores de seguridad descubrieron cuatro extensiones en Chrome Web Store que parecían aplicaciones de notas inofensivas, pero generaban ingresos a sus creadores con anuncios de pago por clic camuflados.

¿Cómo puede hacer eso una extensión? Bueno, para ello, una extensión requiere permisos. Incluso las extensiones más básicas necesitan permisos para leer y modificar los datos de cada página que visitas, lo que les da el poder de hacer lo que quieran con tus datos. Y si no les concedes ese permiso, no se instalan.

Incluso las extensiones que no son maliciosas pueden ser peligrosas, porque la mayoría de las extensiones tienen la posibilidad de recopilar datos sobre los usuarios (recuerda el permiso de leer y modificar los datos de las páginas que visitas). Para ganarse la vida, algunos desarrolladores venden a terceros los datos anónimos que recopilan. Esto suele aparecer en el acuerdo de licencia de usuario final.

El problema es que a veces estos datos no son anónimos, lo que genera serios problemas de privacidad. Las partes que compran los datos pueden identificar a los usuarios.

A pesar de que las extensiones pueden ser peligrosas, algunas de ellas son muy útiles y por eso no querrás abandonarlas por completo. Yo sigo usando una docena y sé que dos de ellas tienen el permiso que ya hemos comentado de leer y modificar.

Puede que sea más seguro no usarlas, pero no es lo mejor, así que necesitamos una forma de usar extensiones más o menos segura.

No instales muchas extensiones. No solo afectan al rendimiento de tu dispositivo, sino que también representan un posible vector de ataque, por lo que reduce su número a unas cuantas que te resulten útiles.

Instala las extensiones únicamente desde tiendas oficiales. Allí las someten a cierto escrutinio, con especialistas en seguridad que filtran las que son maliciosas.

Presta atención a los permisos que requieren las extensiones. Si una extensión que ya esté instalada en tu ordenador solicita un nuevo permiso, es posible que algo vaya mal. Alguien puede haber comprado o secuestrado la extensión. Y antes de instalar cualquier extensión, siempre es buena idea echar un ojo a los permisos que requiere y considerar si están relacionados con la función de la aplicación. Si no encuentras una explicación lógica a los permisos, será mejor que no instales la extensión.