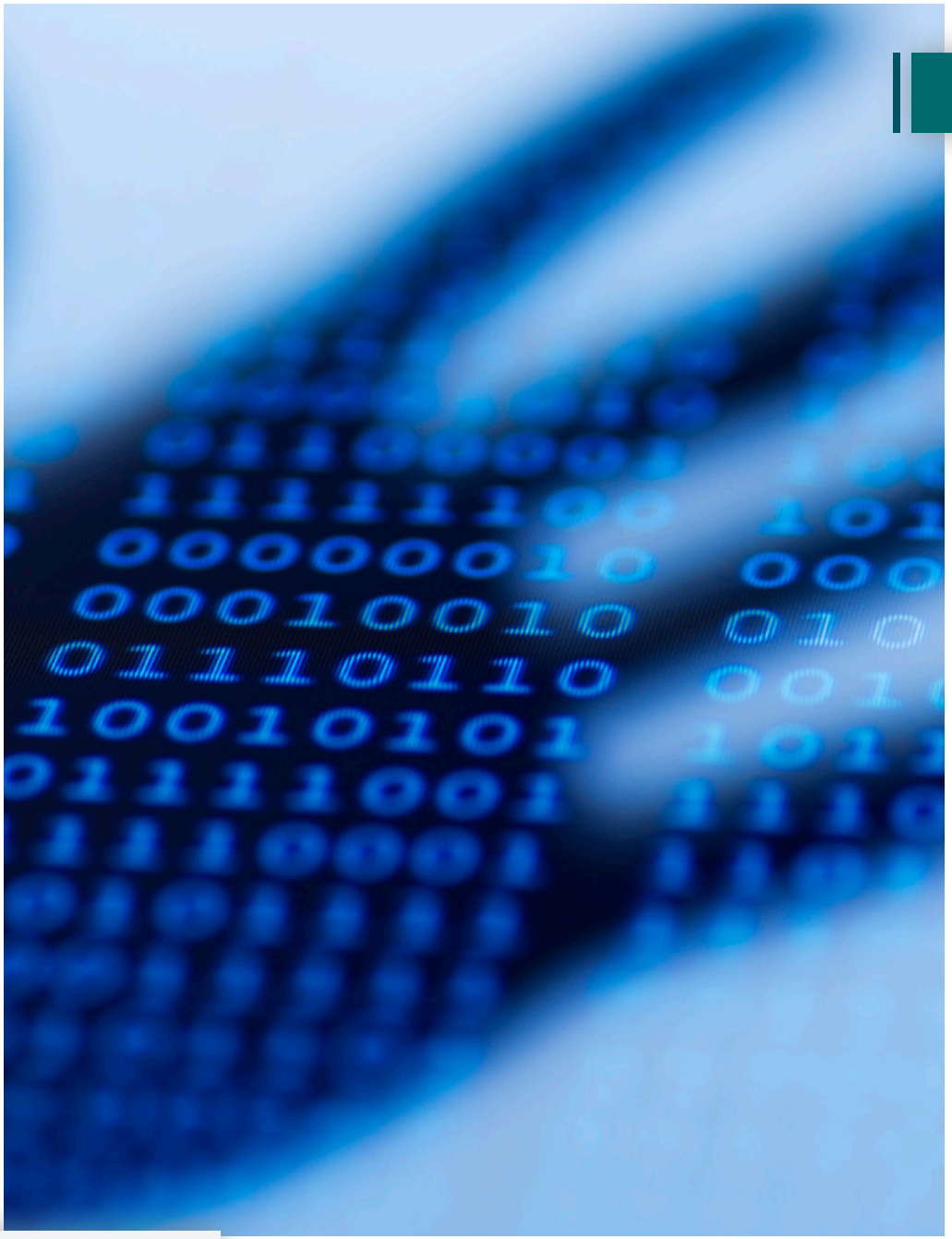
Guía de Seguridad en Redes Inalámbricas



INTRODUCCIÓN

Las conexiones inalámbricas se han popularizado fuertemente los últimos años, tanto en el ámbito hogareño como en el corporativo y en los espacios públicos. La amplia utilización de teléfonos inteligentes (smartphones) y computadoras portátiles ha impulsado la difusión de esta tecnología en diferentes ámbitos. Es muy frecuente que estas sean ofrecidas como un servicio en hoteles, restoranes, cafés y otros lugares públicos; la mayoría de las empresas cuentan con ellas, y en los hogares, estas han reemplazado a las redes cableadas como preferencia de los usuarios.

En todos estos ambientes, cabe la posibilidad que el usuario se conecte a una red Wi-Fi insegura, lo que podría causar problemas de diversa índole como el robo de archivos personales o de contraseñas de acceso a bancos, redes sociales u otros servicios, como también otro tipo de incidentes de seguridad.

¿Cómo armar y configurar de forma segura una red Wi-Fi hogareña? ¿Cómo diferenciar una conexión segura de una que no lo es? ¿Qué medidas se deben adoptar en caso de tener que utilizar inevitablemente una red inalámbrica pública e insegura?

La presente guía le permitirá al usuario comprender los conceptos necesarios para poder navegar de forma más segura tanto en redes inalámbricas públicas como privadas, sea en su hogar como en entornos corporativos.

REDES HOGAREÑAS

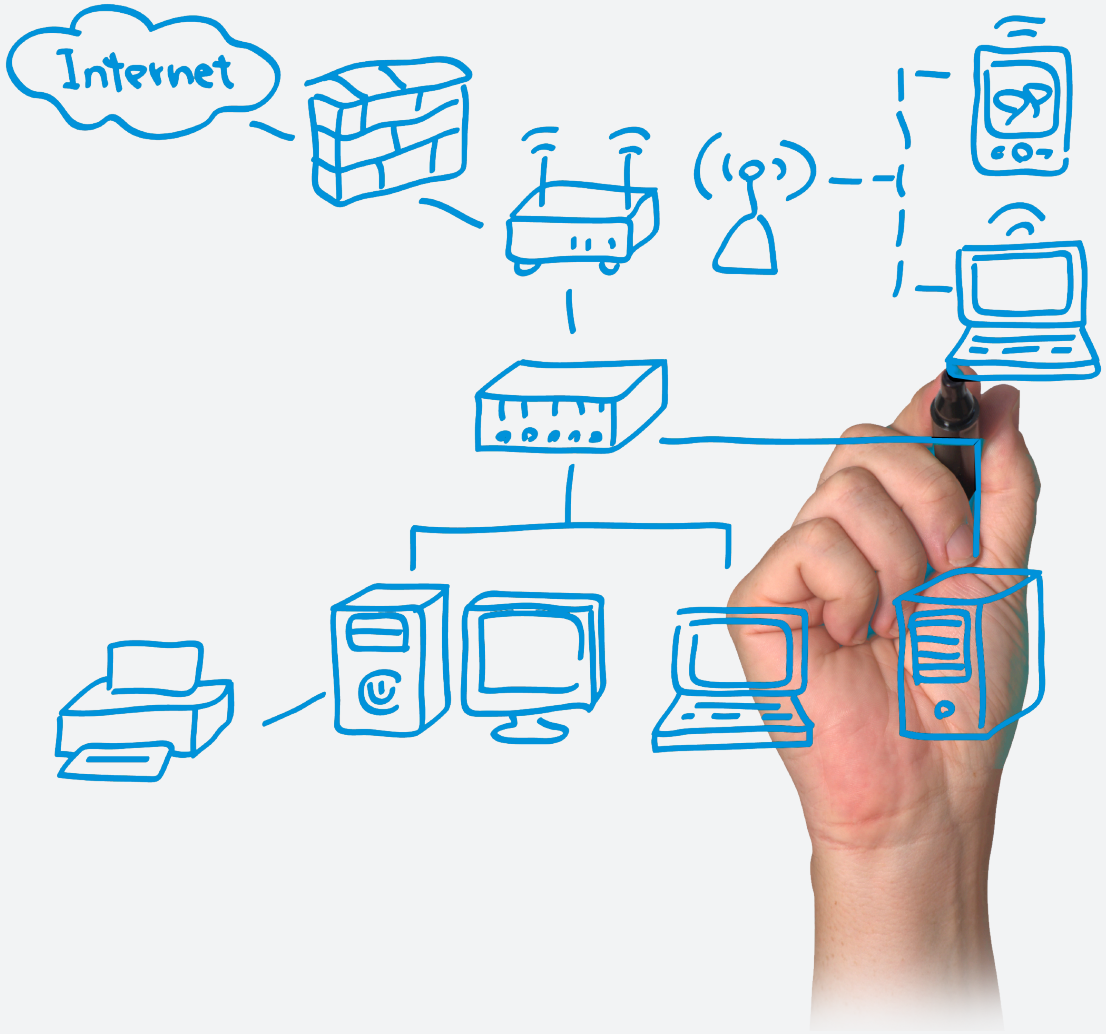
En el hogar, muchos usuarios optan por la vía de instalar un router de forma casera. Es decir, compran el dispositivo, lo conectan a Internet y comienzan a navegar de forma inalámbrica sin fijarse en cómo configurar parámetros relacionados a la seguridad. Esta práctica suele tener como consecuencia que la red no sea segura.

La carencia de configuraciones de seguridad podría permitir que personas no autorizadas por el usuario se conecten a la red y la utilicen de forma tanto benigna (que aún así podría causar problemas como el consumo de ancho de banda o el acceso a información confidencial sin la intención de hacerlo) como de forma maliciosa (originando inconvenientes como el robo de información o el uso de la conexión a Internet del usuario con fines maliciosos).

Una vez que la red se encuentra activa y funcional, es necesario que el usuario tenga en consideración la seguridad de la misma y las amenazas a las que esta puede verse expuesta. Los puntos principales de aseguramiento refieren a la configuración del router y al cifrado utilizado en la red inalámbrica.

ARMADO DE UNA RED INALÁMBRICA

Una vez adquirido un router, el usuario debe conectarlo directamente a Internet por el puerto WAN, es decir, enlazar el router con el cable módem o DSL según el tipo de conexión con la que se cuente. Antes de navegar y conectar dispositivos inalámbricos, es imprescindible configurar los parámetros de seguridad desde una computadora conectada por cable. A continuación se muestra un diagrama de una red inalámbrica tradicional en un hogar, con conexión a Internet, un router Wi-Fi y diversos equipos conectados tanto por cable como de forma inalámbrica:

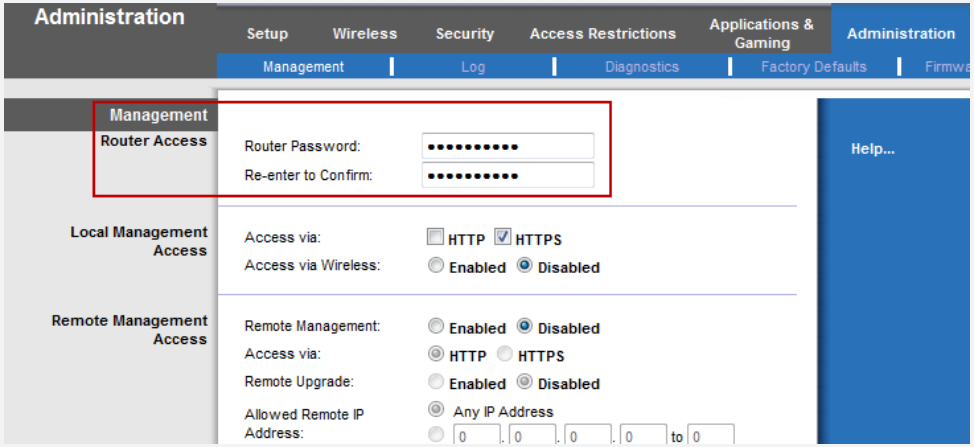


Una vez establecida la red inalámbrica, el usuario debe tener en cuenta la seguridad de la misma, y para ello existen tres configuraciones importantes que se deben realizar al momento en que la red es instalada. Por lo general, es posible ingresar al router a través de un navegador utilizando una dirección del estilo http://192.168.X.X . El manual de configuración suele indicar un nombre de usuario y contraseña por defecto (por ejemplo, admin-admin).

1 MODIFICAR LAS CREDENCIALES DE ACCESO

El primer paso es cambiar la clave de acceso a la configuración del router, ya que una persona ajena podría conocer los datos por defecto y así tener acceso a la configuración de la red. Es recomendable implementar para mayor seguridad una contraseña alfanumérica.

2 ASIGNAR UNA CONTRASEÑA DE ACCESO A LA RED



3 CONFIGURAR EL TIPO DE CIFRADO DE LA RED

Es recomendable utilizar y configurar la red para que utilice cifrado WPA2 con encriptación AES (utilizar WPA o WEP y TKIP sólo en caso de ser necesario ya que son más inseguros). De esta forma, los datos que circulen por la red no serán legibles por parte de terceros que estén monitoreando los mismos.

Con estas tres sencillas configuraciones, el usuario ya habrá modificado radicalmente la seguridad de la red inalámbrica, haciendo mucho menos probable que una persona no autorizada acceda a la red y pueda utilizar la misma con fines maliciosos.

CONFIGURACIÓN DE SEGURIDAD AVANZADA

Más allá del cifrado que se elija y la protección por contraseña, existen otro tipo de medidas de seguridad a tener en cuenta en redes wireless. Las mismas se ven limitadas al modelo de router que el usuario posea en la red hogareña, y son recomendables aplicar cuando se desee un nivel más avanzado de seguridad.

1

CONFIGURAR EL FIREWALL

Si el router lo permite, es posible definir qué servicios y puertos pueden estar disponibles para el acceso externo a la red.

2

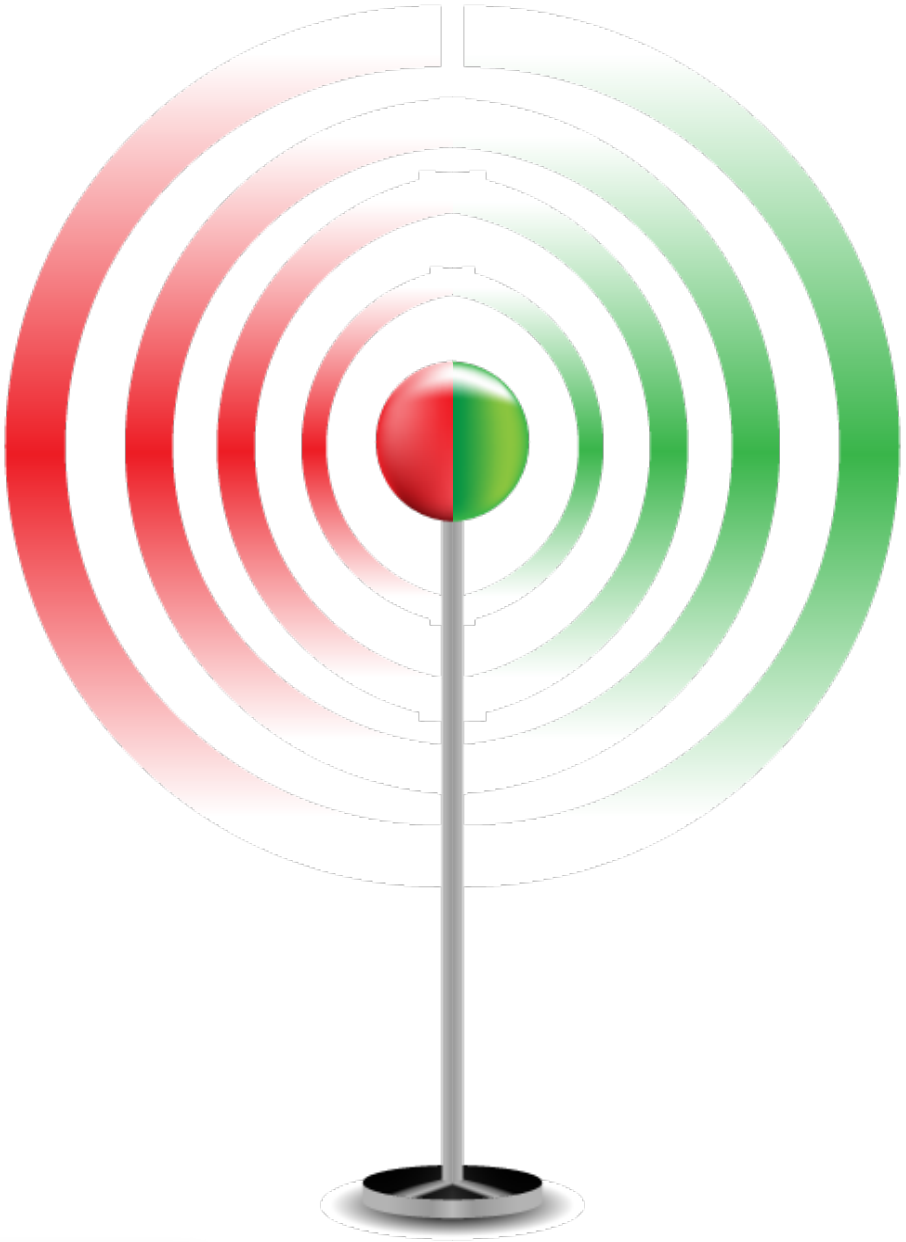
ACCESO AL ROUTER POR HTTPS:

También es posible habilitar la configuración del router a través del protocolo HTTP seguro, para evitar que un atacante capture la contraseña de acceso a la configuración.

3

OCULTAR EL SSID DE LA RED

El SSID (Service Set IDentifier) es el nombre que identifica a la red inalámbrica. El usuario debe cambiar y establecer un SSID. Además, existe la alternativa de "ocultar el SSID", es decir, que el mismo no aparezca cuando otros usuarios aledaños al hogar busquen redes inalámbricas disponibles.



REDES INALÁMBRICAS PRIVADAS

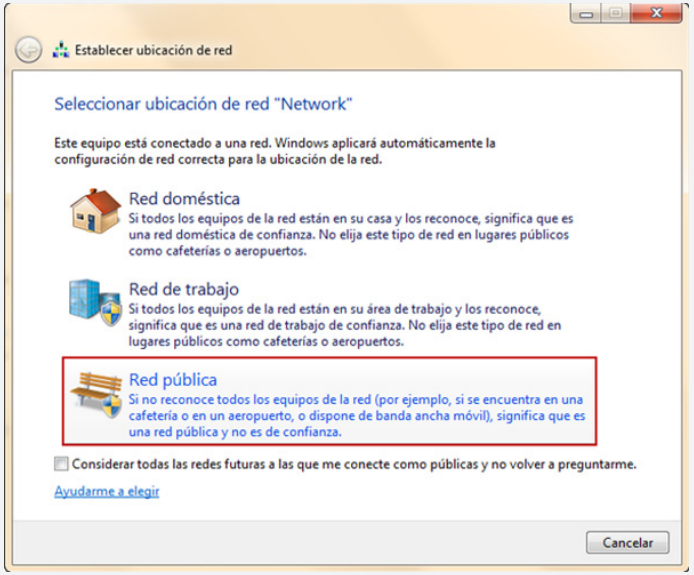
Es frecuente que el usuario también se conecte a redes que no son ni de su propio hogar ni públicas, sino redes de terceros (tanto sea en el trabajo como en lo de un amigo). A pesar de ser privadas, el usuario no conoce a las otras personas conectadas a la misma red, ni sus intenciones. Por lo tanto, se deben tomar los recaudos como si fueran públicas, aún cuando se conozca y se tenga confianza sobre el administrador de la misma.

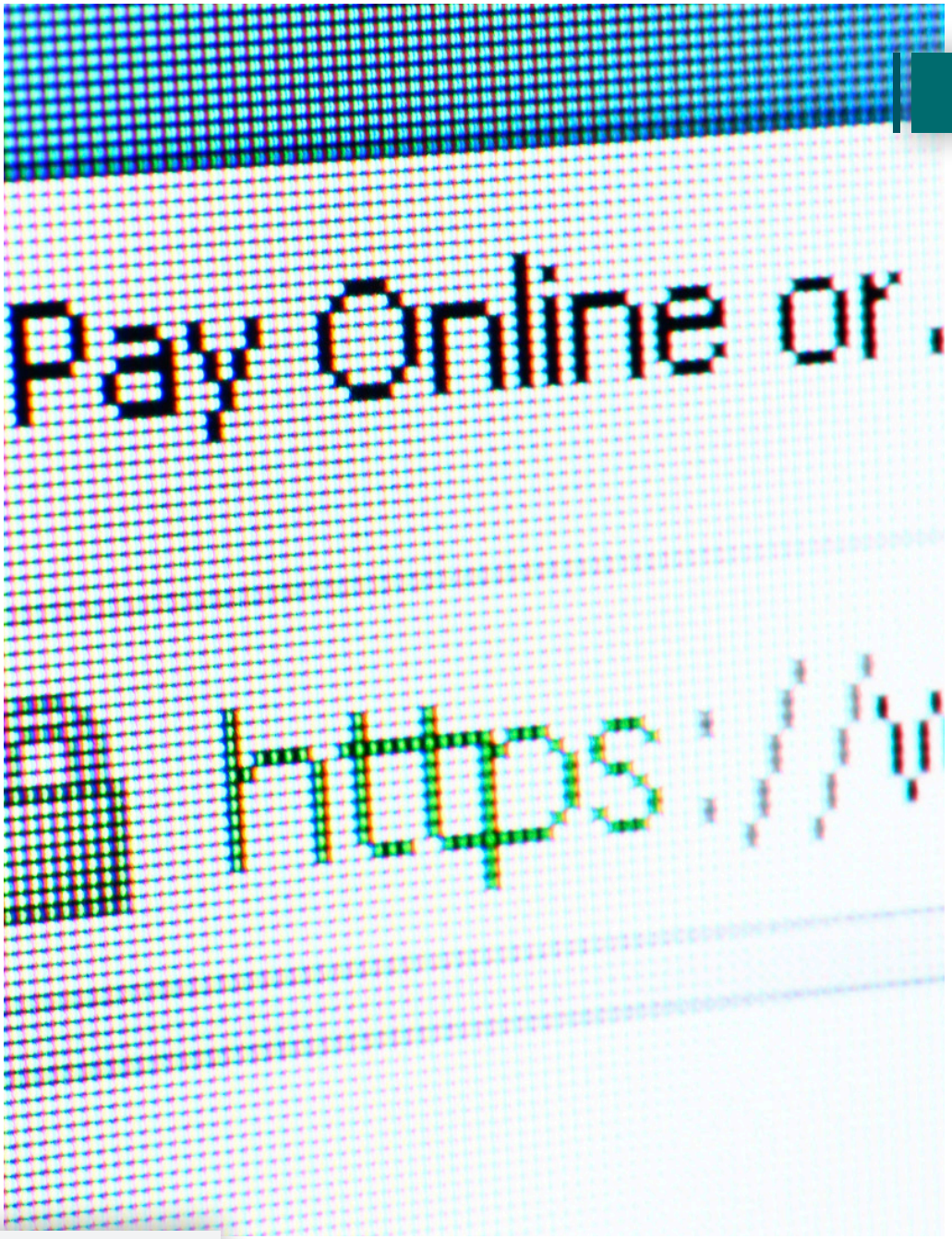
¿Cómo identificar una red inalámbrica segura?

Es importante que cada vez que se conecte a Internet inalámbricamente, verifique si la conexión a la cual está intentando acceder, cuenta con algún tipo de protección. Lo primero es fijarse si la misma está protegida por una contraseña, y posteriormente el tipo de cifrado que utiliza. Una conexión WEP es bastante más insegura que una WPA o WPA2 (la más segura). Es decir, una persona con los conocimientos suficientes, podría leer los datos que circulen por una red WEP o WPA.

REDES WI-FI PÚBLICAS

Cada vez que el usuario se conecta a una red inalámbrica Wi-Fi, Windows o algunos firewall preguntan si se trata de una red hogareña, corporativa o pública. Es importante como primera medida seleccionar siempre "red pública", para que se adopten configuraciones más restrictivas de seguridad, especialmente en lo que respecta a archivos compartidos y acceso al sistema. Si no se tienen en cuenta los controles de seguridad pertinentes, es recomendable evitar el uso de servicios que requieran de información sensible en conexiones inalámbricas compartidas o públicas. En las siguientes páginas se mencionan algunos conceptos y consejos que pueden adoptarse para hacer un uso más seguro de redes Wi-Fi públicas.





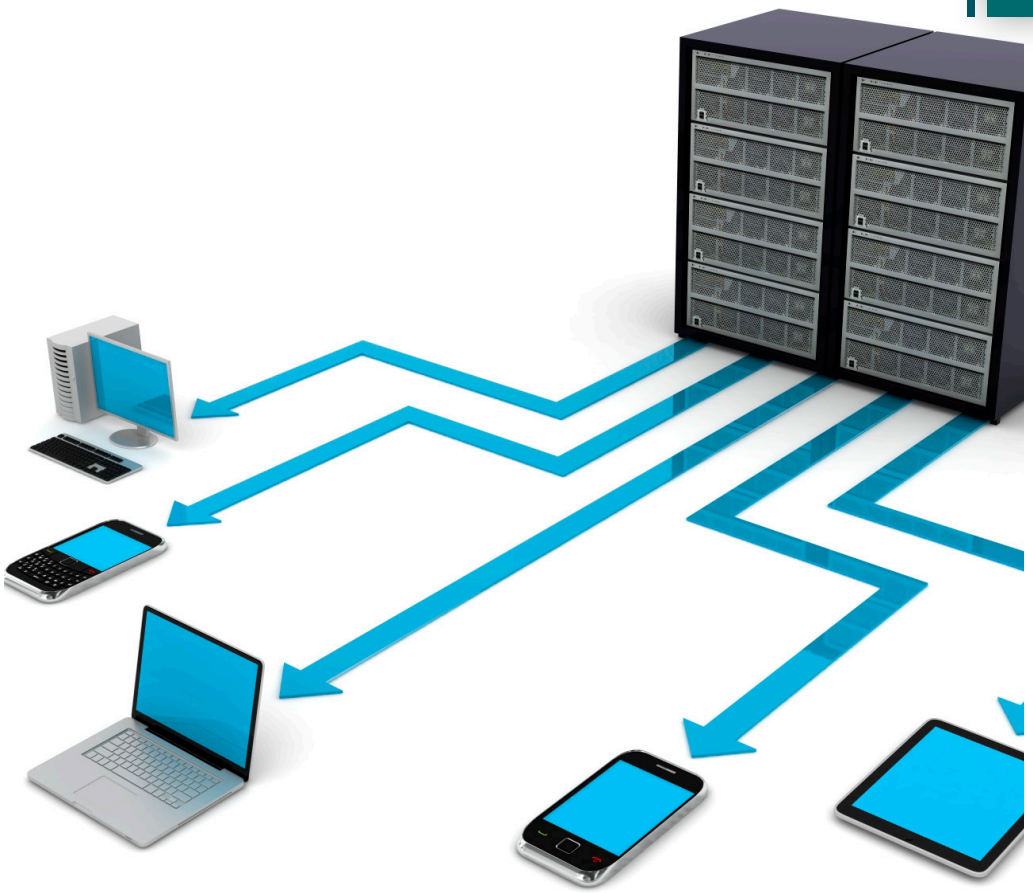
HTTPS

HTTPS (del inglés, Hypertext Transfer Protocol Secure) es un protocolo de transferencia de datos seguros. Es decir, todo lo que se transmite a través del mismo va cifrado para que un tercero no pueda leer la información enviada. Varios servicios web que requieren de contraseñas como bancos, correos electrónicos, redes sociales y demás, emplean este protocolo de seguridad. Si es imprescindible utilizar algún servicio de este tipo en una red wireless insegura, cerciórese que el sitio que está visitando empiece por "https://" y de tener activada esa opción en los servicios como puede ser Facebook, Twitter o similares.

Extensiones para activar HTTPS automáticamente

En algunos casos, el protocolo HTTPS es utilizado solo si el usuario configura su cuenta de correo, red social u otra de forma manual. Sin embargo, existen extensiones como "HTTPS Everywhere" para Mozilla Firefox y Google Chrome que permiten activar dicha funcionalidad automáticamente.

Para más información: https://www.eff.org/https-everywhere



VPN

Una red privada virtual (en inglés, Virtual Private Network) permite extender el acceso desde una red pública hacia una red local conocida y de confianza para el usuario. Las redes VPN utilizan comunicaciones cifradas, es decir que los datos transmitidos a través de la red no pueden ser interceptados e interpretados por un atacante, ya que son ilegibles hasta que llegan a destino.

Estas redes pueden ser configuradas para que todo el tráfico generado por el usuario sea transmitido por la VPN. De este modo, todo el acceso Internet es transmitido por la VPN y se dificulta la posibilidad que un tercero intercepte la información transmitida a través de una red Wi-Fi pública e insegura.

Es frecuente que usuario con dispositivos corporativos cuenten con una red VPN configurada. De estar disponible, se recomienda utilizarla siempre. Asimismo, muchos routers hogareños permiten configurar este servicio, por lo que usuarios que deseen una seguridad más avanzada pueden leer el manual o instructivo para configurarlo.

ACCESO DESDE DISPOSITIVOS MÓVILES

Desde el punto de vista de la seguridad en redes inalámbricas, es amplia la diferencia entre aquellas redes que cifran los datos y aquellas que no. Cuando se accede desde dispositivos móviles a redes públicas e inseguras (entendiendo a estas como redes donde la información no es transmitida cifrada o no poseen contraseña de acceso), es muy frecuente que el usuario utilice diversas aplicaciones que no siempre utilizan comunicaciones cifradas (como HTTPS), por lo que un tercero podría estar "leyendo" las comunicaciones.

Así como desde un equipo de escritorio es posible configurar muchos servicios para que utilicen un protocolo cifrado, muchas aplicaciones móviles no permiten esta configuración por lo que el usuario queda a merced de lo establecido por el fabricante del software. Han existido diversos casos donde se comprueba que populares aplicaciones para smartphones no transmiten la información de forma segura.

Por lo tanto, el usuario debe comprobar que las aplicaciones móviles que transmitan información, tales como los programas de mensajería instantánea, encripten los datos que envían. En caso que un software no implemente este tipo de protección, se debe evitar utilizarlo en redes Wi-Fi públicas y sí hacerlo a través de una red VPN o conexiones móviles como EDGE o 3G, disminuyendo así la posibilidad que un atacante intercepte fácilmente información transmitida en texto plano.

CONCLUSIÓN

La tecnología inalámbrica (Wi-Fi) sin dudas facilita la vida cotidiana de las personas. Gracias a esta, los usuarios ya no dependen de un cable para poder utilizar servicios en Internet. No obstante, esta tecnología también permite a terceros interceptar la información que el usuario transmite de forma más sencilla que en redes cableadas. Esto es más complejo si se tiene en cuenta que existe una extensa cantidad de redes Wi-Fi públicas e inseguras.

A pesar de la problemática planteada, también se ha expuesto a lo largo de la guía que, como otros aspectos de la seguridad informática, la utilización de tecnologías de seguridad, la correcta configuración de los servicios y las buenas prácticas de la conducta del usuario, pueden permitir de forma relativamente sencilla minimizar la probabilidad de sufrir un incidente sobre la información.

En el hogar, es necesario seguir los consejos básicos para configurar una red Wi-Fi segura. En el caso de las redes privadas, es importante considerarlas como si fueran públicas ya que se desconoce qué otras personas están conectadas a la misma y cuáles son sus intenciones. Finalmente, las redes inalámbricas públicas son hoy en día tan populares como peligrosas en muchos casos, por ende el usuario debe implementar los consejos y controles expuestos anteriormente para proteger su información.

Sea por cable o por el aire, la información del usuarios puede estar expuesta; y es siempre necesario considerar la mejor forma de protegerla.