¿Cuál Es El Mejor Cifrado De Seguridad Para Una Red Wi-Fi?

La protección de los datos en una red inalámbrica es algo que no se debe pasar en alto. Existen diferentes métodos para que cualquier persona ajena a la red inalámbrica pueda ***sniffear u obtener los datos que se estén enviado y recibiendo***, si no sabias esto, te aconsejamos leer nuestro anterior articulo, donde hablamos sobre como un atacante puede romper la seguridad de una red inalámbrica. Escoger el mejor cifrado de seguridad para una red inalámbrica, puede ser una tarea que requiera de un buen análisis.

En este articulo trataremos de guiarte, y así puedas decidir cuál es el ***mejor cifrado para una red Wi-Fi***.

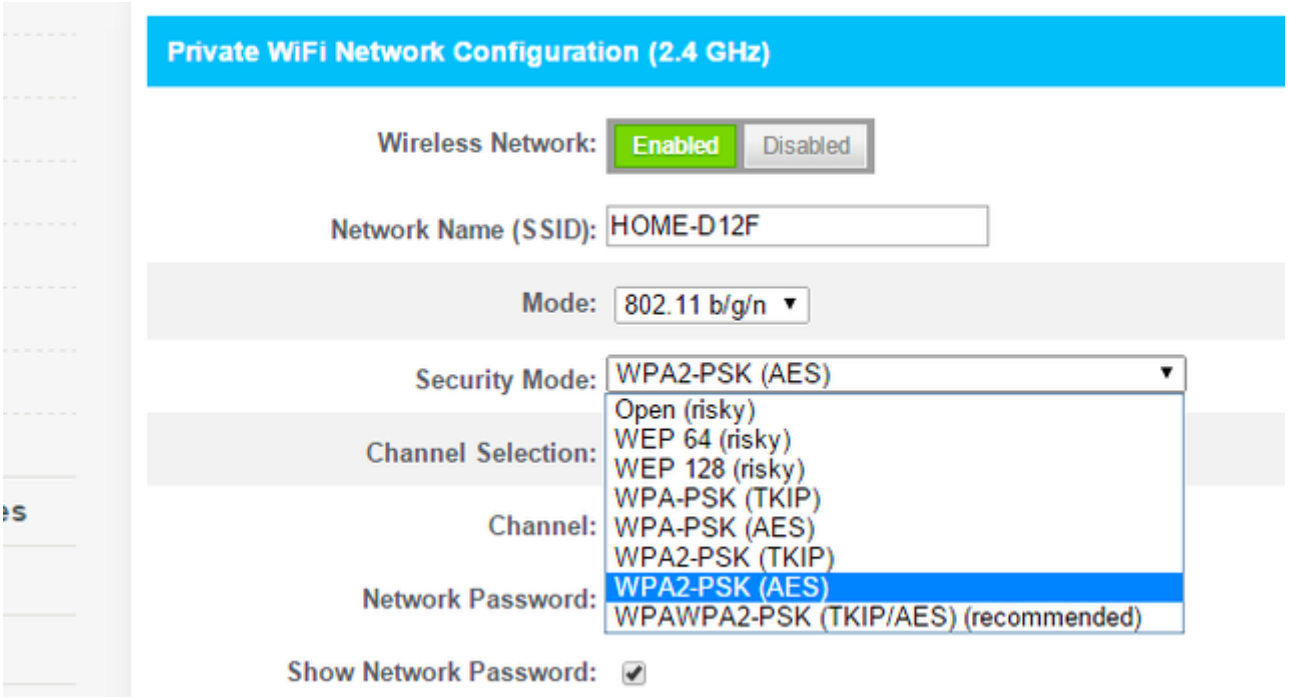
AES vs. TKIP

El cifrado TKIP y AES son dos tipos diferentes de cifrado que pueden ser utilizados por una red Wi-Fi. TKIP significa «Protocolo de integridad de clave temporal.» Fue un protocolo de encriptación provisional introducida con WPA para **reemplazar el cifrado WEP,** como sabrán, este cifrado es bastante débil y es vulnerado con facilidad. TKIP es en realidad muy similar a la encriptación WEP. Este cifrado ya no se considera seguro, y ahora está en desuso. En otras palabras, no debes seguir usándolo ;)

AES es sinónimo de «Advanced Encryption Standard.» Este fue un **protocolo de cifrado más seguro introducida con WPA2**, que sustituyó al estándar WPA provisional. **AES** es un fuerte

estándar de cifrado usado en todo el mundo, incluso ha sido adoptado por el gobierno de Estados Unidos. Por ejemplo, al cifrar un disco duro con TrueCrypt, se puede utilizar el cifrado AES para eso. AES se considera generalmente bastante seguro, y las principales debilidades sería ataques de fuerza bruta (evitadas por el uso de una contraseña fuerte) y las debilidades de seguridad en otros aspectos de WPA2.

El «PSK» en ambos nombres significa «clave previamente compartida», la clave previamente compartida es generalmente su frase de cifrado. Esto lo distingue de WPA-Enterprise, que utiliza un servidor RADIUS para entregar claves únicas en las redes corporativas o gubernamentales.



WPA Usa TKIP y WPA2 Usa AES, Pero …

En resumen, TKIP es un estándar de cifrado más antiguo utilizado por el antiguo estándar WPA. AES es una solución de cifrado más reciente para la seguridad de una red Wi-Fi utilizado por la nueva y segura estándar WPA2. En teoría, ese

es el final de la misma.

Si bien se supone que WPA2 usa AES para una seguridad óptima, también tiene la opción de utilizar TKIP para la compatibilidad con dispositivos asociados. En tal estado, los dispositivos compatibles con WPA2 se conectarán con WPA2 y dispositivos compatibles con WPA se conectará con WPA. Así que «WPA2» no siempre significa WPA2-AES. Sin embargo, en los dispositivos sin un «TKIP» visible o la opción «AES», WPA2 es generalmente sinónimo de WPA2-AES.

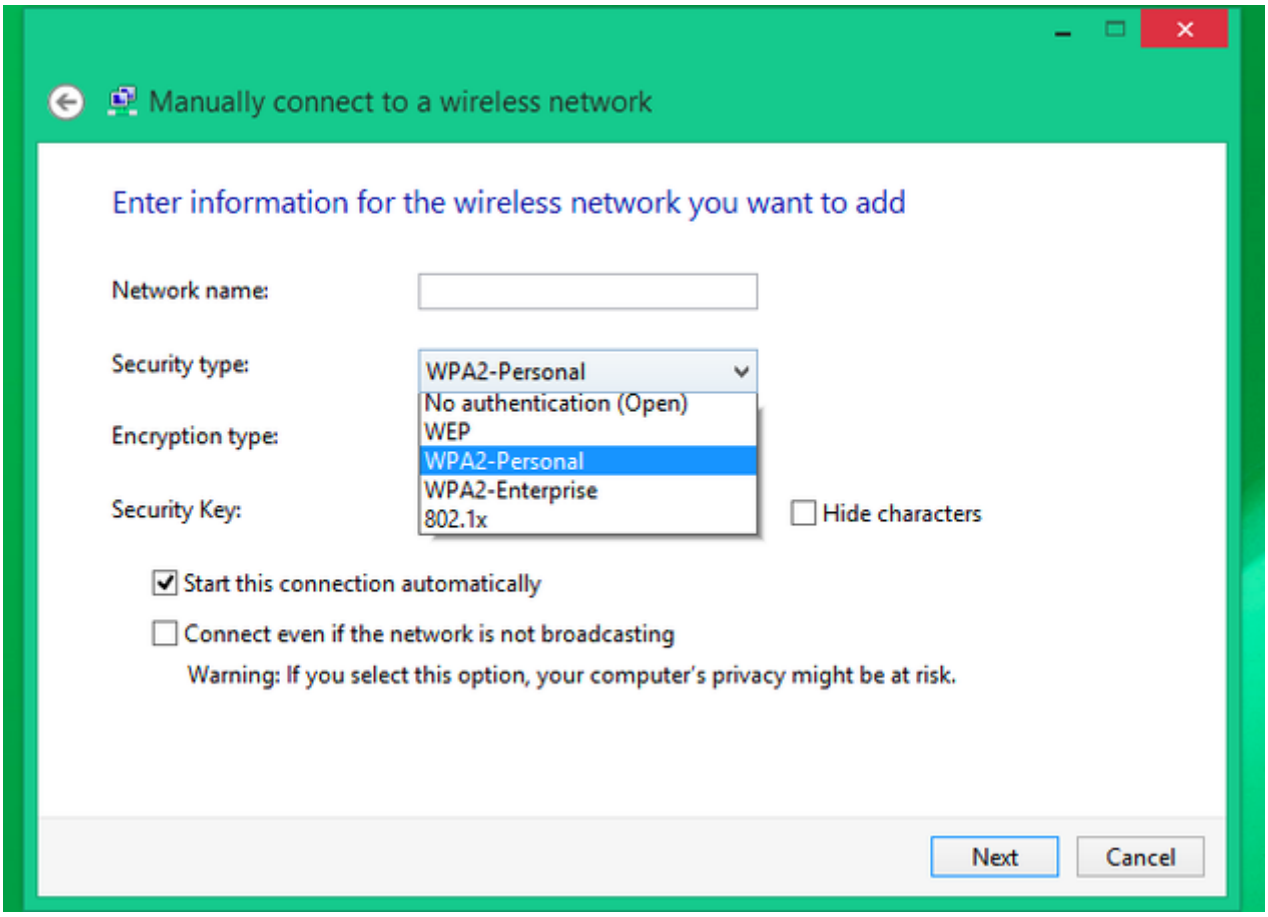
Explicación modos de seguridad de una red Wi-Fi

Confundido todavía? No es raro. A continuación te mostramos algunos métodos de cifrado mas comunes que se encuentran en un router inalámbrico.:

- Abiertas (riesgo): Las redes abiertas Wi-Fi no tienen contraseña.
- WEP de 64 (riesgoso): El viejo estándar de encriptación WEP es vulnerable y no se debe utilizar.
- WEP 128 (riesgoso): WEP con un cifrado de clave de mayor tamaño, no significa que es mucho mejor.
- WPA-PSK (TKIP): Este es básicamente el estándar de cifrado WPA o WPA1. Se ha superado y no es seguro.
- WPA-PSK (AES): Esto selecciona el protocolo de cifrado inalámbrico WPA con el cifrado AES. Los dispositivos que soportan AES casi siempre soportarán WPA2, mientras que los dispositivos que requieren WPA1 casi nunca podrán usar el cifrado AES.
- WPA2-PSK (TKIP): Utiliza el estándar WPA2 con cifrado TKIP más moderno. Esto no es seguro, y es sólo una buena

idea si tienes los dispositivos más antiguos que no pueden conectarse a una red WPA2-PSK (AES).

- WPA2-PSK (AES): Esta es la ***opción más segura***. Utiliza WPA2, el último estándar de encriptación Wi-Fi, y el más reciente protocolo de encriptación AES.
- WPAWPA2-PSK (TKIP / AES) (recomendado): Esto cifrado permite tanto WPA y WPA2 con TKIP y AES. Esto proporciona la máxima compatibilidad con todos los dispositivos antiguos que pueda tener, sino que también garantiza que un atacante no pueda acceder a la red tan fácilmente.



WPA y TKIP desmejora la

velocidad de conexión

Las opciones de cifrado WPA y TKIP pueden también afectar la calidad en el envío y recepción de datos. Muchos routers modernos que soportan Wi-Fi 802.11n y nuevos estándares, desmejorara a 54mbps si habilita WPA o TKIP en sus opciones. Lo hacen para asegurarse de que son compatibles con estos dispositivos más antiguos.

En la mayoría de los routers que hemos visto, las opciones son generalmente WEP, WPA (TKIP) y WPA2 (AES) – tal vez con un WPA (TKIP) + WPA2 (AES), el modo de compatibilidad en una buena medida. Si tienes una extraña clase de router que ofrece las opciones de WPA2 en TKIP o AES, no dudes en elegir la opción AES. Casi todos los dispositivos sin duda trabajan con él, y es más rápido y más seguro. Es una elección fácil, siempre y cuando puedas recordar y tener en cuenta que **AES es la mejor opción**.