Evite estos errores al configurar una red WiFi

Muchos usuarios pasan por alto ciertos aspectos cruciales al momento de configurar su red WiFi en el hogar o en la oficina, que abre la puerta a ciberataques, e intrusos que pueden robar toda su información confidencial como contraseñas para acceder a correos electrónicos o cuentas bancarias.

Otros riesgos a que se pueden enfrentar cuando no se toman medidas es que el internet no funcione rápido, al estar sobrecargado de dispositivos electrónicos como celulares o computadoras.

Estos problemas, son fácilmente evitables si se toman las precauciones adecuadas. Así que se detallan los más frecuentes al configurar una red WiFi y las medidas que se deben tomar para garantizar la seguridad y el rendimiento óptimo de la red.

Cuál es el error más frecuente que existe al configurar una red WiFi

Uno de los errores más básicos que muchos cometen es no cambiar la contraseña predeterminada del router. La mayoría de los dispositivos vienen con contraseñas de fábrica que son bien conocidas por hackers o que pueden encontrarse fácilmente en internet. Dejar estas contraseñas facilita el acceso de intrusos a la red.

Para evitar esto, se recomienda crear una contraseña única y robusta, que combine letras mayúsculas y minúsculas, números y símbolos.

Es crucial no usar información personal obvia, como fechas de nacimiento o nombres de familiares, porque estos datos pueden ser adivinados o fácilmente obtenidos mediante ingeniería social.

Cómo cambiar el nombre de la red WiFi

El SSID, o nombre de la red WiFi, también puede ser una pista para los atacantes. Muchos routers vienen con nombres de red que identifican el fabricante o el modelo del dispositivo, lo que puede ayudar a los cibercriminales a identificar vulnerabilidades conocidas de ese modelo en particular.

Cambiar el SSID a algo más genérico, que no revele información sobre el tipo de router o el propietario de la red, es una forma sencilla de aumentar la seguridad.

Además, es recomendable evitar nombres que atraigan la atención, como “Red rápida” o “WiFi gratis”, porque esto puede invitar a usuarios no deseados a intentar conectarse.

Qué es el cifrado de la red WiFi

Uno de los mayores errores que se cometen es no activar el cifrado de la red WiFi. Este garantiza que los datos que se transmiten entre el dispositivo y el router, no puedan ser interceptados fácilmente por terceros.

El estándar de cifrado más recomendado actualmente es WPA3, que ofrece una mayor seguridad que sus predecesores WPA y WEP. Si el router no es compatible con WPA3, al menos se debe configurar el cifrado WPA2, evitando el uso de WEP, que es extremadamente vulnerable y fácil de hackear.

Cómo configurar una red WiFi de invitados

Permitir que amigos, familiares o incluso vecinos se conecten a la red principal de WiFi puede ser una invitación a problemas. No solo pueden ralentizar el internet al consumir ancho de banda, sino que también, sin saberlo, pueden introducir malware o virus en la red si sus dispositivos están comprometidos.

Una solución sencilla es configurar una red de invitados. Muchos routers permiten crear una red separada para visitantes, lo que limita el acceso a los recursos internos de la red principal. De esta manera, los invitados pueden usar internet sin poner en riesgo la seguridad de los datos personales.

Cuántos dispositivos están conectados a la red WiFi

Varios usuarios instalan su router y se olvidan de monitorear quién o qué dispositivos están conectados. Esto es un error, porque permite que dispositivos no autorizados se conecten y consuman el ancho de banda, o peor aún, que se utilicen para espiar la actividad en la red.

Se recomienda revisar periódicamente la lista de dispositivos conectados al router para identificar cualquier conexión sospechosa. Algunos routers también permiten establecer alertas cuando un nuevo dispositivo se conecta a la red.

Con información de Infobae