Cómo ocultar el WiFi de tu router al vecino

La comodidad de tener una red WiFi en casa puede convertirse en una pesadilla si no se toman medidas de seguridad. Los ciberdelincuentes y usuarios no autorizados pueden aprovechar vulnerabilidades en tu red para robar datos personales, ralentizar tu conexión e incluso controlar tus dispositivos.

Ocultar el SSID dificulta que personas no autorizadas encuentren tu Wifi. Esto es importante si vives en un edificio con varios vecinos, porque reduce el riesgo de que alguien se conecte a tu red.

Guía paso a paso para ocultar la red WiFi de tu casa

Para ocultar el SSID de la red WiFi, se debe acceder a la configuración del router. Cada fabricante tiene una interfaz ligeramente diferente, pero los pasos básicos son similares. A continuación, se describen las etapas generales:

– Ingresar la dirección IP del router en el navegador web. Esta suele ser algo como 192.168.1.1 o 192.168.0.1. Si no se está seguro de cuál es la dirección puedes encontrarla en la documentación del dispositivo o buscando en internet el modelo.

– Hay que introducir el nombre de usuario y la contraseña para acceder a la configuración del router. Si nunca se ha cambiado estas credenciales, es probable que sigan siendo las predeterminadas, como “admin” y “password”.

– Una vez dentro del panel de administración, buscar la sección dedicada a las configuraciones de la red WiFi. Dependiendo del fabricante, esta podría llamarse “Inalámbrico”, “Wireless”, “Configuración WiFi” o similar.

– En la configuración Wi-Fi, se encuentra una opción que dice algo como “Broadcast SSID” o “Transmitir SSID”. Desactivar esta casilla. Al hacerlo, el nombre de la red ya no aparecerá en la lista de redes disponibles para los dispositivos cercanos.

Es recomendable tomar otras medidas para proteger la red WiFi. La Agencia Española de Protección de Datos (AEPD) sugiere las siguientes acciones adicionales para garantizar la seguridad de las redes domésticas:

Qué otras medidas de seguridad se deben implementar

Cambiar las credenciales predeterminadas: Uno de los mayores riesgos de seguridad proviene de dejar el nombre de usuario y la contraseña predeterminados del router sin cambiar.

Usar cifrado WPA3: Si el router no es compatible, al menos corroborar de estar usando WPA2, que sigue siendo más seguro que las opciones anteriores como WEP, las cuales son obsoletas y vulnerables a ataques.

Establecer una contraseña robusta para la red WiFi: Una combinación de letras mayúsculas, minúsculas, números y símbolos es lo ideal. Evita usar palabras o números fácilmente adivinables, como “contraseña123″.

Configurar una red para invitados: Si se reciben visitas frecuentemente y les proporcionan acceso a la red WiFi, considera habilitar una red de invitados.

Con información de Infobae