



USO SEGURO DE REDES INALÁMBRICAS

Guía de Configuración y Buenas Prácticas para Redes Domésticas y de Uso Público

1. INTRODUCCIÓN

Las redes inalámbricas (Wi-Fi) brindan una enorme flexibilidad permitiendo que múltiples dispositivos como computadoras portátiles, teléfonos móviles, televisores inteligentes y tabletas se conecten de manera simultánea compartiendo un Identificador de Conjunto de Servicios (SSID). No obstante, al propagar la información por el aire, estas redes exigen medidas estrictas de cifrado y seguridad para evitar que intrusos no autorizados vulneren su privacidad y consuman su ancho de banda.

MEGANET TELECOMUNICACIONES S.A.S., comprometida con la seguridad digital de sus usuarios, expide esta guía técnica para asegurar la conectividad inalámbrica dentro y fuera del hogar.

2. ASEGURANDO LA RED WI-FI DEL HOGAR

Para resguardar su enrutador (router) doméstico frente a posibles ciberatacantes, siga estas directrices básicas:

- **Cambiar Credenciales Predeterminadas:** Los atacantes conocen perfectamente los SSIDs (nombres de red) y las contraseñas de administración de fábrica de los enrutadores. Acceda a la interfaz web de administración del enrutador y cambie de inmediato la clave de acceso de administrador y el SSID.
- **Habilitar Cifrado Fuerte (WPA2 / WPA3):** Cifre siempre la transmisión de datos inalámbricos. Se recomienda configurar la red utilizando el protocolo de cifrado WPA2-Personal o, idealmente, WPA3, protegiéndola con una contraseña de red robusta. Evite configuraciones obsoletas o inseguras como WEP o WPA básico.
- **Ocultar la Transmisión del SSID (Opcional):** Puede configurar el enrutador para que no transmita públicamente su nombre de red (SSID oculto). Esto requiere introducir manualmente el nombre exacto de la red en los dispositivos que desee conectar. Tenga en cuenta que esto oculta la red a los usuarios comunes, pero no detiene a atacantes experimentados equipados con analizadores de paquetes de red.



3. NAVEGANDO SEGURO EN REDES WI-FI PÚBLICAS

Cuando se encuentra fuera del hogar, los puntos de acceso públicos (centros comerciales, restaurantes, aeropuertos) son de enorme utilidad, pero representan un alto riesgo cibernético. En estas redes abiertas, el tráfico de datos puede ser interceptado por atacantes mediante una técnica denominada "eavesdropping" (escucha pasiva).

Para protegerse en entornos de red públicos, aplique las siguientes medidas:

- **Evite Información Sensible:** Nunca ingrese contraseñas, realice compras en línea o acceda a portales bancarios mientras esté conectado a una red Wi-Fi pública.
- **Deshabilite la Compartición de Archivos:** Configure sus dispositivos para que no compartan archivos ni carpetas en la red local y deshabilite la visibilidad pública en redes catalogadas como "Públicas" en Windows o macOS.
- **Utilice una Red Privada Virtual (VPN):** Una VPN cifra de extremo a extremo todo el tráfico de datos transmitido desde su dispositivo hacia internet a través de un túnel digital seguro. Aunque un atacante logre interceptar los paquetes de datos en la red Wi-Fi pública, el cifrado militar de la VPN impedirá totalmente su lectura o descifrado.

4. SEGURIDAD EN CONEXIONES BLUETOOTH

La tecnología Bluetooth permite enlazar auriculares, parlantes y compartir archivos de corto alcance. Sin embargo, los hackers pueden aprovechar vulnerabilidades de Bluetooth activas para espiar conversaciones, instalar malware, exfiltrar listas de contactos o consumir aceleradamente la batería del dispositivo.

Recomendaciones para Bluetooth:

1. Mantenga apagada la funcionalidad Bluetooth de sus celulares y tabletas cuando no los esté utilizando activamente.
2. No configure su Bluetooth en modo "Visible para todos" permanentemente; use el modo oculto o visible únicamente para dispositivos previamente vinculados.
3. Rechace cualquier solicitud de emparejamiento o transferencia de archivos de remitentes desconocidos.

Pauta del Proveedor MEGANET TELECOMUNICACIONES S.A.S.:

Nuestros técnicos instalan y configuran el CPE (enrutador del hogar) con políticas de cifrado robustas y

contraseñas seguras por defecto. Si requiere modificar el nombre de su red (SSID) o la clave Wi-Fi, contáctenos en nuestros canales oficiales para recibir soporte técnico especializado.