USO DE REDES INALÁMBRICAS EN FORMA SEGURA EN INGENIERIA Y REDES DEL CARIBE S.A.S

Las redes inalámbricas permiten que los dispositivos habilitados con Wi-Fi, como computadoras portátiles y tablets, se conecten a la red por medio de un identificador de red conocido como identificador de conjunto de servicios (SSID).

Para evitar que los intrusos ingresen en su red inalámbrica doméstica, el SSID predeterminado y la contraseña predeterminada para la interfaz de administración en el navegador web deben cambiarse. Los hackers son conscientes de este tipo de información de acceso predeterminada. Además, debe encriptar la comunicación inalámbrica habilitando la seguridad inalámbrica y la función de cifrado WPA2 en el router inalámbrico. De manera opcional, el router inalámbrico también puede configurarse para que no transmita el SSID, lo que agrega una barrera adicional a la detección de la red; no obstante, esto no debe considerarse adecuadamente seguro para la red inalámbrica.

Cuando está lejos de casa, los puntos públicos de acceso inalámbrico permiten tener acceso a su información en línea y navegar por Internet. Sin embargo, es mejor no acceder ni enviar información personal confidencial a través de una red pública inalámbrica.

Verifique si su computadora está configurada para compartir archivos y medios digitales y si requiere la autenticación de usuario con cifrado. Para evitar que una persona intercepte su información (lo que se conoce como “evesdropping”) mientras utiliza una red pública inalámbrica, utilice túneles VPN y servicios cifrados. El servicio VPN proporciona acceso seguro a Internet con una conexión cifrada entre la computadora y el servidor VPN del proveedor de servicios VPN. Con un túnel VPN cifrado, aunque se intercepte una transmisión de datos, no podrá descifrarse.

Muchos dispositivos móviles, como smartphones y tablets, incluyen el protocolo inalámbrico Bluetooth. Esta funcionalidad permite que los dispositivos con Bluetooth habilitados se conecten entre sí y compartan información. Desafortunadamente, Bluetooth puede ser atacado por hackers a fin de espiar algunos dispositivos, establecer controles del acceso remoto, distribuir malware y consumir baterías. Para evitar estos problemas, mantenga Bluetooth desactivado cuando no lo utiliza.