MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

SEGURIDAD EN CONEXIONES INALÁMBRICAS: 5 CONSEJOS DE CIBERSEGURIDAD

Evita realizar transferencias, compras o trámites financieros conectado a redes Wi-Fi abiertas y gratuitas

Las redes Wi-Fi públicas pueden ser inseguras y propensas a ataques cibernéticos. Evita realizar transacciones financieras sensibles o proporcionar información confidencial cuando estés conectado a estas redes.

Evita acceder a redes sociales, aplicaciones web de la organización o cualquier sitio que requiera iniciar sesión conectado a una red pública

Las redes sociales y las aplicaciones web de la empresa suelen contener información personal o confidencial. Evita ingresar a estas plataformas cuando estés conectado a una red Wi-Fi pública para proteger tus datos.

Desactiva la opción de Wi-Fi en tus dispositivos cuando no los estés utilizando

Mantén la opción de Wi-Fi desactivada en tus dispositivos cuando no los estés utilizando para evitar conexiones automáticas a redes Wi-Fi no seguras. Esto reducirá las oportunidades de exposición a posibles ataques o accesos no autorizados a través de la red.

Utiliza una VPN al ingresar al correo o a una aplicación de la empresa desde una red ajena a la institución

Cuando necesites acceder a correos electrónicos o aplicaciones de la empresa desde una red Wi-Fi que no pertenezca a la institución, es recomendable utilizar una VPN (Red Privada Virtual). Esto cifrará toda la información enviada y recibida, proporcionando una capa adicional de seguridad.

No descargues ningún tipo de software cuando estés conectado a redes abiertas

Descargar software de fuentes desconocidas o no confiables mientras estás conectado a redes Wi-Fi abiertas puede exponerte a riesgos de malware. Evita descargar aplicaciones o programas cuando estés conectado a estas redes para garantizar la seguridad de tu dispositivo.

Más información

www.micitt.go.cr

csirt@micitt.go.cr

(506) 2539-2200