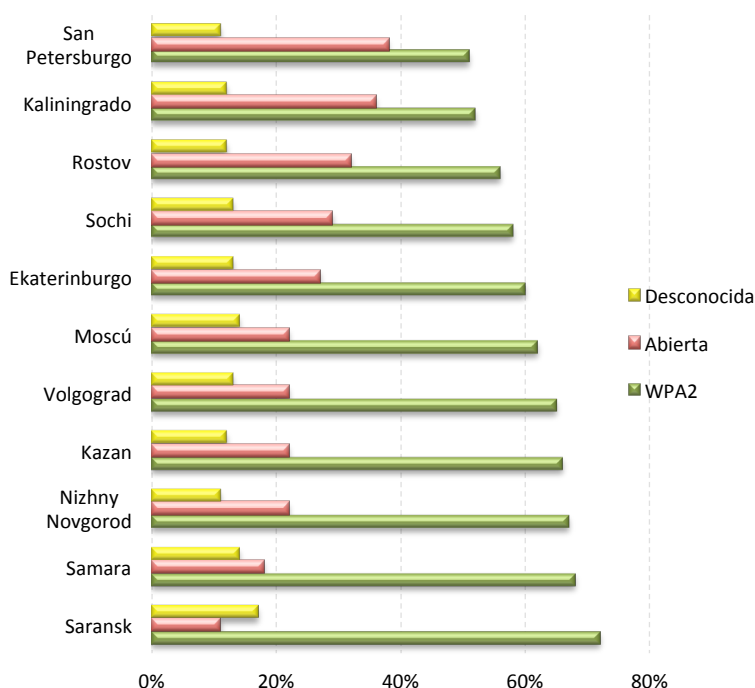


## Accesos WiFi en el Mundial de Rusia

### La FIFA publicó el estado de los accesos WiFi en cada Sede del Campeonato del Mundo



Todos sabemos lo fácil que es para los usuarios conectarse a redes Wi-Fi abiertas en lugares públicos. Bueno, es igualmente sencillo para los delincuentes ubicarse cerca de puntos de acceso poco protegidos, donde pueden interceptar el tráfico de la red y comprometer los datos del usuario.

La falta de cifrado de tráfico esencial para las redes Wi-Fi en las que se llevan a cabo actividades oficiales y mundiales, como en las ubicaciones de la **Copa Mundial de la FIFA 2018**, ofrece un terreno especialmente fértil para los delincuentes.

Con esto en mente, ¿pueden los fanáticos del fútbol sentirse digitalmente seguros en las ciudades anfitrionas? ¿Cómo difiere la situación con el acceso a Wi-Fi de una ciudad a otra? Para responder a estas preguntas se han analizado los puntos de acceso confiables y no confiables existentes en 11 ciudades sede de la Copa Mundial de la FIFA: **Saransk, Samara, Nizhny Novgorod, Kazán, Volgograd, Moscú, Ekaterinburgo, Sochi, Rostov, Kaliningrado y San Petersburgo.**

La característica principal de la investigación es la telemetría, que tiene como objetivo asegurar las conexiones Wi-Fi de los usuarios y activar VPN (Red Privada Virtual) cuando sea necesario.

Las estadísticas se generaron a partir de usuarios que voluntariamente aceptaron que se recopilaran sus datos. Para la investigación, solo se evaluó la seguridad de los puntos Wi-Fi públicos. Incluso con relativamente pocos lugares públicos de Wi-Fi en las ciudades pequeñas se obtuvo una base suficiente para el análisis: casi 32.000 puntos de acceso Wi-Fi.

La ciudad más segura (en términos de Wi-Fi pública) resultó ser **Saransk**, con el 72% de los puntos de acceso protegidos por encriptación de protocolo WPA / WPA2. Las tres ciudades con la mayor proporción de conexiones no seguras son **San Petersburgo** (48% de los puntos de acceso Wi-Fi no están garantizados), **Kaliningrado** (47%) y **Rostov** (44%). Una vez más, se debe tener en cuenta la relatividad de los resultados. Incluso una conexión WPA2 en un café no puede considerarse segura si la contraseña es visible para todos.

### Medidas de seguridad cuando nos conectamos a redes WiFi públicas

Aunque no hayas estado en Rusia para este mundial, y solo lo estés sufriendo por la tele, tené en cuenta estas recomendaciones a la hora de conectarte a una red pública con algún dispositivo (notebook, tablet, celular, etc.)

- ✓ Siempre que sea posible, conectate a través de una red privada virtual (VPN). Con una VPN, el tráfico cifrado se transmite a través de un túnel protegido, lo que significa que los delincuentes no podrán leer sus datos, incluso si obtienen acceso a ellos.
- ✓ No confíes en las redes que no están protegidas con contraseña o que tienen contraseñas fáciles de adivinar o de encontrar. Los defraudadores pueden descubrir la contraseña de la red en una cafetería, por ejemplo, y luego crear una conexión falsa usando la misma contraseña. Esto les permite robar fácilmente los datos personales del usuario. Solo debés confiar en los nombres y contraseñas de red que te proporcionen los empleados de un establecimiento.
- ✓ Para maximizar tu protección, apagá tu conexión Wi-Fi cuando no la estés usando. Esto también ahorrará vida a la batería. Te recomendamos que también desactives las conexiones automáticas a las redes Wi-Fi existentes.
- ✓ Si no estás 100% seguro de que la red inalámbrica que estás usando es segura, pero aún necesitás conectarte a Internet, intentá limitarte a las acciones básicas del usuario, como buscar información. Debés abstenerte de ingresar datos de inicio de sesión para las redes sociales o servicios de correo, y definitivamente no realizar ninguna operación de banca en línea ni ingresar los datos de tu tarjeta bancaria en ninguna parte.
- ✓ Para evitar convertirte en un objetivo cibercriminal, debés habilitar la opción "Usar siempre una conexión segura" (HTTPS) en la configuración de tu dispositivo. Se recomienda habilitar esta opción cuando visites cualquier sitio web que consideres que puede carecer de la protección necesaria.