Publicado en Ciudad de México el 26/07/2017

# [Riverbed da a conocer cinco maneras de cuidar la información personal al utilizar redes Wi-Fi públicas](http://www.notasdeprensa.es)

## Las redes públicas en cafeterías, aeropuertos, estaciones de tren y en el lugar de trabajo sin duda son muy convenientes, especialmente cuando se quieren evitar grandes cuentas por roaming o el plan mensual de datos se está agotando. En ese momento es cuando se confía en los hotspots Wi-Fi, ya que con sólo uno clic se puede acceder a una conexión rápida a Internet siendo la mayoría de las veces de manera gratuita

 Riverbed Technology, la compañía de rendimiento de aplicaciones y Xirrus el proveedor líder de redes Wi-Fi de próxima generación que refuerza la solución SD-WAN Riverbed SteelConnect, comparten consejos prácticos para que los usuarios se mantengan protegidos al acceder a internet mediante redes Wi-Fi públicas. La posibilidad de acceder a una conexión inalámbrica a través de hotspots públicos contiene cierto riesgo. Los hackers, que están conectados a la misma red, pueden controlar datos personales sin mucho esfuerzo. Muchos proveedores no utilizan seguridad de cifrado. El cifrado transforma toda la información que utiliza en línea en un código que es inaccesible para otros y, por lo tanto, asegura que sus datos personales sean seguros. Un dispositivo que está conectado a una red abierta puede ser hackeado en menos de dos segundos sin que el usuario se de cuenta. Existe el riesgo de que un hotspot sea creado por un ciberdelincuente, imitando ser uno público y seguro. Esto ocurre más comúnmente en lugares donde se espera que haya Wi-Fi público, por ejemplo, cerca de lugares turísticos populares. Los hotspots Wi-Fi falsos utilizan nombres inofensivos como and #39;Wi-Fi gratuito and #39; y pueden usarse para recopilar datos personales e información, como datos bancarios, contraseñas, así como correos electrónicos. Para evitar caer en lo anterior, a continuación 5 consejos para protegerse mientras se esté conectado a un hotspot Wi-Fi público. Habilitar firewalls: Se debe asegurar que el dispositivo está protegido con un firewall fuerte para evitar posibles amenazas de seguridad de otros usuarios de la red. Mantener el software actualizado para tener la última protección de antivirus es muy importante. Utilizar una Red Privada Virtual (VPN): Esto cifrará y permitirá el anonimato. Los atacantes sólo pueden ver que hay una conexión a un servidor VPN pero no son capaces de monitorear qué datos se envían usando esa red. Simplemente hay que descargar una aplicación VPN en el dispositivo y hay que encenderla al conectarse a una red pública. Estar atentos: Antes de conectarse a una red Wi-Fi pública, es prioritario leer los términos y condiciones en caso de hayan. Además, hay que asegurar de enviar sólo información en sitios web que comiencen con HTTPS en lugar de HTTP. Esto significa un sitio seguro que cifra los datos transmitidos y su información tiene un mayor grado de seguridad. Examinar con precaución: Generalmente, se debe evitar acceder a sitios web que soliciten datos confidenciales como contraseñas, números de tarjeta de crédito o de cuenta. Si eso es inevitable, hay que salir de las cuentas personales tan pronto como haya terminado, por lo que ya no están sujetos a la exposición. Apagar la red Wi-Fi cuando no esté en uso: Incluso cuando no esté conectado a una red Wi-Fi, la computadora portátil o smartphone todavía envía datos desde y hacia cualquier red dentro de un rango determinado. Para evitar que un dispositivo se conecte automáticamente a redes que puede haber utilizado en el pasado, se deben desactivar las conexiones automáticas en su configuración. Hay una manera de utilizar los hotspots públicos de forma segura sin descargar ninguna aplicación. Xirrus EasyPass combina seguridad y simplicidad, permitiendo que los invitados, visitantes y empleados creen de forma automática y sencilla su propia red Wi-Fi personal segura en una Wi-Fi pública. Esto protege a los usuarios y sus datos al acceder a redes públicas Wi-Fi, redes invitadas y entornos de hotspots. Conecta con RiverbedFacebook LinkedIn Riverbed Blog Riverbed Community Twitter (@Riverbed) YouTube SlideShare Google+Riverbed ofrece la plataforma más completa para que las empresas aseguren que sus aplicaciones funcionen como se espera, la información está disponible cuando se necesita y los problemas en el rendimiento pueden ser detectados y resueltos antes de impactar en el negocio. Riverbed permite a las empresas híbridas transformar el rendimiento de las aplicaciones en una ventaja competitiva al maximizar la productividad de los empleados y aprovechar las TI para crear nuevas formas de agilidad operativa. Los 28.000 clientes de Riverbed incluyen 97% de los Fortune 100 y 98% de Forbes Global 100. Más información enwww.riverbed.com. Riverbed y cualquier nombre o logotipo de producto o servicio de Riverbed utilizados en el presente documento son marcas comerciales de Riverbed Technology, Inc. Todas las demás marcas comerciales aquí utilizadas pertenecen a sus respectivos propietarios.

**Datos de contacto:**

Flor Carreño

Marketing Q S

56152196

Nota de prensa publicada en: [https://www.mexicopress.com.mx/riverbed-da-a-conocer-cinco-maneras-de-cuidar](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Emprendedores E-Commerce Software Ciberseguridad Dispositivos móviles



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)