



Navegando por un túnel con una VPN

La Red Privada Virtual (o VPN por sus siglas en inglés) es un programa informático que podemos instalar ya sea en nuestra computadora o teléfono celular, y que sirve para navegar por internet de forma más segura.

Igual que cuando caminamos sobre la arena, al navegar en internet dejamos huellas o **rastros digitales**. Los rastros digitales son diferentes tipos de datos. Algunos son intencionales, por ejemplo un mensaje que publicamos en Twitter. Otros en cambio son involuntarios, como nuestro historial de navegación o nuestra **IP** (una secuencia de números que nos identifica cuando nos conectamos a internet).

Igual que un rompecabezas, cuando nuestros rastros digitales se juntan revelan muchas cosas sobre nuestra vida, incluyendo información privada como nuestro estado de salud, nuestros intereses sexuales, etc.



Empresas tecnológicas como Google recolectan activamente todo tipo de datos sobre nuestro comportamiento e intereses en internet, y luego venden nuestros perfiles a empresas publicitarias. Los gobiernos y aparatos militares también tienen acceso a nuestros rastros digitales y cuentan con recursos para analizar esa información y crear perfiles específicos sobre nosotros.

¿Qué podemos hacer?

No podemos tener total control sobre nuestros datos, porque no todos los datos son iguales, ni fueron creados en el mismo sitio, ni se almacenan en el mismo lugar. Pero podemos tomar algunos pasos para reducir nuestra huella digital. Uno de esos pasos es usar una VPN.

La idea de una VPN es que nos conectamos a internet, no desde el punto en el que nos encontramos, sino que salimos de una forma segura por un punto diferente a internet. Una VPN hace un túnel de cifrado entre nuestra computadora y ese nuevo punto de salida hacia internet y todo el tráfico pasa a través de ese túnel. De esta forma logramos que terceras personas **no puedan ver que páginas estamos visitando**.



¿Que quiere decir otro punto de salida de internet?

La información de las páginas web está almacenada en otras computadoras que están siempre conectadas a internet, estos son los servidores web. Cuando hacemos clic en un enlace, la solicitud de información va a nuestro proveedor de internet (por ejemplo Claro, Movistar o Tigo), y luego continúa dando saltos de un servidor a otro hasta llegar al que tiene la información que queremos, para luego regresar con lo que le habíamos pedido. Por la forma cómo funciona la red, nuestro proveedor de internet y todos los demás servidores saben que páginas estamos visitando, y por lo general guardan registros de esta actividad.

Suscríbete a ResistenciaDigital en Telegram @CanalResistenciaDigital

Con una VPN no salimos a la red a través de nuestro proveedor de internet directamente, sino a través de nuestro **proveedor de VPN**. De esta forma **ocultamos nuestra ubicación geográfica** al cambiar de IP, **evadimos la censura** geolocalizada y navegamos de forma más **privada y segura**.

Algunas VPNs que sugerimos revisar son IpredatorVPN, Mullvad, y Bitmask que tiene varios proveedores: Riseup y Calyx (disponibles en F-Droid), Colnodo y Código Sur.



¿Cómo escoger una VPN?

Por lo general los proveedores de VPN no guardan registro de nuestra actividad en internet, pero no siempre es el caso. Algunas VPNs cobran por el servicio y otras son gratuitas, pero esto no implica que unas sean mejor que otras por eso. Es muy importante elegir un proveedor de VPN que nos de **confianza**, que se posicione en defensa de la **seguridad y privacidad** de las personas usuarias, y que sea cercano a los **movimientos sociales** y grupos **activistas**.

También es bueno que sea un colectivo o empresa con quien se pueda tener una relación directa, y de quienes conozcamos su trabajo o podamos conocer su historia y prácticas de seguridad.



¡No olvides que puedes imprimir tu propia MilpaDigital y compartirla!



CódigoSur
EDICIONES