

¿Pueden las VPN superar las restricciones a plataformas de streaming en Venezuela?

En Venezuela, la censura digital continúa intensificándose bajo la administración de Nicolás Maduro, afectando significativamente la vida cotidiana de los ciudadanos que cuentan con servicios en línea. Durante el segundo fin de semana de agosto, nuevas plataformas como Disney Plus, Max Latinoamérica, Mercado Libre y Binance se sumaron a la [lista de sitios bloqueados](#) por el gobierno, según reportes de la organización VE Sin Filtro.

Estos bloqueos, aplicados principalmente por la estatal Cantv a través de DNS, reflejan una tendencia creciente hacia la restricción del acceso a servicios de entretenimiento y herramientas digitales, obligando a los usuarios a buscar soluciones alternativas como el uso de VPNs (Redes Privadas Virtuales), pero ¿son realmente efectivas?

□ [#CANTV](#) está bloqueando plataformas de streaming [@StreamMaxLA](#) y [@disneyplusla](#) desde hace días.

Tanto Max, como Disney+ sufren un bloqueo DNS en CANTV.

No hay una explicación oficial hasta el momento de estos bloqueos a plataformas de entretenimiento. pic.twitter.com/CgN2XE4fJw

– VE sin Filtro (@vesinfiltro) [August 11, 2024](#)

El equipo de [Redes Ayuda](#) conversó con **TalCual** para explicar si existen limitaciones o riesgos al usar una VPN para acceder a plataformas de streaming y servicios en línea.

¿Qué es una VPN?

Una VPN es una herramienta que permite a los usuarios navegar por Internet de una forma más segura y privada. Esta crea un “túnel virtual” entre tu dispositivo (teléfono, tablet, computadora) y el servidor que estés utilizando, que puede estar en cualquier parte del mundo. Al activar una VPN, toda la información que viaja entre tu dispositivo y el servidor de la VPN estará cifrada, es decir, que esta información no podrá ser leída por terceros, como hackers o tu proveedor de Internet.

«Cuando nos conectamos a una VPN, parece como si estuviéramos navegando en Internet desde una ubicación diferente a la que realmente estamos. Por ejemplo, si estás en Caracas y te conectas a un servidor VPN ubicado en Miami, los sitios web que visitas creerán que te encuentras en Miami, Estados Unidos, en lugar de Venezuela. Esto es especialmente útil en contextos de censura como el que se vive en el país, donde los principales proveedores de Internet (ISP) bloquean el acceso a plataformas digitales como X y a decenas de sitios web de medios de comunicación», declaró Redes Ayuda.

¿Qué puedes ver y qué no?

La organización explicó que servicios de streaming como Disney+, Max, Netflix han implementado tecnología que permite detectar y bloquear temporalmente el acceso a sus contenidos cuando un usuario se conecta desde servidores VPN. Esto significa que puede ser relativamente fácil para la plataforma identificar que estás usando una VPN para acceder a su contenido.

«Cuando una plataforma detecta que estás usando una VPN, normalmente restringe el acceso al contenido de varias maneras. Puede bloquear temporalmente el acceso hasta que desactives la VPN, mostrarte un mensaje advirtiéndote que estás utilizando una VPN, o limitarte a un catálogo reducido disponible en la región del servidor VPN al que estás conectado. Es importante entender que, aunque una VPN te permite cambiar tu ubicación virtualmente, esto no garantiza el acceso a todos los catálogos de contenido».

Algunos títulos pueden tener licencias diferentes según la región, lo que significa que, incluso con una VPN activa, no siempre podrás acceder al contenido que deseas.

Además, aunque el uso de una VPN para acceder a contenido bloqueado no es ilegal, puede violar los términos y condiciones de las plataformas de streaming. Esto, aunque no es común, podría resultar en medidas contra la cuenta del usuario, como advertencias, restricciones temporales o, en casos extremos, la suspensión de la cuenta.

Redes Ayuda explica que las plataformas de entretenimiento suelen actualizar sus sistemas regularmente para bloquear el acceso de usuarios que intentan eludir las restricciones regionales con VPNs. «Esto se debe a que no les conviene como plataforma que los usuarios utilicen herramientas para acceder a contenido fuera de sus regiones designadas», indican.

Ventajas y desventajas de una VPN

Resaltaron la importancia de conocer bien la VPN que se descarga, ya que algunas VPN gratuitas o de baja calidad pueden comprometer la privacidad, registrar la actividad en línea, o incluso exponer los dispositivos a malware.

Otra desventaja significativa es la posible disminución en la velocidad de conexión a Internet al usar una VPN, lo que puede afectar la calidad del video, resultando en tiempos de carga más largos y una reducción en la calidad de la imagen. Esta situación no solo afecta la experiencia del usuario, sino que también agrava la frustración de quienes pagan por servicios de entretenimiento y se ven limitados por bloqueos del gobierno.

La organización también menciona que algunas aplicaciones de VPN, como [Riseup](#), [ProtonVPN](#), [TunnelBear](#) o [Psiphon](#), ofrecen una función de «split tunneling» o «túnel dividido», que permite seleccionar qué aplicaciones específicas no usarán la VPN y accederán directamente a través del proveedor de Internet. Esta opción puede ser útil para mantener una conexión más estable mientras se accede a servicios de streaming.

Esto es especialmente útil si, por ejemplo, quieres mantener la VPN activa para acceder a plataformas bloqueadas como X, pero al mismo tiempo se necesita usar aplicaciones como las de bancos o servicios de streaming como Disney+ o Max, que pueden bloquear el acceso si detectan una VPN.

«Por ejemplo, imagina que tienes activa tu VPN para evadir la censura y acceder a sitios web de noticias bloqueados mientras navegas por Internet. Sin embargo, necesitas acceder a la aplicación de tu banco o a Disney+, que no permiten el uso de VPN. Si tu VPN tiene la opción de «split tunneling», puedes configurarla para que la aplicación del banco o la de streaming no pasen por la VPN. De este modo, cuando abras estas aplicaciones con la VPN activa, se conectarán directamente a través del servidor de tu proveedor de Internet, permitiéndote utilizarlas sin problemas. Mientras tanto, todo el resto de tu tráfico, como la navegación web o el uso de redes sociales, seguirá protegido por la VPN», explicó el equipo.

Recomendaciones para elegir una VPN confiable

Redes Ayuda compartió sus recomendaciones para elegir e instalar VPN confiable y con interfaces simples e intuitivas para su

activación. Las principales son Proton, TunnelBear, Psiphon, Riseup, que solo requieren un par de clics para activarse y no necesitan configuraciones complicadas. De hecho, algunas de ellas permiten el acceso sin necesidad de crear una cuenta.

Te recomendamos tener mas de una opción de VPN instalada en tus dispositivos. Entre las opciones que hay, te recomendamos:

- Proton VPN
- Psiphon
- Lantern
- Tunnel Bear
- RiseupVPN

Toma en cuenta que NO debes activar mas de una VPN al mismo tiempo.

Activa tu VPN, evade...

- RedesAyuda (@RedesAyuda) [August 9, 2024](#)

Comentan que, aunque pueda parecer algo complicado, estas herramientas están diseñadas para ser fáciles de usar, incluso para quienes no tienen mucha experiencia con la tecnología.

«Si es tu primera vez usando una VPN, no dudes en pedir ayuda. Puedes recurrir a un familiar, amigo, o incluso buscar orientación e información en Internet. Existen fuentes confiables como RedesAyuda o VE Sin Filtro que, a través de sus redes sociales, ofrecen videos tutoriales que explican de manera sencilla qué herramientas descargar, cómo instalarlas y cómo utilizarlas», señalaron.

Una de las mayores ventajas de usar una VPN es la posibilidad de seguir accediendo a sitios de noticias o a plataformas como X (anteriormente Twitter), que actualmente están bloqueadas por los principales proveedores de Internet en Venezuela. Con una VPN, se pueden evadir estos bloqueos y continuar presente en estos espacios ejerciendo tu derecho al acceso a la información y a la libertad de expresión, en un contexto donde cada vez censuran nuestros espacios.

Es recomendable tener al menos dos VPN instaladas en tus dispositivos, aunque no se deben activar ambas al mismo tiempo; tener más de una opción te proporciona flexibilidad si alguna de las VPN presenta problemas.

Por último, es fundamental mantener siempre actualizadas estas aplicaciones, ya que las actualizaciones suelen incluir mejoras

y nuevas funciones que pueden ser beneficiosas.

Con información de TalCual