

Guía de buenas prácticas para saltar el bloqueo comunicacional en la web

Justicia social en Venezuela para acceder a internet.



Guía de Buenas Prácticas para Saltar el Bloqueo Comunicacional en la Web

Indice

Introducción.....	2
1. Buenas Prácticas para Saltar el Bloqueo Comunicacional	3
1.1. Uso adecuado de internet	3
1.2. Prácticas seguras para saltar el bloqueo de sitios web y redes sociales	8
1.3. Recomendaciones generales	10
2. Aplicaciones para saltar el bloqueo comunicacional en la Web.....	11
2.1 Aplicaciones para PC	11
2.2 Aplicaciones para Dispositivos Móviles.....	12
2.3 Instalando Aplicaciones para PCs.....	13
1. Kproxy	13
2. Opera	15
3. Proton	17
4. Psiphon.....	21
5. Tor	22
6. Windscribe.....	23
2.4 Instalando Aplicaciones para Dispositivos Móviles.	25
1. Opera	25
2. Proton	25
3. Tor	26
4. Windscribe.....	27
5. Hide Me VPN.....	27
6. Urban	28
7. Turbo	29
3. Patrocinadores	31

Introducción

Esta Guía comienza dando consejos prácticos sobre el uso adecuado de Internet; desde los muy básicos como el uso apropiado de las contraseñas, las cookies, los dispositivos de seguridad que deben tener los equipos de acceso y trabajo, así como las precauciones para identificar los peligros que se corren mediante el uso de navegadores y cuáles son las mejores prácticas que se deben tener en cuenta para acceder a esta red global.

Se tiene presente y, se corresponde con una de las partes resaltantes de la Guía, la identificación de Prácticas Seguras para saltar el bloqueo de sitios web y plataformas de redes sociales, con el fin de ayudar a los usuarios en el acceso a la información, garantizando al propio tiempo el anonimato y el cifrado de datos.

El objetivo principal de la Guía se logra cuando ofrecemos los resultados de la revisión de las aplicaciones para saltar el bloqueo comunicacional en la Web y en plataformas tecnológicas sociales; y esto se logra luego de instalar y probar la mayoría de las aplicaciones de software que se ofrecen y promueven en Internet para este fin; además, se indican cuáles son las opciones recomendadas resultantes de este estudio, tanto para PCs como para móviles, basados en criterios tales como: rendimiento, velocidad, seguridad y anonimato del usuario, y se fundamentados en las sugerencias que existen en la web sobre cuáles de ellas son recomendadas para Venezuela; de igual manera, se indica dónde ubicar y seguir el correspondiente lugar de encuentro y las ayudas publicadas por los autores u organizaciones que las promueven.

Guía al usuario en el procedimiento a seguir en cada aplicación y se despliegan pantallas que identifican cada uno de los pasos que se deben seguir en la implementación o instalación del software recomendado, haciendo muy sencillo el trabajo a seguir. Todo esto hace que el usuario no requiera amplios conocimientos técnicos en la materia.

Por último, se debe aclarar que la Guía Antibloqueo no pretende ir en contra de obligaciones legales o judiciales nacionales, vinculadas con la prohibición de algunas publicaciones de información, y deja en manos de cada individuo u organización, la responsabilidad de su uso.

1. Buenas Prácticas para Saltar el Bloqueo Comunicacional

1.1. Uso adecuado de internet

Al seguir buenas prácticas sobre el uso de internet se garantiza la seguridad y protección de los datos en el momento de acceder a páginas web y redes sociales bloqueadas; así como también se evita ser víctima de delincuentes o agentes de inteligencia que podrían localizarte física y virtualmente. Entre las prácticas que más utilizan se pueden mencionar las siguientes:

A.1 Utiliza una buena contraseña al requerir servicios de internet

- Se recomienda seleccionar una contraseña que contenga como mínimo 6 caracteres y que esté conformada por letras mayúsculas, minúsculas, números y algún carácter especial.
- No es recomendable utilizar contraseñas débiles de fácil acceso, como la fecha de cumpleaños o números en serie.
- Es conveniente cambiar periódicamente la contraseña.
- Utiliza contraseñas diferentes en los servicios online que tengas habilitados, tales como: banca, correo electrónico, redes sociales, etc.

Crea contraseñas seguras, que no contengan datos personales y que combinen símbolos, letras y números.

A.2 Toma precauciones al momento de guardar la contraseña en el navegador

- No se recomienda guardar la contraseña en el navegador que utilizas para acceder a internet, cuando éste le da la opción de recordarla. Si en algún momento se guardó verifica que fue eliminada.
- Deshabilita la opción de guardar la contraseña del navegador, por defecto ésta opción está activa.
- Toma precauciones de borrar la contraseña cuando navegues en computadores públicos o que no uses frecuentemente.

No guardes la contraseña en el navegador que utilizas para acceder a internet.

A.3 Elimina las cookies al momento de acceder a un sitio web

- Elimina las cookies¹ de la sesión que se habilita al momento de acceder a un sitio web.
- Se recomienda borrar las cookies después de navegar y borrar el historial de navegación; o configurar el navegador para que se borren automáticamente.
- Otra opción que se sugiere es navegar en modo privado o incógnito, de esta manera se inicia una sesión sin utilizar los datos ya almacenados en el navegador y al terminar se borrarán las cookies, el historial de navegación y otros datos que se hayan creado.

Después de acceder a un sitio web elimina las cookies, éstas guardan información que recuerdan datos de navegación como hábitos y preferencias.

A.4 Mantén un antivirus en tus dispositivos que te garantice la seguridad al descargar archivos y acceder a internet

- Se recomienda utilizar un buen antivirus que garantice un análisis riguroso de los dispositivos que se utilizan para acceder a internet, y que inmediatamente después de la descarga de cualquier archivo los analice e informe cualquier anomalía.
- Es recomendable estar informado sobre las últimas amenazas y fraudes que circulan por internet, te ayudarán a estar más protegido y conocer los virus potenciales.

No dejes tus dispositivos desprotegidos, utiliza un buen antivirus.

¹ Las cookies son unos pequeños ficheros que guardan información sobre la sesión que habilitas al acceder a un sitio web, de esta manera se facilitan las conexiones futuras y se recuerdan datos de navegación como hábitos y preferencias.

A.5 Mantén actualizado el software de los dispositivos que se utilizan para acceder a internet y los navegadores

- Actualiza los sistemas operativos y el software de los dispositivos que utilices para acceder a internet, siempre que sea posible.
- No utilices sistemas operativos o software que no te permitan realizar las actualizaciones del mismo.
- Actualiza el software sólo de sitios oficiales.

Actualiza el sistema operativo y software de los dispositivos que utilizas para acceder a internet.

A.6 Utiliza conexiones seguras para acceder a internet, ten cuidado con el uso de redes públicas

- Es importante reconocer el URL (dirección) del sitio que se visita y asegurarse de que haya una conexión segura (https://) sin errores o alertas de parte del navegador. Si el navegador dice que la conexión no es segura, desconfía inmediatamente del sitio.
- Asegúrate de que la red inalámbrica a la que te estás conectando a internet sea segura. Si no tienes claro que es segura, mejor no acceder a aplicaciones o páginas web que contengan tus datos personales. No confíes en las redes públicas.
- Ten cuidado al utilizar computadores de uso público. Si se usa, no olvides cerrar las sesiones abiertas de los navegadores y servicios de internet que utilizaste.
- Asegúrate de eliminar del computador público la información o datos que descargaste al utilizar el correo electrónico, acceder a páginas web, o servicios como Google Drive o Dropbox; ya que al utilizar estos servicios se transfiere información, imágenes, posicionamiento, historial, etc.
- Es recomendable utilizar el navegador de incógnito cuando se accede a computadores o dispositivos de uso público.

Utiliza siempre conexiones seguras y se más riguroso al usar redes públicas.

A.7 Realiza buenas prácticas al utilizar servicios de internet como el correo electrónico y las redes sociales

- Elimina los correos no solicitados o de dudosa procedencia.
- No abras los enlaces que aparezcan en los correos electrónicos no solicitados o de remitentes que desconoces para evitar ser víctima de fraudes y malware.
- Verifica la información que aparezca en internet. No des credibilidad a todo lo que se publique en internet sin contrastar la veracidad de las noticias, ni difundiendo bulos o noticias falsas.
- Comprueba las opciones de privacidad de los perfiles que tengas en redes sociales (lo que otras personas pueden ver cuando acceden a tu perfil).
- No dejes las opciones de privacidad de las redes sociales por defecto, que sólo se publique lo que desees.
- Tras la apertura de una cuenta en redes sociales, en cualquier lugar o aplicación es necesario revisar siempre las opciones de configuración del lugar.
- No dejes las opciones por defecto tras la apertura de una cuenta en redes sociales, en cualquier lugar o aplicación.
- Las opciones de configuración por defecto suelen pasar desapercibidas pero influyen en la privacidad de los datos; por lo general incluyen el permiso para envío de mensajes propagandísticos, la apertura al público general de nuestros mensajes o imágenes personales y hace que demasiada información quede accesible a desconocidos, poniendo en riesgo la protección de los datos e información personal.
- Es importante ser consciente de los peligros que puede entrañar, indicar tu localización geográfica a través de redes sociales.

- No des información de tu geolocalización. La geolocalización permite obtener la situación física de un dispositivo en un determinado momento. Los dispositivos móviles, conectados permanentemente a internet, permiten geolocalizarlos siempre que se le dé el permiso.
- Publicar la posición del dispositivo móvil en redes sociales o en internet puede ser un regalo para un delincuente cibernético o agente de inteligencia.

Aplica buenas prácticas al usar el correo electrónico y las redes sociales. No seas víctima de fraudes y violación de la privacidad de tus datos e información personal, por parte de delincuentes o agentes de inteligencia. No des información de tu geolocalización en las redes sociales.

A.8 Se vigilante de la seguridad de tus datos e información almacenada en tus dispositivos

- Realiza copias de seguridad de la información que almacenas en tus dispositivos. De esta manera, en caso de intrusión (hackeo), pérdida o robo del dispositivo, siempre podrás recuperar tus datos.
- Mantén una copia de tus datos e información en servicios habilitados en la nube, tales como: Google Drive, Dropbox, entre otros.

Resguarda tus datos e información personal en dispositivos de almacenamiento local y servicios en la nube.

1.2. Prácticas seguras para saltar el bloqueo de sitios web y redes sociales

Ante un bloqueo de sitios web y redes sociales es recomendable realizar prácticas que ayuden a los usuarios a acceder a la información, garantizando el anonimato y cifrado de datos. Entre las prácticas documentadas y más recomendadas se pueden mencionar las siguientes:

B.1 Utiliza aplicaciones y herramientas que garanticen el anonimato y el cifrado de datos²

- **VPN:** Mantén activa en tu dispositivo una Red Privada Virtual (RPV en español o VPN en sus siglas en inglés). La VPN funciona como un intermediario que utiliza direcciones IP de distintos países que proporcionan estas aplicaciones para ingresar a páginas web bloqueadas o restringidas por el Proveedor de Servicio de Internet (PSI en español o ISP en sus siglas en inglés).
- **PROXY:** Activa un Proxy en el dispositivo, esta herramienta permite realizar una solicitud para acceder a la página web desde una dirección IP distinta a la establecida por el Proveedor de Servicio de Internet (ISP), lo que permitirá el ingreso a la página bloqueada.
- **TOR:** Activa en el dispositivo el Sistema The Onion Router (TOR en sus siglas en inglés). TOR desvía la conexión del ISP que utiliza el usuario que intenta acceder a contenido bloqueado, mediante nodos que forman parte de esta red, cada uno de estos nodos posee una dirección IP distinta que es proporcionada por TOR aleatoriamente, lo cual hace que el proceso de acceder a una página web sea más seguro. TOR funciona como un puente que evita que el ISP detecte a la persona que hace la petición de ingreso; este sistema se habilita a través de un navegador.

Para el caso de esta Guía de Buenas Prácticas se recomienda utilizar las VPN; ya que garantizan mecanismos sencillos para acceder a páginas web bloqueadas y redes sociales, así como también el anonimato y cifrado de tus datos.

² <https://redesayuda.org/2019/06/13/ante-la-censura-del-regimen-herramientas-para-evadir-la-censura/>

B.2 Otras alternativas para saltar el bloqueo que requieren más conocimientos tecnológicos, por parte del usuario³

- **DNS:** Cambia el Sistema de Nombres de Dominio (DNS en sus siglas en ingles) en el dispositivo que se utiliza para acceder al sitio web bloqueado. Se recomienda utilizar los siguientes servidores DNS: Servidores DNS de Google (8.8.8.8 y 8.8.8.4) y Servidores de IBM (1.1.1.1).
- **Usa la IP del dominio en lugar de la URL.** En la mayoría de los casos el ISP realiza el bloqueo a nivel de DNS, lo que impide que se pueda acceder a la URL del sitio web, pero no a la IP del dominio. Por lo tanto, una práctica recomendada es utilizar la IP del dominio en vez de la URL del sitio web.
- **Usa traductores online:** Algunos traductores online sirven para acceder a páginas web bloqueadas. En este caso se recomienda ingresar a la herramienta, como Google Translate, escribir la URL, solicitar traducirla a otro idioma, diferente en el que se encuentra originalmente, y se deja que el traductor online acceda a la web bloqueada.
- **Usa plugin Anonymo X en Chrome o Firefox:** AnonymoX es un plugin o extensión para Chrome y Firefox que permite: navegar de forma anónima por internet, cambiar la IP y el país de esta, acceder a páginas web bloqueadas. Por lo tanto, es recomendable mantener activo el plugin Anonymo X para acceder a páginas web bloqueadas.
- **Usa la página web llamada unblocked:** Esta web permite acceder a versiones alternativas de decenas de páginas web que suelen estar bloqueadas. Por lo tanto, ingrese a la página *unblocked*, coloque el nombre de la web deseada, si se encuentra en la lista que contiene *unblocked*, se puede acceder a la misma.
- **Restablece la web bloqueada a través del correo electrónico:** Al utilizar el servicio web2mail se puede recuperar una copia de la web bloqueada por correo electrónico. Por lo tanto, el uso de web2mail representa una alternativa para acceder a páginas web.
- **Usa el caché de Google:** Si el bloqueo de la página es reciente se puede buscar el dominio de la página web bloqueada en Google, para ello se requiere pinchar sobre la flecha verde que está justo a la URL, seguidamente se abre la opción Caché, la cual permite acceder a la versión guardada que tiene Google de una web en concreto.

³ <https://www.adslzone.net/como-se-hace/internet/saltarse-bloqueo-pagina-web/>

1.3. Recomendaciones generales

- a. El uso de herramientas y aplicaciones para desbloquear páginas web es responsabilidad de los ciudadanos. No se recomienda acceder a páginas web censuradas legalmente por organismos públicos o judiciales, y/o que contengan contenidos que atentan contra la moralidad de los ciudadanos y población vulnerable, como niños y adolescentes.
- b. Se recomienda a los ciudadanos que estén informados sobre el marco legal que permite la defensa de los Derechos de Internet y Derechos Económicos, Sociales y Culturales (Ver anexo - marco legal. De esta manera, se puede detectar la violación de los mismos y aplicar prácticas que garanticen su seguridad jurídica, al momento de desbloquear sitios web.
- c. Se replicador de las buenas prácticas del uso de internet entre tus amigos y personas que tienen menos conocimientos sobre el uso de las tecnologías digitales. Estas prácticas pueden evitar que seas víctima de delincuentes informáticos y agentes de inteligencia que podrían atentar contra tu integridad, al momento de desbloquear sitios web y acceder a contenidos de interés.
- d. Toda buena práctica enriquece tu educación tecnológica, y te garantiza tu seguridad y protección de tus datos. No navegues abiertamente, se recomienda navegar de forma anónima por Internet.
- e. Si estas usando una VPN es recomendable mantenerla conectada y activa continuamente en tus dispositivos. De esta manera, se puede navegar en internet protegido y seguro; así como también se logra desbloquear sitios web de manera transparente.
- f. Si notas que la velocidad de tu conexión es más lenta, activar una VPN podría ayudarte. Solo como una solución temporal, pues lo recomendable es ponerte en contacto con tu proveedor del servicio si tienes problemas de conexión.
- g. Si te conectas a redes inalámbricas públicas usa una VPN. Las redes inalámbricas públicas son muy peligrosas y es la manera más fácil de ser víctima de delincuentes informáticos.
- h. Si realizas cualquier transacción financiera es posible que tu banco te bloquee si usas una VPN, por lo que recomendamos mantener la VPN desactivada cuando vayas a hacer alguna transacción financiera.
- i. Es importante ser precavidos al usar VPN gratuitas. Son buenas para ver contenidos bloqueados pero no es recomendable usarlas para transacciones bancarias o en sitios donde debas revelar datos confidenciales o sensibles como números de tarjetas de crédito.

2. Aplicaciones para saltar el bloqueo comunicacional en la Web.

Luego de instalar y probar la mayoría de las aplicaciones de software que se ofrecen y promueven en Internet para saltar el bloqueo de sitios web y plataformas tecnológicas sociales, nos permitimos mostrar a continuación, las opciones más recomendadas, tanto para PCs como para móviles, e indicar el correspondiente lugar de encuentro y las ayudas publicadas por los autores u organizaciones que las promueven.

2.1 Aplicaciones para PC

Aplicación	URL Oficial	Manual Instalación	Ayuda y Soporte Técnico
 Kproxy	https://kproxy.com/	1. Kproxy	https://kproxy.com/help.html
 Opera	https://www.opera.com/es-419/	2. Opera	https://www.opera.com/es/help
 Proton	https://protonvpn.com	3. Proton	https://protonvpn.com/support/ https://protonvpn.com/support/proton-vpn-setup-guide/
 Psiphon	https://www.psiphon3.com/es/index.html	4. Psiphon	https://psiphon3.com/es/user-guide.html
 Tor	https://www.torproject.org/es/	5. Tor	https://support.torproject.org/es/ https://2019.www.torproject.org/docs/documentation.html.en – Manuales – Guías de instalación – Tor Wiki – Preguntas frecuentes generales de Tor
 Windscribe	https://windscribe.com/	6. Windscribe	https://esp.windscribe.com/support https://esp.windscribe.com/guides

2.2 Aplicaciones para Dispositivos Móviles

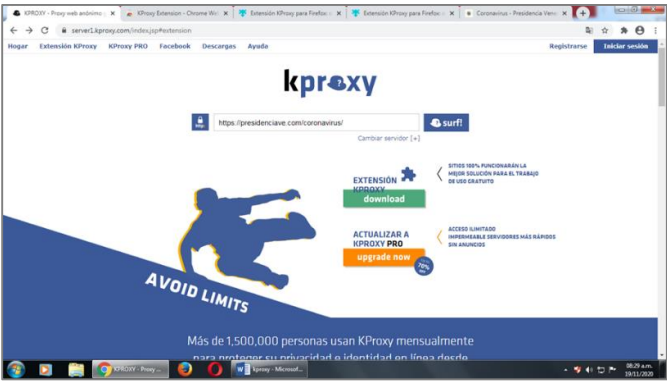
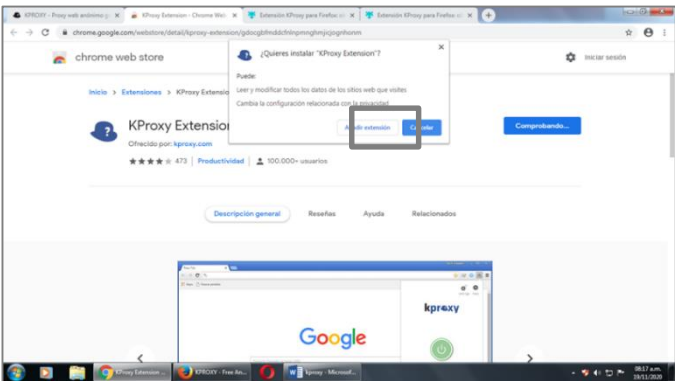
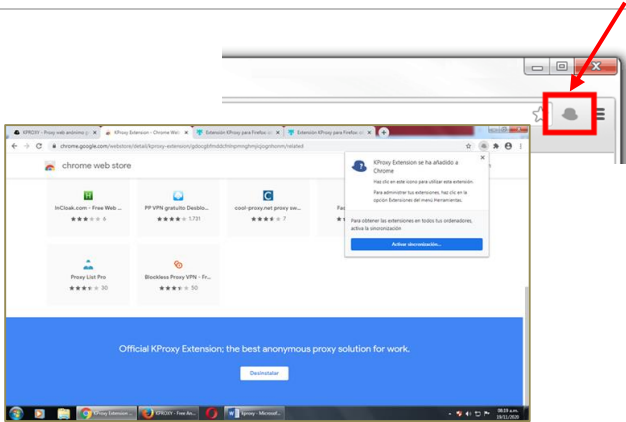
Aplicación	URL Oficial / Aplicación Play Store	Manual Instalación	Ayuda y Soporte Técnico
 Opera	https://www.opera.com/es-419/ https://play.google.com/store/apps/details?id=com.opera.browser	1. Opera	https://www.opera.com/es/help
 Proton	https://protonvpn.com https://play.google.com/store/apps/details?id=ch.protonvpn.android	2. Proton	https://protonvpn.com/support/how-to-install-the-protonvpn-apk/ https://protonvpn.com/support/protonvpn-setup-guide/ https://protonvpn.com/support/best-android-vpn-app/
 Tor	https://www.torproject.org/es/ https://play.google.com/store/apps/details?id=org.torproject.android	3. Tor	https://support.torproject.org/es/tor-mobile/
 Windscribe	https://windscribe.com/ https://play.google.com/store/apps/details?id=com.windscribe.vpn&hl=es	4. Windscribe	https://esp.windscribe.com/guides/manual_android
 Hide me	https://hide.me/es/ https://play.google.com/store/apps/details?id=hideme.android.vpn	5. Hide me	https://hide.me/es/vpnsetup/android/ https://hide.me/es/support
 Urban	https://www.urban-vpn.com/ https://play.google.com/store/apps/details?id=com.urbanvpn.android	6. Urban	https://www.urban-vpn.com/thank-you/ https://www.urban-vpn.com/es/
 Turbo	https://turbovpn.com/ https://play.google.com/store/apps/details?id=free.vpn.unlock.proxy.turbovpn	7. Turbo	https://turbovpn.co/faq

2.3 Instalando Aplicaciones para PCs.

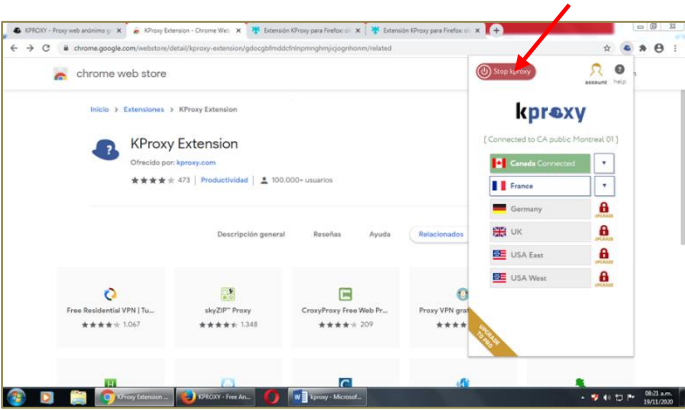
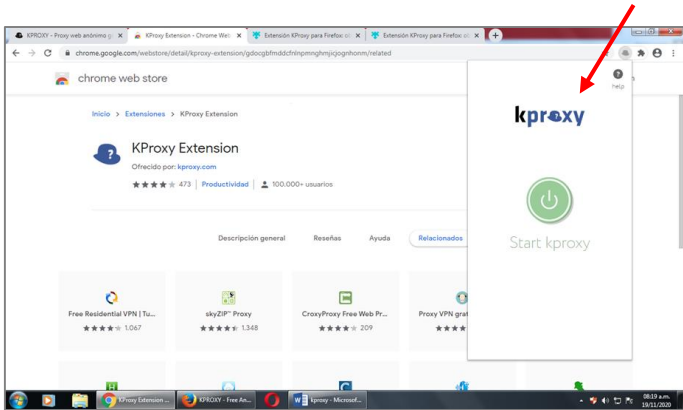
1. Kproxy

Esta herramienta puede ser instalada en Google Chrome o Firefox en forma de extensiones.

¿Cómo Instalar la extensión KProxy en Google Chrome?

1. Ingresa a la página oficial https://kproxy.com/ Aparecerá la pantalla inicial de Kproxy	2. Haz Click en el botón verde con letras blancas que dice download <i>Extension Kproxy</i> Aparece un recuadro que te pregunta si quieres instalar “Kproxy Extension”? Pulsa el botón blanco con letras azules <i>Añadir extensión</i>	3. Aparece un recuadro que te indica que ha sido añadida la extensión. Una vez instalada la extensión, encontrarás un nuevo botón en tu navegador Google Chrome, en la margen derecha.
		

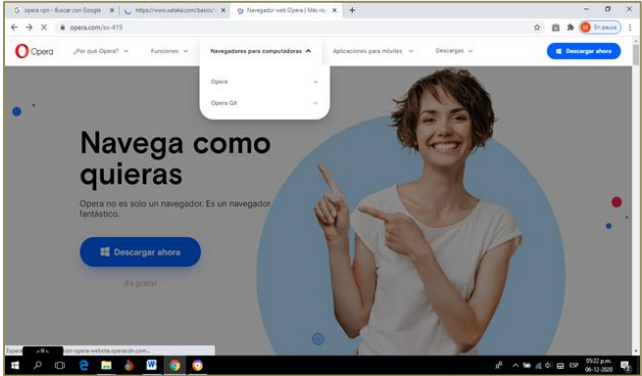
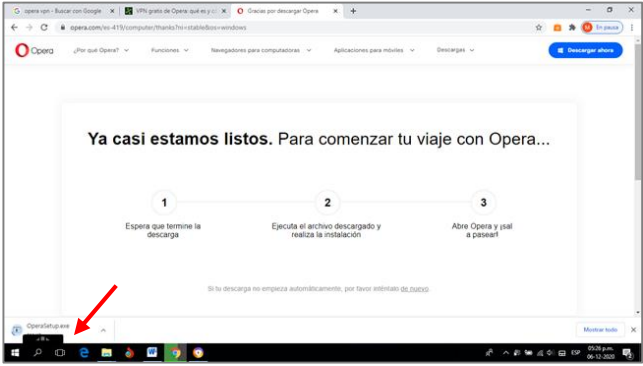
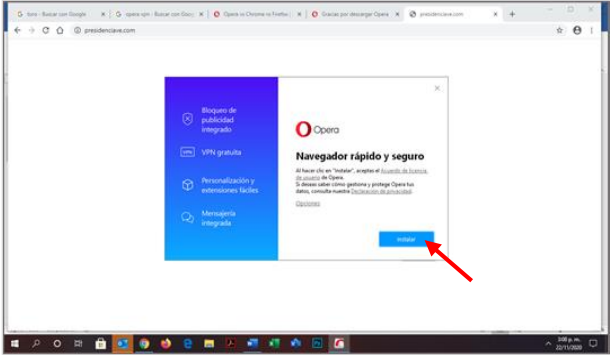
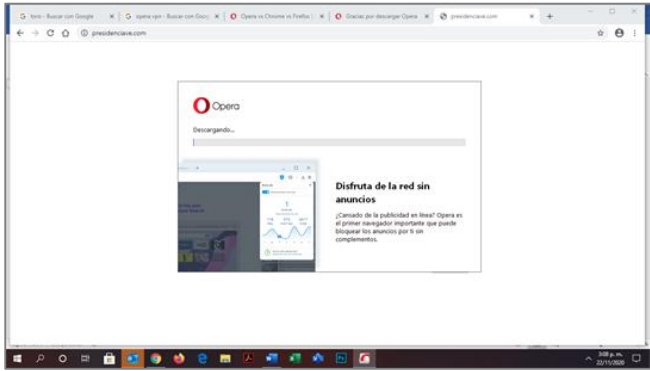
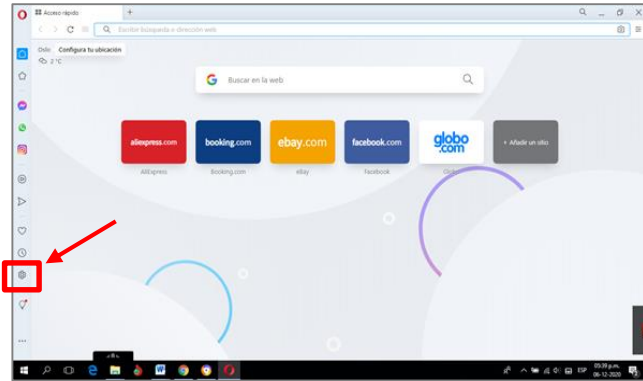
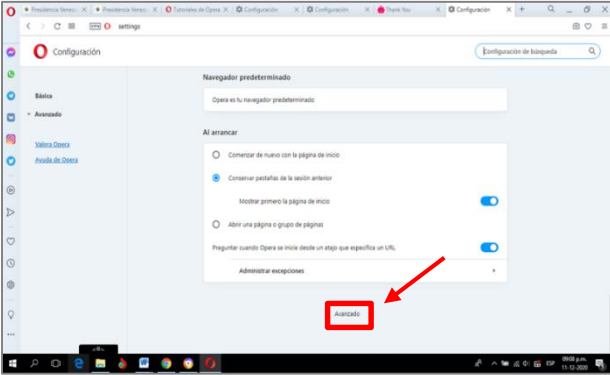
4. Al hacer Click en el ícono de Kproxy Extensión, se abre la ventana de inicio de la aplicación.
Se conectará automáticamente a tu servidor más cercano, y podrás ya navegar protegido.
Puedes verificar tu nueva dirección IP y ubicación <https://www.myip.com/> u otra aplicación de tu preferencia.
5. Observa que estás conectado a la **ubicación en verde**.
Puedes cambiar tu ubicación seleccionando cualquier otra.
Pulsa el botón rojo *Stop kproxy* al terminar de navegar y podrás activarla de nuevo cuando así lo desees
6. Aparece un recuadro que te indica que ha sido añadida la extensión.
Una vez instalada la extensión, encontrarás un nuevo botón en tu navegador Google Chrome, en la margen derecha.



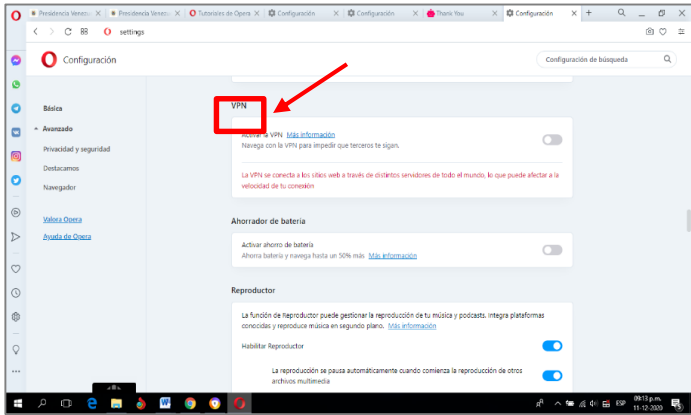
Podrás encontrar Ayuda para la extensión en <https://kproxy.com/help.html>

2. Opera

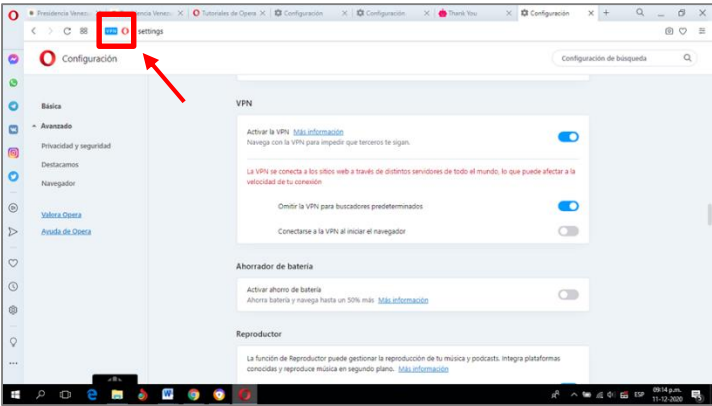
¿Cómo instalar Opera en Google Chrome?

1. Ingresa a la página oficial https://www.opera.com/es-419. Aparecerá la pantalla inicial de Opera. Pulsa el botón azul con letras blancas que dice <i>Descargar Ahora</i>	2. Comienza a descargar la aplicación.	3. Una vez descargada Opera, pulsa el botón <i>Ejecutar</i>.
		
4. Pulsa el botón azul para <i>Instalar</i> la aplicación	5. Esto te tomará unos minutos hasta que te aparece la siguiente pantalla. En el menú de la barra lateral seleccionas el ícono de <i>Configuración</i>	6. En la siguiente pantalla avanzas hasta el final y pulsa sobre la palabra <i>Avanzado</i>
		

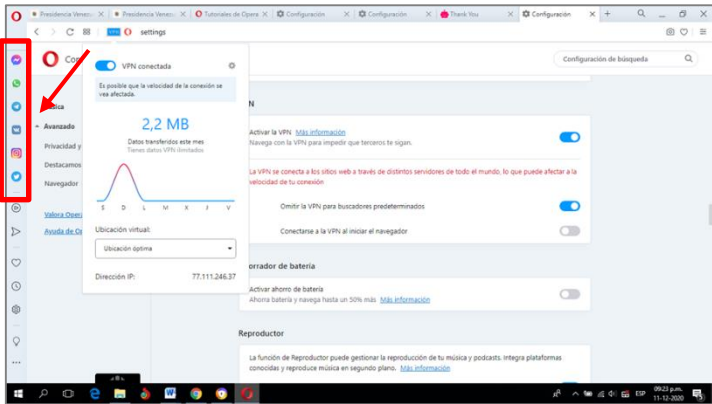
7. Aparece una nueva pantalla en la que buscas la palabra **VPN** y luego le das a **Activar la VPN**.



8. En la parte superior izquierda, al lado de la barra de direcciones, aparecerá un botón que dice **VPN** que te indica que ya estas conectado.



9. Ya puedes navegar con Seguridad. En la barra lateral aparecen los íconos de las distintas redes sociales.



Podrás encontrar Ayuda y Asistencia Técnica en <https://www.opera.com/es/help>

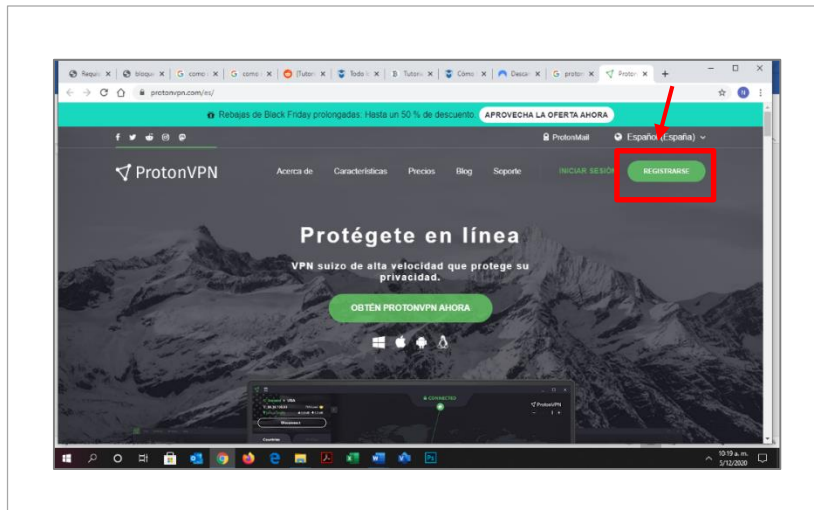
3. Proton

¿Cómo instalar ProtonVPN?

Ingresa a la página oficial <https://protonvpn.com>

Aparecerá la pantalla inicial de **Proton** donde debes registrarte con una cuenta de correo electrónico.

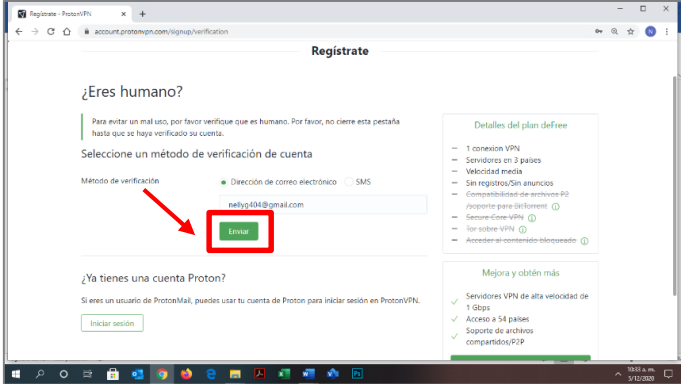
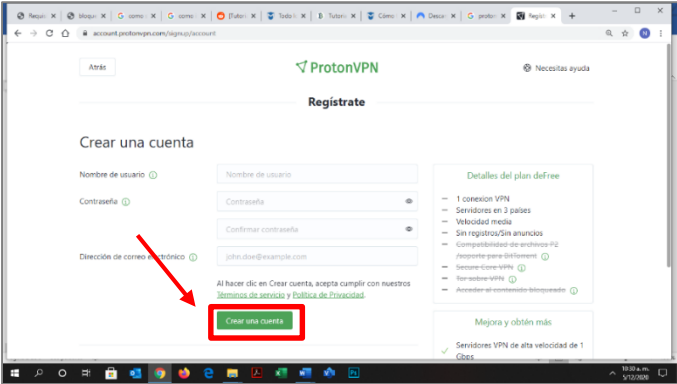
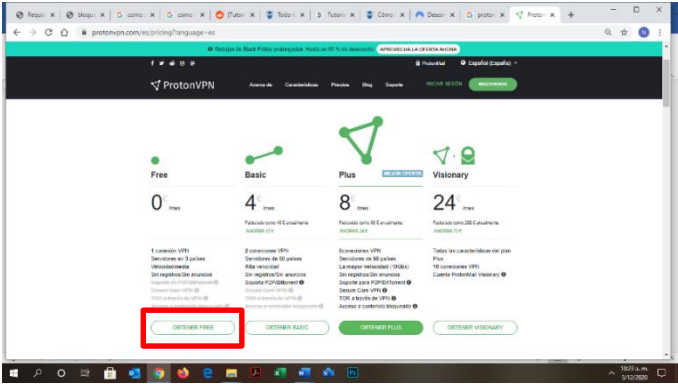
Pulsa sobre el botón verde con letras blancas que dice Registrarse.



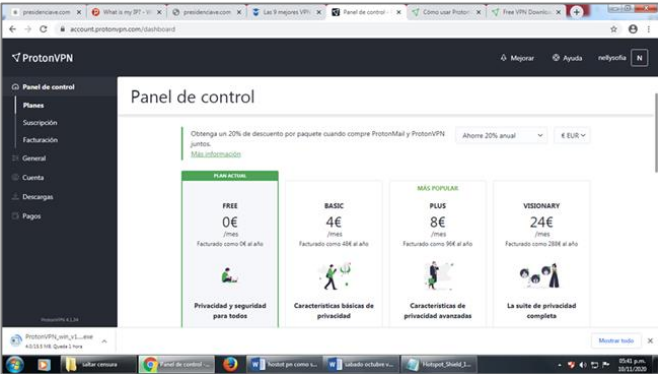
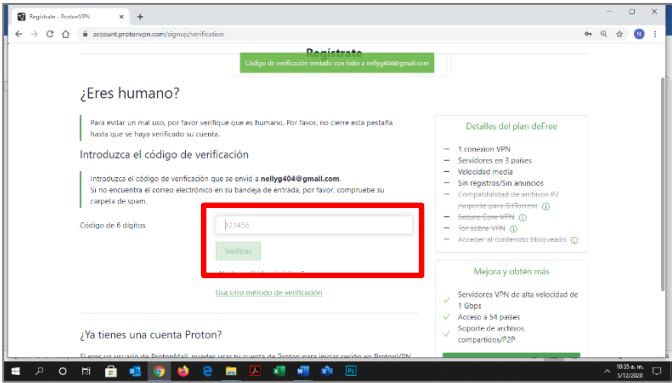
Ahora deberás registrarte en ProtonVPN, para luego poder proceder a la instalación y configuración de la aplicación.

A. ¿Cómo Registrarte en ProtonVPN?

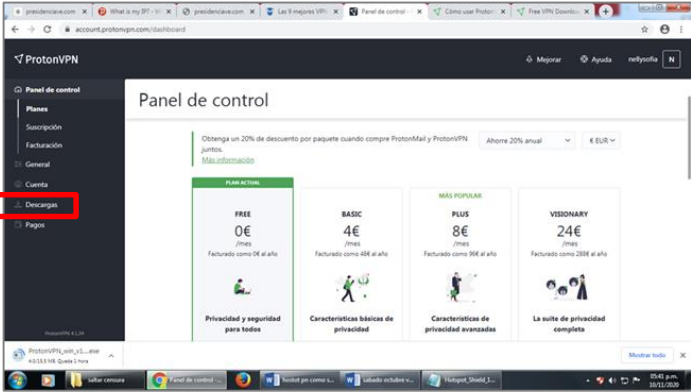
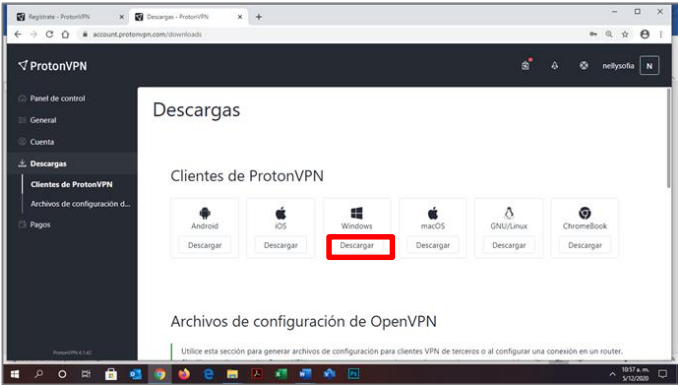
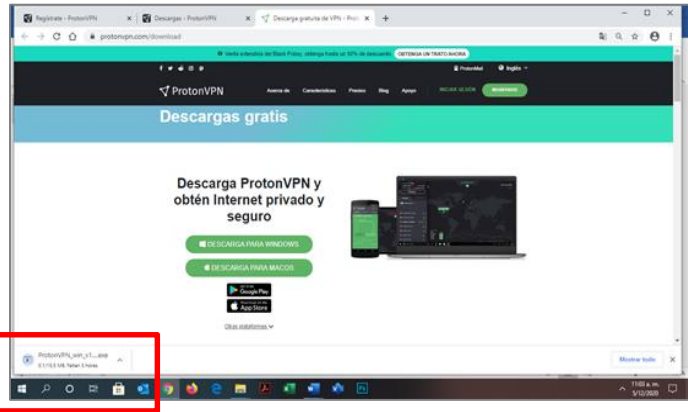
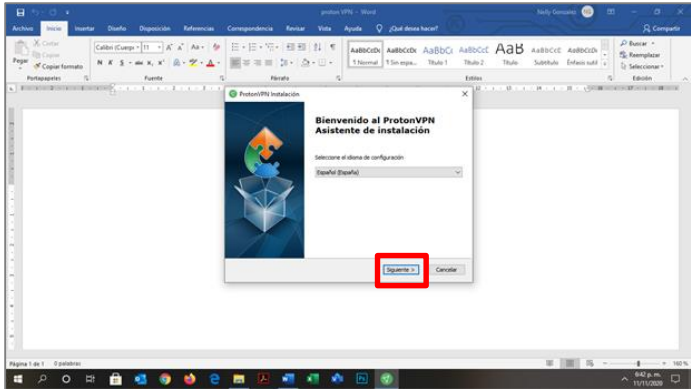
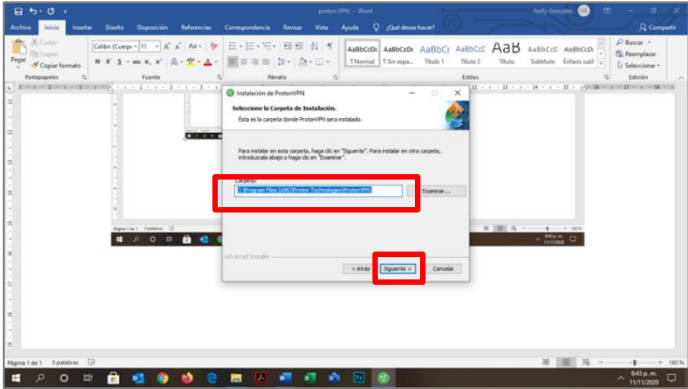
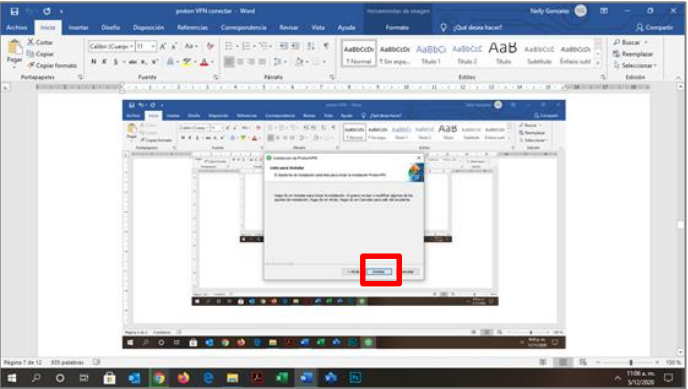
1. Para seleccionar el plan gratuito, en la siguiente pantalla, pulsa sobre el botón blanco con las letras verdes que dice *Obtener Free*.
2. A continuación, debes registrarte introduciendo los datos que te solicitan: Nombre de usuario, Contraseña, Confirmar Contraseña, Dirección de correo electrónico.
3. Pulsa sobre el botón verde *Crear una cuenta*
4. Aparece una nueva ventana. Pulsa sobre el botón *Enviar* y recibirás el código de verificación a través de la cuenta de correo electrónico con el que te has registrado.



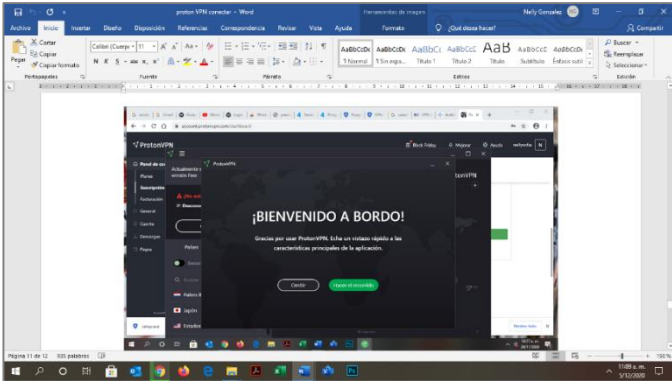
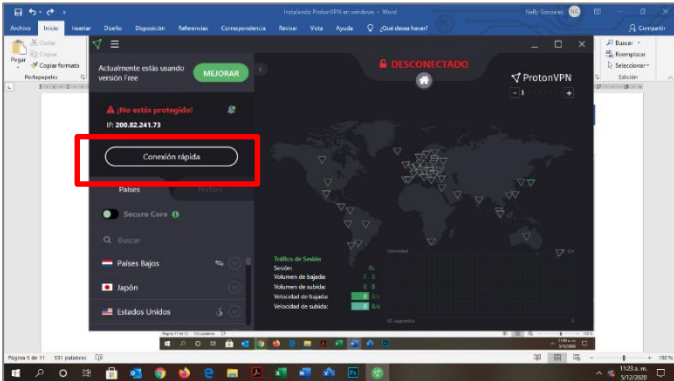
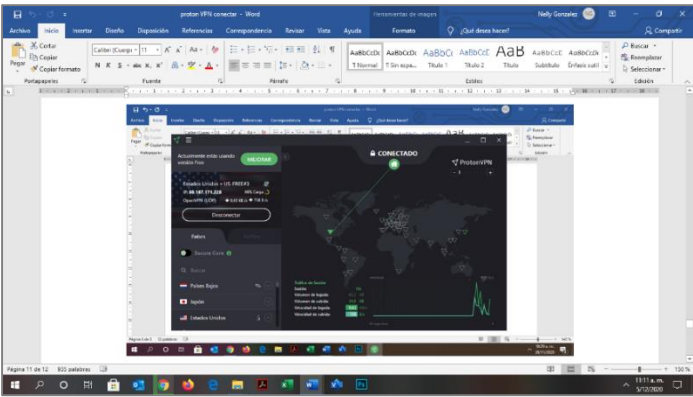
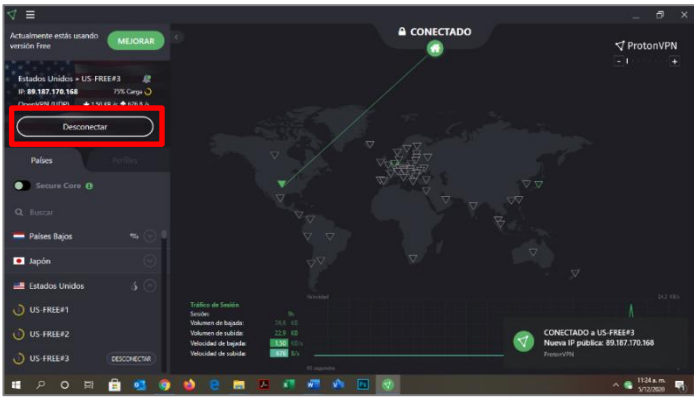
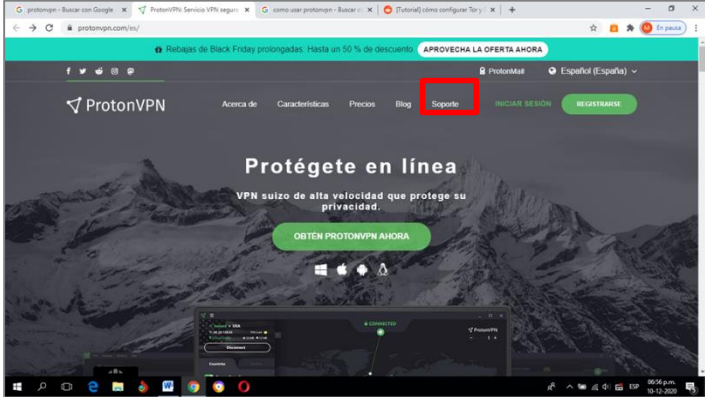
5. Introduce el código de verificación en el espacio en blanco y pulsa sobre *Verificar*.
6. Si el proceso de registro ha sido correcto aparecerá tu Panel de Control de usuario de ProtonVPN.



B. ¿Cómo Instalar ProtonVPN?

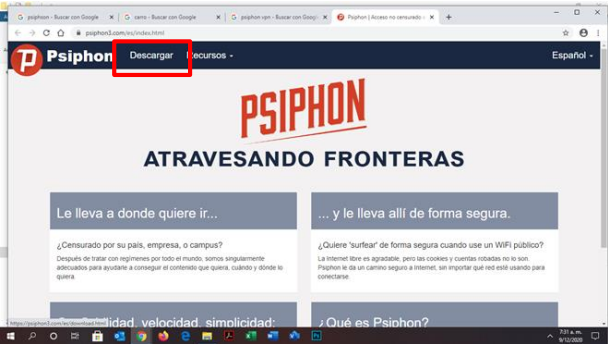
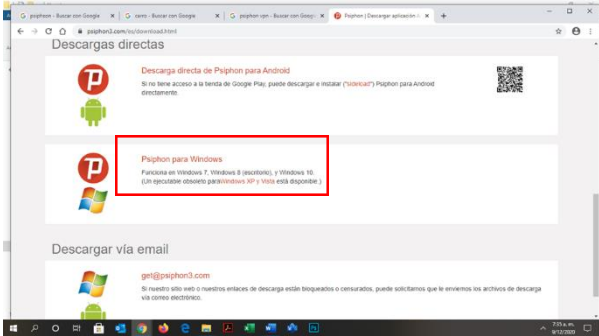
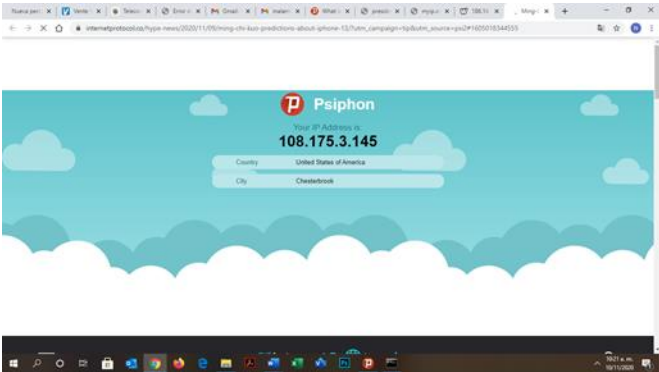
1. En el panel de control selecciona el plan gratuito, y luego en el menú de la izquierda pulsa la palabra <i>Descarga</i>.	2. Selecciona el Cliente VPN correspondiente a tu sistema operativo. Para este caso trabajaremos con Windows. Pulsa en el botón <i>Descargar</i>.	3. Si utilizas Windows y Chrome, pulsa sobre el <i>instalador</i> descargado en la esquina inferior izquierda. De lo contrario lo tendrás en la carpeta de Descargas.
		
4. Ejecutar. Ya estás en el ProtonVPN Asistente de Instalación. Selecciona el idioma de configuración y pulsa en <i>Siguiente</i>. Comenzará la instalación.	5. En la siguiente ventana te aparece la ruta de instalación, vuelve a pulsar sobre <i>Siguiente</i> o cambia la ruta a la carpeta que prefieras.	6. Pulsa sobre el botón <i>Instalar</i>. La instalación tardará uno segundos. Cuando la instalación haya finalizado, pulsa sobre el botón <i>Finalizar</i>.
		

C. ¿Cómo Configurar el Cliente ProtonVPN?

1. El cliente se abre automáticamente cuando finaliza la instalación. Introduce tu usuario y contraseña y pulsa sobre el botón verde para <i>Iniciar</i> sesión	2. Puedes seguir el tutorial de bienvenida para ver las funciones básicas y de pago.	3. Pulsa sobre el botón <i>Conexión Rápida</i> que aparece en la parte superior izquierda para conectarte al servidor gratuito que te da la mayor velocidad.
		
4. En este momento tu conexión a internet es privada. En la parte superior izquierda aparecerá el país de la VPN al que estás conectado. En el mapa central aparecerá la situación del servidor al que estás conectado.	5. Puedes verificar tu cambio de dirección IP https://www.myip.com/ en esta página o cualquier otra de tu preferencia. Cuando desees salir pulsa sobre la palabra <i>Desconectar</i>.	<i>Podrás encontrar Ayuda y Asistencia Técnica en https://protonvpn.com/support/ y en https://protonvpn.com/support/protonvpn-setup-guide/</i>
		

4. Psiphon

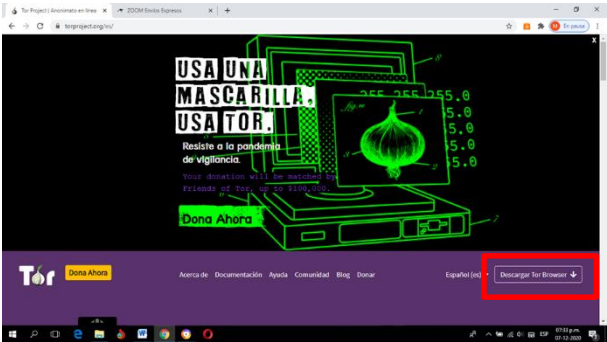
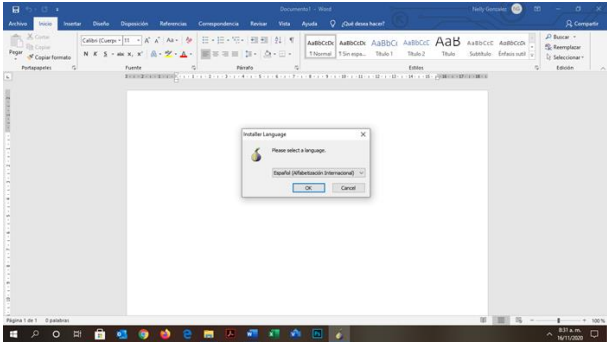
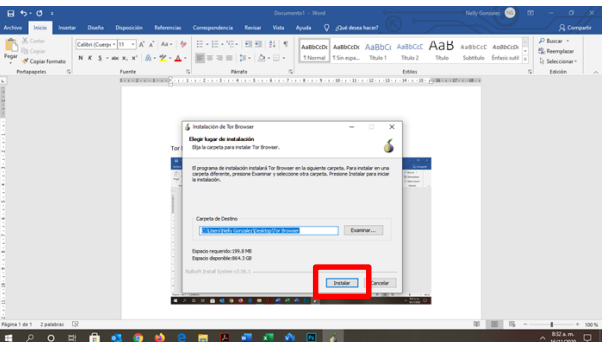
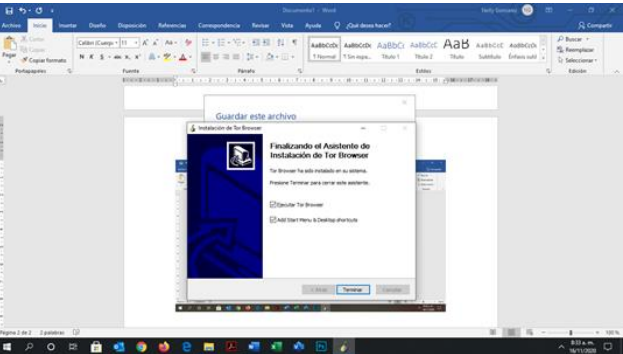
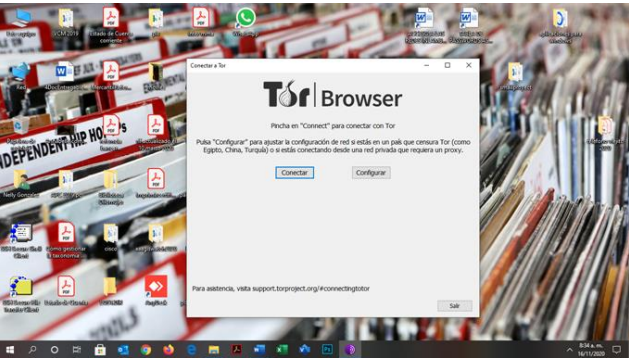
¿Cómo instalar Psiphon?

1. Ingresa a la página oficial https://psiphon3.com/es/indexhtml. Aparecerá la pantalla inicial de Psiphon. Pulsa el botón de <i>Descarga</i>.	2. Aparecen las distintas aplicaciones según el sistema operativo. Selecciona <i>Psiphon para Windows</i>.	3. Una vez descargada, se ejecuta. Aparece la siguiente página y ya está conectado automáticamente.
		
4. Al ejecutar Pishon3 conecta a un servidor. Puedes cambiarlo. Muestra tu ubicación y tu dirección IP	5. En <i>Registro de Logs</i>, puedes ver el registro de los pasos cronológicamente para conectarse.	6. En <i>Configuración</i>, puedes especificar parámetros de utilidad.
		

Podrás encontrar Ayuda y Asistencia Técnica en *Cómo usar Psiphon* en <https://psiphon3.com/es/user-guide.html>

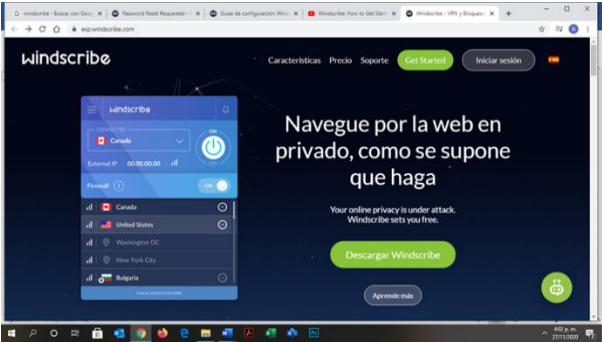
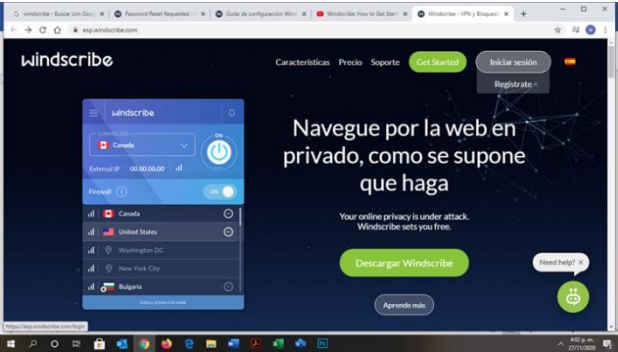
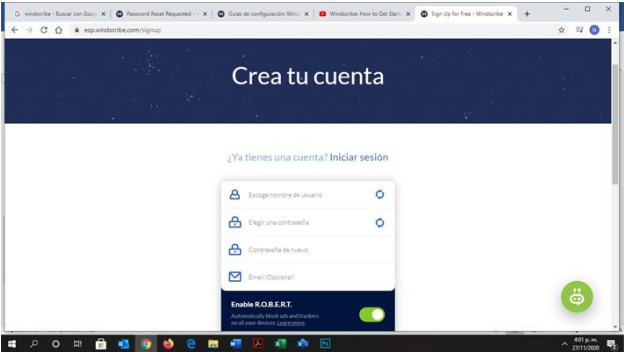
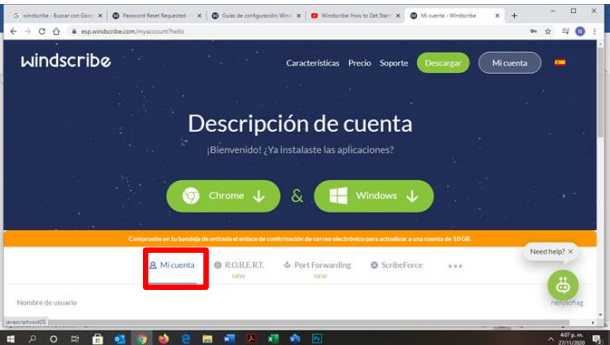
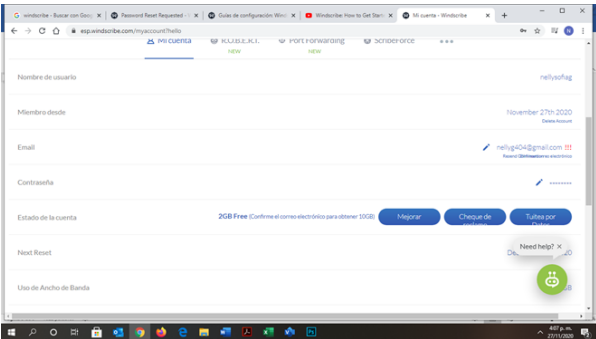
5. Tor

¿Cómo instalar Tor?

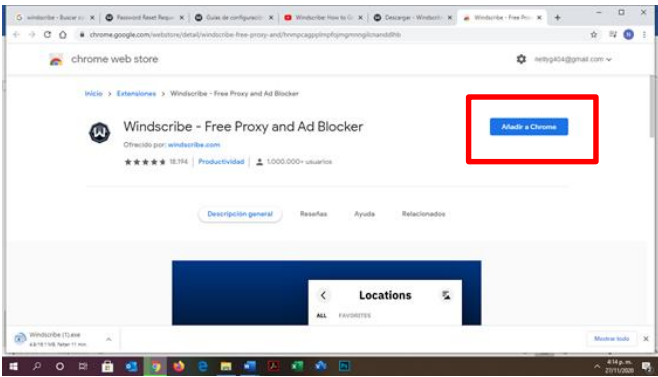
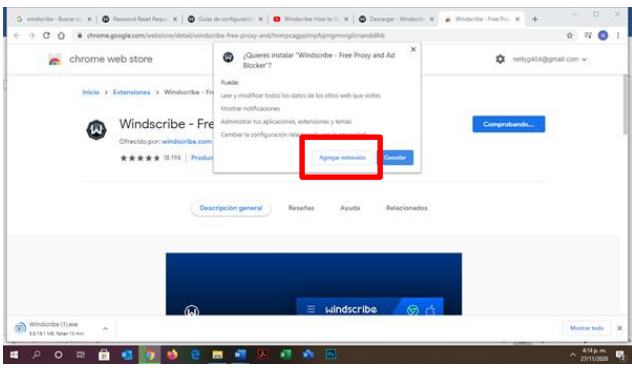
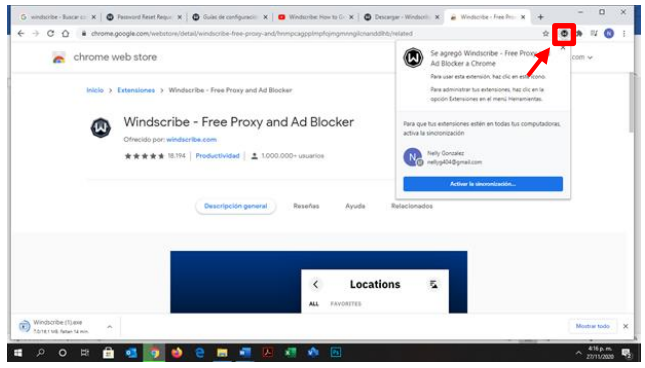
1. Ingresa a la página oficial https://www.torproject.org/es/download y pulsa <i>Descargar Tor Browser</i>.	2. Una vez descargada, se ejecuta. Completa el proceso del asistente de instalación. Selecciona el lenguaje a usar.	3. Elige el lugar de instalación y pulsa <i>Instalar</i>.
		
4. Para culminar la instalación pulsa <i>Terminar</i>. El Navegador Tor se iniciará de inmediato y los accesos directos de <i>Iniciar Navegador Tor</i> se agregarán al Menú Inicio y al Escritorio.	5. Si pulsas el botón <i>Conectar</i>, te conectarás a la red Tor sin configuración adicional. Te aparecerá una barra de estado mostrando el progreso de la conexión de Tor. Ahora puedes navegar en forma protegida.	<i>Podrás encontrar Ayuda y Asistencia Técnica en https://2019.www.torproject.org/docs/documentation.html</i> En la página principal aparece una ayuda para los nuevos en Tor en la parte superior izquierda.
		

6. Windscribe

A. ¿Cómo Registrarte en Windscribe?

1. Ingresa a la página oficial. https://windscribe.com/. Aparecerá la pantalla inicial de Windscribe. Antes de descargar la aplicación, debes registrarte. Pulsa el botón gris que dice <i>Iniciar Sesión</i>	2. Aparece la opción para registrarse. Pulsa el botón <i>Regístrate</i>, para crear tú cuenta.	3. Crea tu cuenta. Te pedirá un usuario y una contraseña. Luego confirma la contraseña y una dirección de correo opcional (si no lo pones no podrás recuperar o cambiar contraseña; solo tendrás 2gb para navegar por mes)
		
4. Al crear la cuenta aparece la siguiente pantalla. Selecciona <i>Mi Cuenta</i>.	5. Aparecerá información referente a la cuenta. Te llegará un correo electrónico para confirmar tú correo y obtener 10GB. Selecciona <i>Confirmar</i>, y te llevará a una página que dirá: <i>Email Confirmado</i>.	
		Estas registrado. Ahora podrás descargar la aplicación e instalarla.

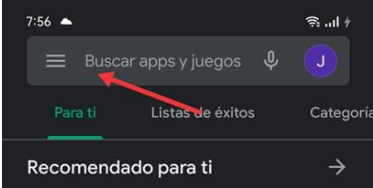
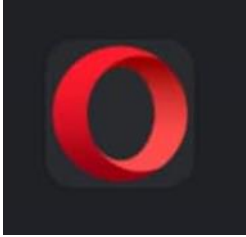
B. ¿Cómo Instalar Windscribe?

1. En la página principal pulsa la palabra <i>Descarga</i>. Aparecen las opciones de descarga para Chrome y para Windows.	2. Selecciona <i>Chrome</i>.	3. Aparece la siguiente pantalla donde debes escoger <i>Añadir Chrome</i>.
		
4. Seleccionas <i>Agregar Extensión</i>.	5. Aparece la siguiente pantalla, y para usar la extensión se debe hacer clic en el icono señalado en el margen superior derecho.	
		Estas conectado en modo protegido. Puedes navegar sin problemas.

2.4 Instalando Aplicaciones para Dispositivos Móviles.

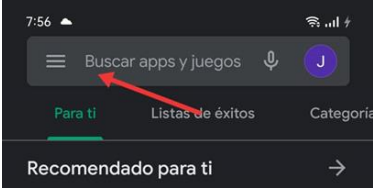
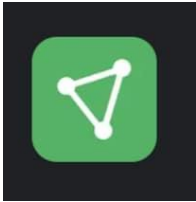
1. Opera

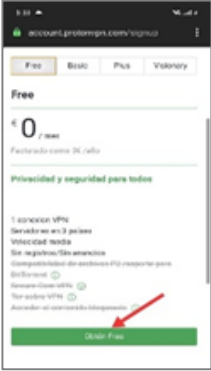
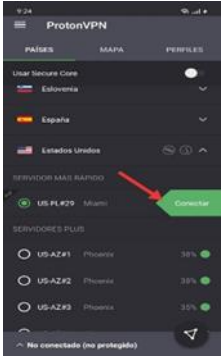
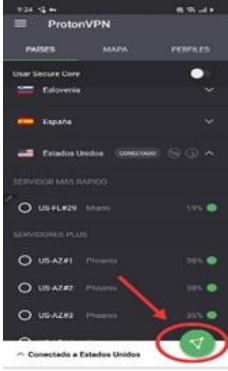
¿Cómo instalar Opera?

1. Abrir la aplicación <i>Play Store</i> en tu dispositivo Android buscar Opera .	2. Pulsa el botón verde <i>Instalar</i>	3. Abrir y Navegar sin ningún tipo de configuración, registros ni bloqueos.
		
Podrás encontrar <i>Ayuda y Asistencia Técnica</i> en https://www.opera.com/es/help y https://help.opera.com/es/mobile/android/		

2. Proton

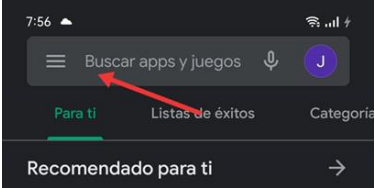
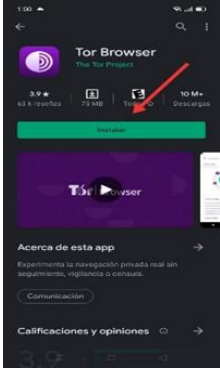
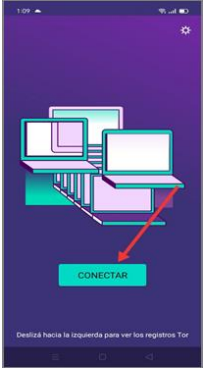
¿Cómo instalar Proton?

1. Abrir la aplicación <i>Play Store</i> en tu dispositivo Android buscar Proton .	2. Pulsa botón verde <i>Instalar</i>	3. Pulsa sobre el ícono de <i>Proton</i> para abrir la aplicación.
		
4. Pulsa el botón <i>Siguiente</i> hasta llegar a la ventana en que te solicita Registrarte	5. Pulsa el botón <i>Registrarse</i>	6. Selecciona el plan gratuito al pulsar la palabra <i>Free</i> .
		

7. Ahora selecciona <i>Obten Free</i> .	8. Completa los datos que te son solicitados, y pulsa el botón <i>Crear Cuenta</i> .	9. Para conectarte pulsa el botón verde Conectar. Puedes hacerlo seleccionando el país de tu preferencia.
		
10. Para desconectarte, pulsa el botón verde con el ícono de Proton.	<i>Podrás encontrar Ayuda y Asistencia Técnica en:</i> Cómo instalar el APK de ProtonVPN https://protonvpn.com/support/how-to-install-the-protonvpn-apk/ Guía de configuración para nuevos usuarios https://protonvpn.com/support/protonvpn-setup-guide/ Aplicación VPN ProtonVPN para Android https://protonvpn.com/support/best-android-vpn-app/	
		

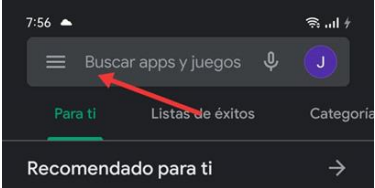
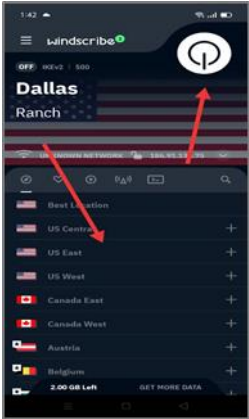
3. Tor

¿Cómo instalar Tor?

1. Abrir la aplicación <i>Play Store</i> en tu dispositivo Android buscar <i>Tor</i> .	2. Pulsa botón verde <i>Instalar</i>	3. Abre la aplicación y pulsa en <i>Conectar</i> . Espera la <i>carga</i> de parámetros para navegar sin configuraciones adicionales, registros, ni bloqueos.
		
<i>Podrás encontrar Ayuda y Asistencia Técnica en</i> https://support.torproject.org/es/tormobile/		

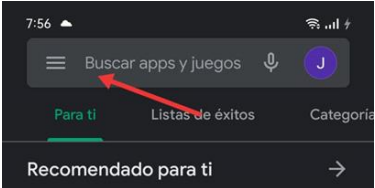
4. Windscribe

¿Cómo instalar Windscribe?

1. Abrir la aplicación <i>Play Store</i> en tu dispositivo Android buscar Windscribe .	2. Pulsa botón verde <i>Instalar</i>	3. Crea un usuario e ingresa tú correo electrónico para la asignación del plan de navegación.
		
4. Selecciona de la lista el servidor de tú preferencia y pulsa en el botón de <i>Encendido</i> para conectarte a la red.	Podrás encontrar Ayuda y Asistencia Técnica en https://esp.windscribe.com/guides/manual_android	
		

5. Hide Me VPN

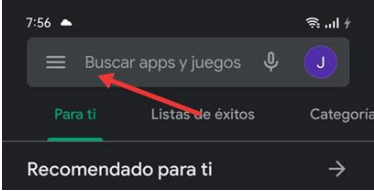
¿Cómo Instalar Hide Me VPN?

1. Abrir la aplicación <i>Play Store</i> en tu dispositivo Android buscar Hide Me .	2. Pulsa botón verde <i>Instalar</i>	3. Selecciona <i>Get Your Free Play</i> .
		

4. Pulsa el botón blanco <i>Activate</i> .	5. Para habilitar la red, selecciona el botón <i>Enable VPN</i>	6. Ahora selecciona <i>Connect to VPN</i> .
		
7. Para poder iniciar hay que aceptar los términos de privacidad. Pulsa donde dice <i>Permitir Siempre</i> .	8. Ya estás conectado a Hide.me VPN . Para desconectarte sólo debes pulsar en <i>Desable VPN</i> .	<i>Podrás encontrar Ayuda y Asistencia Técnica en</i> https://hide.me/es/vpnsetup/android/ https://hide.me/es/support
		

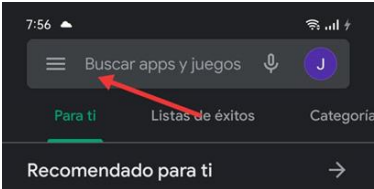
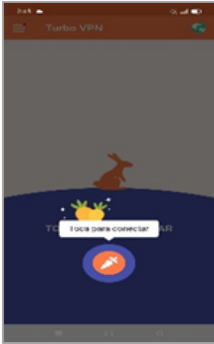
6. Urban

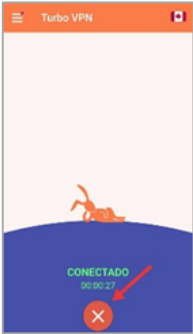
¿Cómo Instalar Urban?

1. Abrir la aplicación <i>Play Store</i> en tu dispositivo Android buscar Urban .	2. Pulsa botón verde <i>Instalar</i>	3. Abrir la aplicación y selecciona el modo gratuito.
		

4. Selecciona <i>Accept</i> para estar de acuerdo con la licencia de Usuario de Urban .	5. Selecciona la ubicación de tú preferencia y luego pulsa el botón <i>Play</i> .	6. Si deseas desconectarte, pulsa el botón de <i>Pausa</i> .
		
<i>Podrás encontrar Ayuda y Asistencia Técnica en</i> https://www.urban-vpn.com/thank-you/ ¿Cómo se instala? https://www.urban-vpn.com/es/ Información general de la aplicación		

7. Turbo
¿Cómo Instalar Turbo?

1. Abrir la aplicación <i>Play Store</i> en tu dispositivo Android buscar Turbo .	2. Pulsa botón verde <i>Instalar</i>	3. Pulsa el botón naranja para <i>Empezar Ahora</i> .
		
4. Para cerrar el anuncio de pago, pulsa sobre la <i>X</i> .	5. Pulsa en el ícono de la <i>zanahoria</i> para conectarte.	6. Luego acepta los términos de privacidad.
		

7. Para seleccionar el país de tu preferencia, pulsa sobre el ícono del <i>mapamundi</i> .	8. Pulsa ícono de la X para desconectarte.	<i>Podrás encontrar Ayuda y Asistencia Técnica en:</i> https://turbovpn.co/faq
		

3. Patrocinadores

Proyecto subvencionado por Swedish International Cooperation Agency (Sida), gestionado por la Asociación para el Progreso de las Comunicaciones (APC), y desarrollado por la Fundación Escuela Latinoamericana de Redes – Venezuela.

