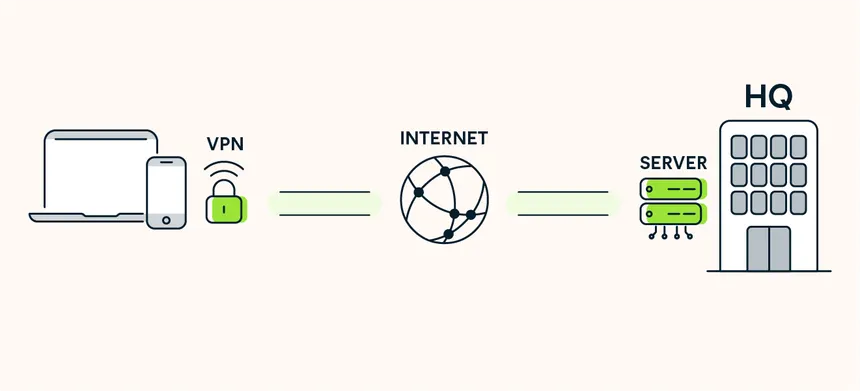
**2.-Realiza un trabajo de investigación sobre las redes privadas virtuales que incluya la siguiente información:**

1. **Información general sobre el funcionamiento de las redes privadas virtuales.**
2. **Clasificación de las VPN: según la tecnología del operador, según el nivel OSI, según la topología.**
3. **Modos de conexión mediante VPN.**
4. **VPN a nivel de red: IPSec.**
5. **VPN a nivel de transporte: SSL.**
6. **VPN a nivel de aplicación: SSH.**

**Que es una red privada virtual (VPN)**

Una VPN o red privada virtual crea una conexión de red privada entre dispositivos a través de Internet. Las VPN se utilizan para transmitir datos de forma segura y anónima a través de redes públicas. Su funcionamiento consiste en ocultar las direcciones IP de los usuarios y cifrar los datos para que nadie que no esté autorizado a recibirlos pueda leerlos.



**¿Para qué sirve una VPN?**

Los servicios de VPN se utilizan principalmente para enviar datos de forma segura a través de Internet. Las tres funciones principales de las VPN son:

# **Privacidad**

Sin una red privada virtual (VPN), tus datos personales, como contraseñas e información financiera, pueden ser accesibles y vendidos a terceros. Las VPN protegen esta información mediante cifrado, especialmente al conectarse a redes wifi públicas.

# **Anonimato**

Su dirección IP contiene información sobre su ubicación y su actividad de navegación. Todos los sitios web de Internet rastrean estos datos por medio de las cookies y otras tecnologías similares. Pueden identificarlo cada vez que los visite. Una conexión VPN oculta su dirección IP para que permanezca en el anonimato en Internet.

# **Seguridad**

Las VPN utilizan la criptografía para proteger su conexión a Internet de accesos no autorizados. También puede actuar como mecanismo de cierre, al finalizar programas preseleccionados en caso de actividad sospechosa en Internet. Esto disminuye la probabilidad de que los datos se vean comprometidos. Estas características permiten a las empresas dar acceso remoto a los usuarios autorizados a través de sus redes empresariales.

**Funcionamiento de una VPN**

Una conexión VPN redirige los paquetes de datos de su máquina a otro servidor remoto antes de enviarlos a terceros a través de Internet. Las principales características de la tecnología VPN son las siguientes:

# **Protocolo de túnel**

Una red privada virtual crea un túnel de datos seguro entre su máquina local y otro servidor VPN situado a miles de kilómetros. Cuando se conecta, este servidor VPN se convierte en el origen de todos sus datos. Su proveedor de servicios de Internet (ISP) y otros terceros ya no pueden ver el contenido de su tráfico de Internet.

# **Cifrado**

Los protocolos VPN como IPSec cifran los datos antes de enviarlos a través del túnel, protegiendo las comunicaciones mediante autenticación y cifrado de los paquetes IP. Esto hace que los datos sean ilegibles durante el tránsito y solo puedan ser decodificados al llegar al destino, evitando el uso indebido de información personal y asegurando la conexión a Internet.



**Clasificación de una VPN**

Las redes privadas virtuales (VPN) pueden clasificarse de varias maneras, incluyendo según la tecnología del operador, el nivel del protocolo OSI y la topología. Aquí te presento una clasificación según estos criterios:

# **Según la tecnología del operador:**

Las VPN pueden clasificarse según el tipo de tecnología que utiliza el operador para proporcionar el servicio. Esto incluye protocolos como OpenVPN, IKEv2, L2TP, PPTP, Wire Guard y SSTP. Cada protocolo tiene sus propias características y niveles de seguridad

# **Según el nivel del protocolo OSI:**

Las VPN pueden clasificarse según el nivel del protocolo OSI en el que operan. Por ejemplo, una VPN de capa 2 opera en la capa de enlace de datos, mientras que una VPN de capa 3 opera en la capa de red. La capa 2 requiere que los clientes configuren sus propios enrutadores para transportar todo el tráfico de capa 3, mientras que la capa 3 maneja el enrutamiento en los enrutadores del proveedor de servicios

# **Según la topología:**

Las topologías de red utilizadas en las VPN pueden ser de tipo Cliente-Servidor o Full-Mesh. En la topología Cliente-Servidor, un servidor central interconecta el resto de las sedes, mientras que en la topología Full-Mesh, todos los nodos o sedes están conectados entre sí sin necesidad de un servidor central

**Modos de conexión de una VPN**

# **Teletrabajo**

El uso más común de una conexión VPN es permitir la interconexión de redes que no están físicamente conectadas, como en el caso de trabajadores fuera de la oficina o empresas con sucursales en diferentes ciudades que necesitan acceder a una única red privada.

Desde una perspectiva de seguridad, permitir el acceso directo a la red de una empresa desde Internet es riesgoso, incluso si está protegido por una contraseña, ya que esta puede ser capturada en una red WiFi pública o espiada por un atacante.

En cambio, cuando se utiliza una conexión VPN, el riesgo se reduce considerablemente. El acceso está protegido, la conexión se cifra y el trabajador puede acceder a la red de manera segura, como si estuviera en la oficina.

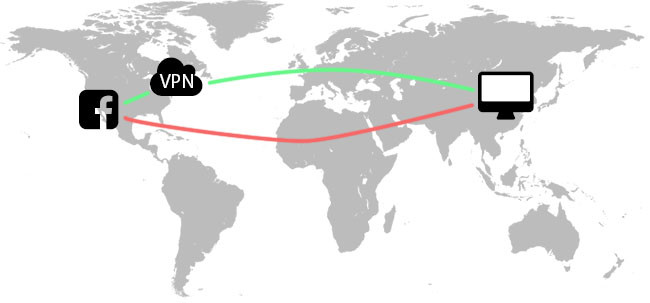


# **Evitar censura y bloqueos geográficos de contenido**

Con el apogeo de Internet y la picaresca tanto de los proveedores de contenidos como de los usuarios, se han ido popularizando otros usos más lúdicos de las conexiones VPN, muchos de ellos relacionados con un concepto muy sencillo: falsear dónde estás.

Al conectarte con VPN, tu dispositivo se comunica con el servidor VPN, y es éste el que habla con Internet. Si tú estás en China y el servidor VPN está en Estados Unidos, generalmente los servidores web creerán que estás navegando desde este país, dejándote acceder a los contenidos disponibles solo allí, como podría ser Netflix.

De igual modo, esta misma lógica se puede usar para acceder a aquellos contenidos que estuvieran censurados o bloqueados en tu país, pero no allí donde se encuentra el servidor VPN. Así es como millones de ciudadanos chinos logran conectarse a Facebook y otras 3.000 webs bloqueadas en el país.



# **Capa extra de seguridad**

Aunque no es estrictamente necesario, sí es común que las conexiones VPN vengan acompañadas de un cifrado de los paquetes que se transmiten con ellas, por lo que es normal oír la recomendación de que, si necesitas conectarte a un punto de acceso Wi-Fi público, al menos uses te conectes con una VPN.

Iniciar sesión en cuentas bancarias mientras usas una red WiFi pública no confiable es arriesgado, ya que un atacante puede capturar tus datos sin cifrar. Una conexión VPN cifra los paquetes, protegiendo tu información. Sin embargo, al confiar en la VPN, también dependes de su proveedor, que podría capturar tu tráfico, guardar registros o vender tu ancho de banda. Una VPN es tan segura como su proveedor, por lo que si no confías en él, es mejor no usarla, ya que podría ser un riesgo adicional.

# **Descargas P2P**

Otro uso común de las conexiones VPN se encuentra en las descargas P2P, lo cual en estos tiempos generalmente es sinónimo de descargar desde BitTorrent. Antes de que me pongas un parche en el ojo, una pata de palo y me obligues a pasar por la quilla, las conexiones VPN también tienen usos en la descarga P2P aunque bajes torrents completamente legales.

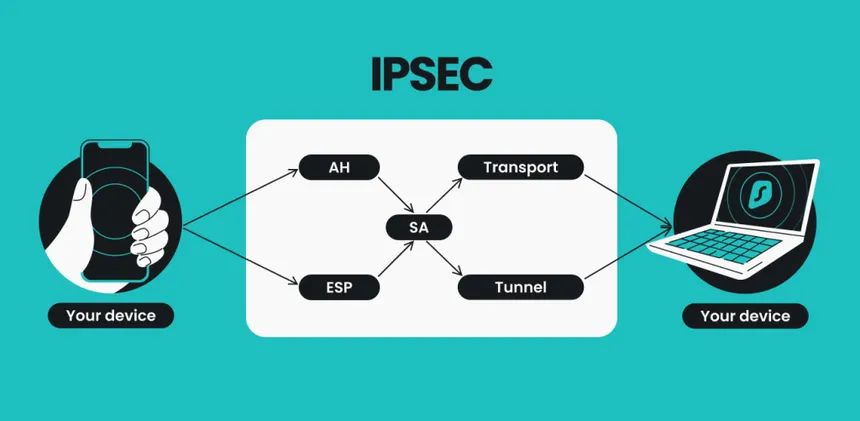
Desgraciadamente es cada vez común que los proveedores de Internet decidan meter las narices en cómo enviamos y recibimos los ceros y unos en la Red, y aunque les encanta que visitemos páginas web normales, que descarguemos no les hace tanta gracia: demasiado tráfico, y además probablemente te estás descargando algo ilegal.

Algunos proveedores bloquean por completo las descargas P2P, mientras que otros simplemente la boicotean para que funcione mal y te rindas por ti mismo. Igual que puedes usar una conexión VPN para evitar la censura de tu país, también puedes en ocasiones evitar que tu proveedor de Internet boicotee tus descargas P2P.

**VPN a nivel de red: IPSec**

# **¿Qué es IPSec?**

IPSec está compuesto por varios protocolos de seguridad diferentes y está diseñado para garantizar que los paquetes de datos enviados a través de una red IP permanezcan invisibles e inaccesibles para terceros. IPSec proporciona altos niveles de seguridad para el Protocolo de Internet. El cifrado se utiliza para garantizar la confidencialidad y para la autenticación.



# **¿Cómo Funciona IPSec Junto Con los Protocolos VPN?**

IPSec se usa junto con otros protocolos VPN para proporcionar un servicio rápido y seguro. Tenemos dos opciones principales:

1. **L2TP/IPSec**

L2TP es un protocolo de túnel comúnmente utilizado en sistemas operativos y dispositivos para VPN, pero por sí solo no ofrece cifrado. Al combinarse con IPSec, proporciona altas velocidades y una seguridad excepcional para los datos, utilizando cifrado AES.

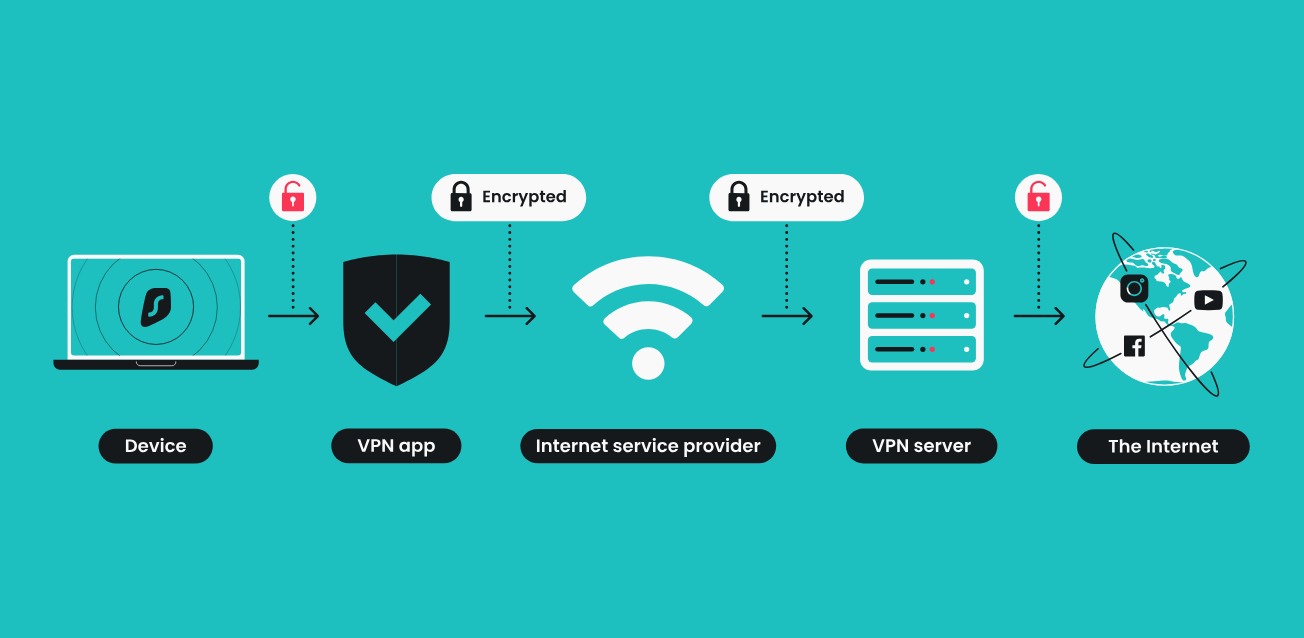
1. **IKEv2/IPSec**

IKEv2, desarrollado por Microsoft y Cisco, es compatible de forma nativa con Windows 7+, iOS y Blackberry, y tiene versiones de código abierto para Linux. Al combinarse con IPSec, es un protocolo de túnel eficaz para VPN. Destaca por su capacidad de respuesta y flexibilidad, ya que se reconecta automáticamente tras una breve pérdida de señal y, gracias al protocolo MOBILE, maneja cambios de red con facilidad.

**VPN a nivel de transporte: SSL**

# **¿Qué es una VPN SSL?**

La VPN SSL es una VPN que utiliza un protocolo de software particular, SSL. Para las empresas, este tipo de VPN permite a los usuarios remotos acceder de forma segura a una red corporativa utilizando un navegador web normal, sin tener que instalar aplicaciones especializadas en cada dispositivo.



# **Tipos de VPN SSL**

Con la ayuda de una VPN SSL, un usuario puede establecer conexiones seguras a servicios HTTP internos utilizando navegadores web estándar o aplicaciones cliente. Eso depende de cuál de las dos VPN SSL utilices: portal o túnel.

1. **VPN de portal SSL**

Una VPN de portal SSL, también conocida como VPN sin cliente o VPN basada en web, es un tipo de VPN SSL que ofrece acceso remoto a los recursos de red a través de un portal web. Permite a los usuarios acceder de forma segura a aplicaciones, archivos y otros recursos alojados en una red privada utilizando un navegador web estándar.

1. **VPN de túnel SSL**

Una VPN de túnel SSL, también llamada extensor de red SSL (SNX), es otro tipo de VPN SSL que establece un túnel cifrado seguro entre el dispositivo del usuario y la red privada. Permite acceder a los recursos de la red como si el dispositivo del usuario estuviera conectado directamente. Sin embargo, este tipo requiere un cliente VPN instalado en el ordenador del usuario.

**VPN a nivel de aplicación: SSH**

# **¿Qué es una VPN SSH?**

SSH es un protocolo utilizado principalmente para acceder de forma segura a sistemas remotos y ejecutar comandos en ellos. Aunque tradicionalmente no se utiliza como una VPN completa, SSH puede actuar como una VPN a nivel de aplicación, proporcionando un canal seguro entre un cliente y un servidor

# **Características de SSH**

* **Cifrado de extremo a extremo**: SSH cifra todas las comunicaciones entre el cliente y el servidor, protegiendo los datos de posibles interceptaciones.
* **Tunelización**: SSH permite crear túneles seguros, en los que se pueden redirigir puertos de red y acceder a aplicaciones o servicios como si estuvieran en la misma red local, incluso si se encuentran en diferentes ubicaciones.
* **Autenticación**: SSH puede requerir autenticación mediante contraseñas o claves públicas/privadas, lo que proporciona una capa adicional de seguridad.
* **Uso específico**: Mientras que las VPN tradicionales protegen todo el tráfico de red, SSH a nivel de aplicación generalmente se utiliza para asegurar conexiones específicas, como acceder a una base de datos remota o un servidor web.
* **Conexión segura**: Aunque no es una VPN completa, SSH permite a los usuarios conectarse a una red privada de forma segura, como si estuvieran físicamente presentes en la misma red, pero a nivel de aplicaciones y puertos específicos.

