

SAÚL RUIZ PLAZA

01

INTRODUCCIÓN A LAS VPNS





¿QUÉ ES UNA VPN?



Una VPN (Red Privada Virtual) es una tecnología que **crea una conexión segura y cifrada** entre tu dispositivo e Internet. Esto protege tus datos, oculta tu ubicación y te permite navegar con mayor privacidad, especialmente en redes públicas.



¿CÓMO FUNCIONA?



La VPN establece un "**túnel**" **cifrado** entre tu dispositivo y un servidor remoto:

1. **Cifrado**: La información se transforma en un formato ilegible para terceros.
2. **Redirección del tráfico**: El tráfico pasa por el servidor VPN, ocultando tu IP real.
3. **Acceso seguro**: Los datos se envían y reciben con protección contra ataques.

Ejemplo: Al conectarte desde una red Wi-Fi pública, la VPN **impide** que hackers intercepten tus datos personales.

USOS PRINCIPALES



- **Seguridad en Wi-Fi públicas:** Protege tus datos al conectarte a redes abiertas en cafeterías, aeropuertos o bibliotecas.
- **Privacidad en línea:** Oculta tu IP y previene el rastreo de anunciantes y terceros.
- **Acceso global:** Desbloquea contenido restringido geográficamente, como películas de Netflix en otros países.
- **Trabajo remoto seguro:** Conecta empleados a redes empresariales de forma segura.



BENEFICIOS



- **Privacidad mejorada:** La VPN oculta tu dirección IP real, protegiendo tu identidad en línea.
- **Seguridad:** Cifra tus comunicaciones, especialmente importante cuando utilizas redes Wi-Fi públicas.
- **Acceso a contenido restringido:** Te permite acceder a servicios y contenido bloqueados geográficamente (por ejemplo, Netflix o BBC).
- **Prevención de seguimiento:** Bloquea a los anunciantes y sitios web que intentan rastrear tu actividad.

TIPOS



- **VPN de acceso remoto:** Permite a los usuarios acceder a una red privada desde cualquier lugar. Ideal para trabajo remoto o acceso a servicios internos de una empresa.
- **VPN de sitio a sitio:** Utilizada para conectar dos redes físicas a través de Internet, como en el caso de las sucursales de una empresa.
- **VPN de acceso dedicado (MPLS):** Conecta oficinas y centros de datos sin pasar por Internet público, ofreciendo mayor seguridad.



PROTOSCOLOS

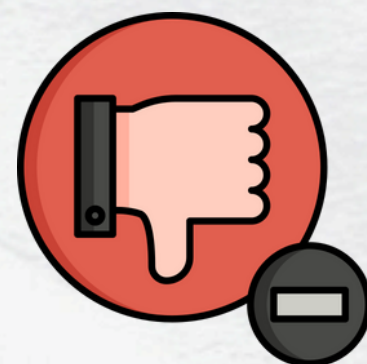
- **OpenVPN:** Abierto y altamente seguro. Es uno de los protocolos más utilizados.
- **IPsec:** Ofrece un alto nivel de seguridad y es ampliamente utilizado en redes privadas.
- **WireGuard:** Relativamente nuevo, conocido por su eficiencia y alto rendimiento.
- **PPTP:** Más rápido, pero menos seguro. Recomendado solo para usuarios que priorizan la velocidad sobre la seguridad.



@SAULRUIZPLAZA



DESVENTAJAS



- **Velocidad reducida:** El cifrado y la ruta adicional del tráfico pueden disminuir la velocidad de conexión.
- **Costo:** Las mejores VPNs suelen ser servicios de pago. Las opciones gratuitas pueden ser menos seguras o limitadas.
- **Compatibilidad:** Algunas aplicaciones o servicios pueden no funcionar correctamente cuando se utiliza una VPN.
- **Confianza en el proveedor:** No todos los proveedores de VPN mantienen políticas estrictas de privacidad. Elegir un proveedor confiable es crucial.

@SAULRUIZPLAZA



¿CUAL VPN DEBO UTILIZAR?



- **Privacidad:** Busca una política estricta de no guardar registros (No-Logs Policy).
- **Velocidad:** Prioriza servidores rápidos y estables para streaming o juegos.
- **Ubicación:** Servidores en varios países facilitan acceso a contenido restringido.
- **Compatibilidad:** Verifica que funcione con todos tus dispositivos y sistemas operativos.
- **Seguridad:** Opta por protocolos avanzados como **OpenVPN o WireGuard**.
- **Soporte:** Elige proveedores con atención 24/7.



MUCHAS GRACIAS

¡Compártelo con tus
amigos!

[@SAULRUIZPLAZA](https://www.instagram.com/SAULRUIZPLAZA)