

# VPN

En primer lugar, tu VPN utiliza un cifrado para mezclar tus datos con un código ilegible. Para descifrarlo, es necesario tener la clave correcta, de lo contrario, solo se ven cadenas aleatorias de letras, números y símbolos. A continuación, la VPN redirige tu tráfico de internet a un servidor VPN remoto para superar las restricciones de tu ISP (Proveedor de Servicios de Internet) y para enmascarar tu dirección IP. Además, las mejores VPNs eliminan los registros de los datos que pasan por sus servidores como tu dirección IP, tu historial de navegación, etc. Así, mantendrás tu anonimato y tendrás protección frente a tu ISP, hackers y otras entidades.

Sin una VPN, todo lo que hagas en internet queda totalmente expuesto (incluso en el modo de incógnito). Puesto que tu tráfico no está cifrado ni se redirige a través de un servidor seguro, tu ISP, entre otros, puede registrar tus datos y venderlos. Si alguien descubre tu verdadera dirección IP, puede encontrar tu ubicación real y tu historial de navegación, lo que supone un gran riesgo, sobre todo en países donde no existe la neutralidad de red. Sinceramente, pensar en que los cibercriminales puedan encontrar este tipo de información asusta de verdad.

Una VPN de primer nivel te protege mucho más que un servicio gratuito o que no utilizar una VPN. Aun así, hasta los mejores proveedores tienen debilidades que podrían aprovechar los cibercriminales. Antes de comprar una suscripción a largo plazo, deberías tener en cuenta estos 5 puntos débiles para que elijas el servicio más seguro posible. Para obtener tus datos, los hackers podrían intentar:

## 1. Descodificar el cifrado de la VPN

El riesgo es mayor si utilizas servicios de baja calidad, pero la mayoría de los cibercriminales no intentan descodificar el cifrado que usan las VPNs de máxima calidad porque es caro, difícil y requiere mucho tiempo. Se estima que incluso la Agencia de Seguridad Nacional de EE. UU. necesitaría 100 millones de dólares y más de un año para intentar hackear una de las claves de cifrado de una VPN de primer nivel.



Sin embargo, no todas las VPNs usan los mismos estándares de cifrado. Por ejemplo, los cifrados DES y Blowfish son más antiguos y quizá menos seguros, por lo que deberías evitar aquellos servicios que los utilicen.

## **2. Robar claves de cifrado**

A un ladrón le resulta más fácil entrar en tu casa si consigue robar las llaves. Lo mismo ocurre con los hackers; descodificar datos cifrados a través de la programación es difícil, por eso suelen intentar robar claves de cifrado para descifrarlos. Ya ha habido casos en los que los hackers han robado claves de servidores VPN cuya seguridad se había visto comprometida.

Los hackers utilizan claves de cifrado robadas para lanzar ataques Man-In-The-Middle (MITM) con el fin de descifrar los datos al pasar entre dos puntos. Podríamos decir que es espionaje online, como si tu cartero abriera una carta antes de dejarla en el buzón. Los cibercriminales pueden incluso alterar los datos que vayas a recibir. Cuando intentas acceder a un sitio, te envían una página falsa para interceptar tus datos de acceso.

## **3. Aprovechar las fugas de IP y DNS**

Aprovechar las fugas de IP y DNS no es técnicamente hackear, es una vulnerabilidad muy común en las VPNs de baja calidad.

En conjunto, tu dirección IP y las solicitudes de DNS pueden revelar mucha información sobre ti como tu ubicación física y toda tu actividad en internet. Una VPN debería poder ocultar tu dirección IP y las solicitudes de DNS. Pero si hay algún problema con el software del servicio o no incluye la funcionalidad de desconexión automática (kill switch), los cibercriminales podrían hacerse con datos confidenciales a partir de una fuga.



#### **4. Aprovechar las debilidades de los servidores**

Algunas VPNs no son dueñas de toda su red y pueden alquilar servidores administrados por centros de datos en otros países. Si el proveedor VPN no supervisa correctamente la administración de estos servidores, los hackers podrían encontrar puntos débiles para acceder a la red. Puesto que algunas VPNs aún guardan los datos en discos duros, tu información permanece en los servidores hasta que se elimine en la fase de mantenimiento. Si los hackers acceden a un servidor mal administrado, podrían acceder a estos datos y a las claves de cifrado.

#### **5. Robar registros de usuarios**

La cantidad de datos de usuarios que almacenan estos servicios varía enormemente de uno a otro. Pero cuantos más datos guarde una VPN sobre ti, más información pueden robar los hackers. Los cibercriminales pueden acceder a un servidor vulnerable y robar los registros de los usuarios. Ha habido casos de VPNs que han dejado sus servidores y sus registros totalmente expuestos, revelando así información confidencial como direcciones de domicilios, nombres completos, detalles de pago e historiales de navegación. Con tales datos en su poder, los hackers podrían extorsionarte con facilidad, cometer estafa o robar tus datos de acceso.

Y lo que es peor aún: creía que todas las VPNs que aseguraban tener una política de cero registros (no-logs policy) protegerían al usuario, pero no siempre es así.



Aunque existe una pequeña posibilidad de que incluso los servicios más seguros puedan verse comprometidos, las VPNs con un gran nivel de seguridad son la mejor opción para protegerte frente a los hackers. Si no eres un objetivo con un valor incalculable, los cibercriminales no van a intentar hackear una VPN de primer nivel para robar tus datos. Para ellos, es mucho más fácil acceder a los dispositivos que no están protegidos por una VPN. Un servicio seguro puede:

- Cifrar tus datos con seguridad de nivel militar para que nadie pueda acceder a ellos, ni hackers, ni tu ISP (Proveedor de Servicios de Internet), ni publicistas ni agencias del gobierno.
- Enmascarar tu dirección IP para ocultar tu verdadera ubicación ante posibles espías.
- Eliminar cualquier rastro de tu historial en internet para que nadie pueda conocer tu actividad en internet como pueda ser el acceso a contenido bloqueado, las descargas torrents o el acceso a la dark web.
- Evitar el rastreo de tu actividad en internet por parte de anunciantes y páginas web, entre otros, y evitar así los anuncios dirigidos.
- Detectar y bloquear contenido peligroso como malware, ransomware (secuestro de información), virus, estafas por suplantación de identidad (phishing) y otros métodos que utilizan los cibercriminales para robar tus datos de acceso o controlar tus dispositivos.



## Mejores VPN de pago

### ExpressVPN



ExpressVPN

Español

### Oferta especial: 12 meses + 3 meses GRATIS

¡Obtenga acceso a todas las aplicaciones de ExpressVPN, un ancho de banda ilimitado de alta velocidad y soporte técnico las 24 horas, los 7 días, en 3 sencillos pasos!

**PASO 1** Seleccione el plan que más le convenga:

Plan	Costo mensual	Garantía
1 Mes	€12,09 al mes	€12,09 facturados cada mes.* Garantía de devolución de dinero a 30 días.
12 Meses (+ 3 MESES GRATIS)	€6,22 al mes (Ahorre 49%)	€181,20 / €93,28 facturados los primeros 15 meses y posteriormente cada 12 meses.* Garantía de devolución de dinero a 30 días.
6 Meses	€9,32 al mes	€55,95 facturados cada 6 meses.* Garantía de devolución de dinero a 30 días.

**MÁS POPULAR**

garantía de devolución de dinero a 30 días


\*Todos los pagos se cobrarán en USD.

- Cifrado AES de 256 bits de primer nivel combinado con protocolos casi imposibles de hackear para proteger tus datos.
- Protección frente a fugas (*leak protection*) y funcionalidad de desconexión automática (*kill switch*) para evitar a los espías.
- Compatible con *malware blockers* y *ad blockers* para protegerte frente a contenido peligroso.
- Más de 3.000 servidores cifrados en 94 países (incluidos España y México) para navegar de forma segura.
- Protege hasta 5 dispositivos al mismo tiempo.


ExpressVPN tiene su sede en las Islas Vírgenes Británicas. Las leyes en las Islas Vírgenes Británicas permiten más privacidad y anonimato que las leyes en los Estados Unidos o en Europa, lo cual convierte a ExpressVPN en una VPN extraterritorial ideal



## CyberGhost










Refuerce su privacidad digital: **3 años por 1.99 € al mes**  
La oferta termina en **06 Días 18 Horas 26 Min 18 Seg**



[Elige un plan](#) > Selecciona un método de pago

Todos los planes de facturación incluyen:

- ✓ Más de 7900 servidores VPN
- ✓ 7 dispositivos protegidos
- ✓ Asistencia en vivo las 24 horas
- ✓ Disponible para:       

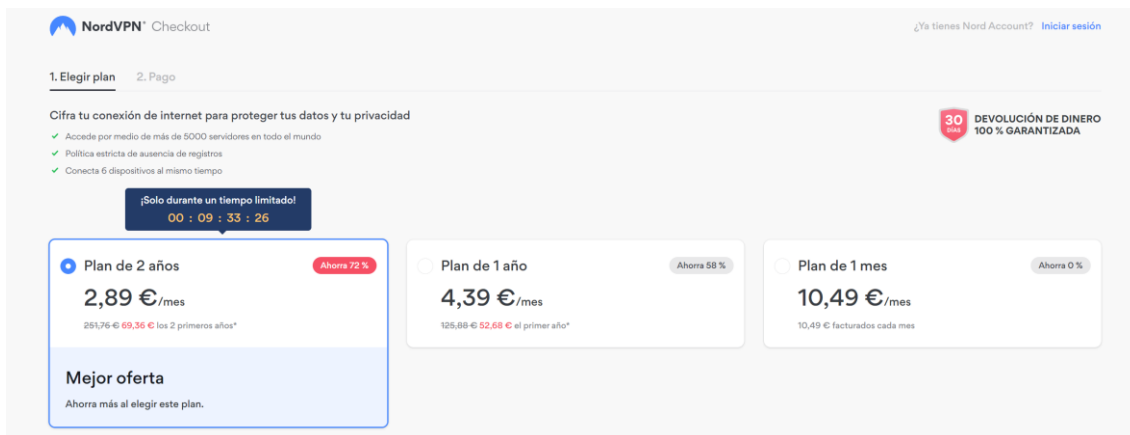
<p>MEJOR OFERTA - 83%</p> <p>3 años <b>3 años + 3 meses</b> <b>1.99 €</b>/mes Facturado 77.61 € cada 3 años</p> <p><a href="#">Obtenga el plan</a></p> <p>Garantía de reembolso de 45 días</p>	<p>2 años <b>2.95 €</b>/mes Facturado 70.8 € cada 2 años</p> <p><a href="#">Obtenga el plan</a></p> <p>Garantía de reembolso de 45 días</p>	<p>1 año <b>3.75 €</b>/mes Facturado 45 € cada año</p> <p><a href="#">Obtenga el plan</a></p> <p>Garantía de reembolso de 45 días</p>	<p>1 Mes <b>11.99 €</b>/mes Facturado 11.99 € cada mes</p> <p><a href="#">Obtenga el plan</a></p> <p>Garantía de reembolso de 14 días</p>
--	---	---	---

⚠ ¡IMPORTANT!  
El plan de 39 MESES incluye los mayores ahorros y es totalmente reembolsable durante 45 días.

- Protocolos de cifrado de nivel militar para navegar de forma segura.
- Protección frente a fugas (*leak protection*) y funcionalidad de desconexión automática (*kill switch*) para proteger tus datos.
- *Malware blocker* y *ad blocker* para mayor protección.
- Más de 7.000 servidores seguros en 89 países (incluidos España y México).
- Protege hasta 7 dispositivos simultáneamente.
- Tiene su sede en Rumanía



## NordVPN



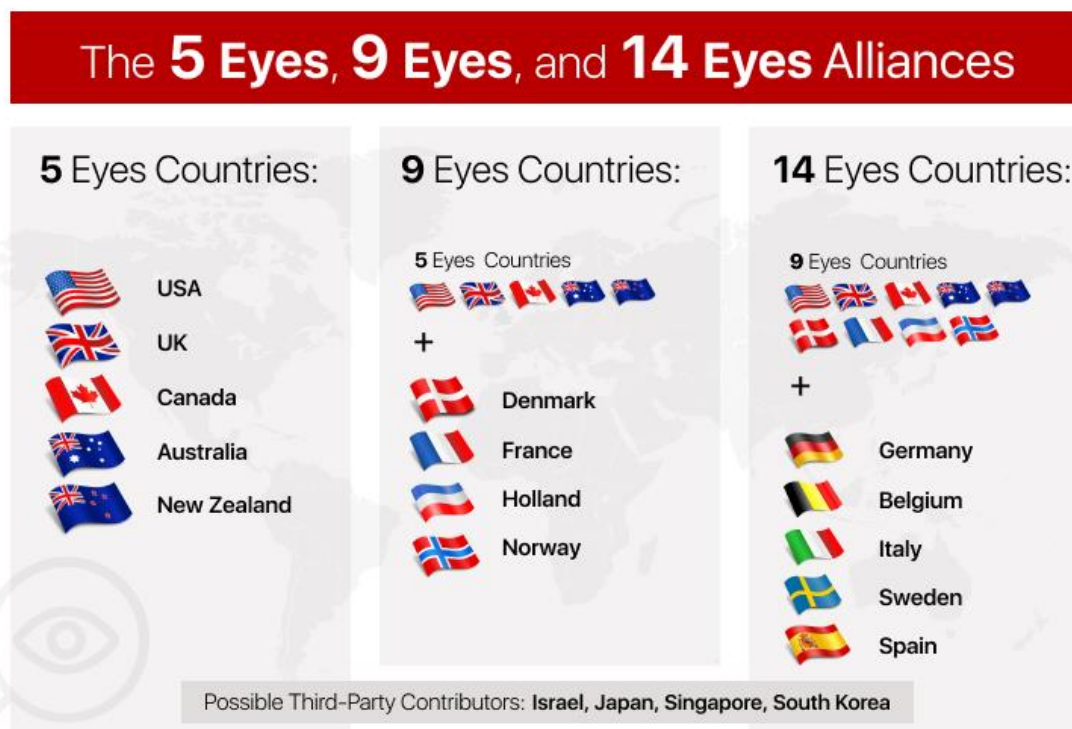
The screenshot shows the NordVPN checkout page. At the top, it says "NordVPN Checkout" and "¿Ya tienes Nord Account? [Iniciar sesión](#)". Below this, there are two tabs: "1. Elegir plan" and "2. Pago". The "1. Elegir plan" tab is active. It features a section titled "Cifra tu conexión de internet para proteger tus datos y tu privacidad" with three bullet points: "Accede por medio de más de 5000 servidores en todo el mundo", "Política estricta de ausencia de registros", and "Conecta 6 dispositivos al mismo tiempo". To the right of this section is a red badge that says "30 días DEVOLUCIÓN DE DINERO 100 % GARANTIZADA". Below the bullet points is a blue box with a white border that says "¡Solo durante un tiempo limitado!" and a timer "00 : 09 : 33 : 26". There are three plan options: "Plan de 2 años" (2,89 €/mes, 251,76 € 69,36 € los 2 primeros años\*, Ahorra 72 %), "Plan de 1 año" (4,39 €/mes, 125,88 € 52,68 € el primer año\*, Ahorra 58 %), and "Plan de 1 mes" (10,49 €/mes, 10,49 € facturados cada mes, Ahorra 0 %). The "Plan de 2 años" is highlighted with a blue border and a blue dot. Below the plans is a section titled "Mejor oferta" with the text "Ahorra más al elegir este plan."

- Más de 60 servidores en África y en la India.
- Más de 2.360 servidores que se ubican en Europa.
- 2.200 servidores en América.
- Al menos 443 servidores en la región asiática.
- 6 dispositivos
- Cifrado AES-256 bit





## La alianza de los 5, 9 o 14 ojos



**Otros países contribuyentes:** Israel, Japón, Singapur, Corea del Sur

La Alianza de los Cinco Ojos nació a raíz de un pacto de inteligencia de la época de la guerra fría llamado el UKUSA Agreement (Acuerdo UK-EEUU). Originalmente se trataba de un acuerdo de intercambio de información entre Estados Unidos y Reino Unido que tenía como fin descifrar inteligencia soviética.

A finales de 1950s, Canadá, Australia y Nueva Zelanda también se habían unido a la Alianza; estos cinco países de habla sajona forman la Alianza de los Cinco Ojos como la conocemos hoy en día. El acuerdo de intercambio de información entre estos cinco países sólo se ha visto reforzado con el tiempo, y se ha extendido a la vigilancia de la actividad en Internet.

Las prácticas de intercambio de información de estos países tienen graves consecuencias para los usuarios de Internet, y especialmente de VPNs. **Es seguro asumir que, si cualquiera de estos 14 países consigue acceso a tus datos en Internet, tus datos serán compartidos con los otros países.**





## Datos a tener en cuenta

Dependiendo del país en el que tenga su sede, **tu proveedor VPN podría ser obligado a proporcionar información de sus usuarios al gobierno**. Estos datos podrían luego ser compartidos con otros países de la alianza, y ni siquiera sabrías que tu privacidad se ha visto comprometida.

Las muchas formas que tienen las VPNs de verse bajo la jurisdicción de varios gobiernos son el motivo de que **las mejores VPNs para privacidad tengan políticas estrictas de no guardar registros**, conocidas en inglés como “no-logs”. Esto quiere decir que no guardan ningún tipo de información identificativa de sus usuarios o de su actividad en Internet.

