Nombre: _____ **Fecha:** _____ **Puntuación:** _____

Cómo elegir una VPN Hoja de trabajo

Evaluación de proveedores de VPN, estándares de seguridad, auditorías y políticas de registro

RESUMEN DE APRENDIZAJE SOBRE VPN

ALUMNO
CONDICIÓN DE ESTUDIANTE
Itinerario de defensor de redes

SEGURO
ESTADO DE LA CONEXIÓN
Proteger los paquetes de datos

ACTIVO
PROTECCIÓN CONTRA FUGAS
Protección contra fugas de DNS e IPv6

¡Hola! Este paquete de actividades te guía por los principios fundamentales de las redes privadas virtuales (VPN). Explorarás cómo los túneles cifrados protegen tus datos, cómo funcionan los protocolos de red y cómo identificar y mitigar las fugas de privacidad.

PUNTOS DE CONTROL DE LA HOJA DE TRABAJO

- [ ] **Partes 1-4: Domina los conceptos y protocolos de las VPN.**
- [ ] **Partes 5-7: Resuelve crucigramas y sopas de letras.**
- [ ] **Partes 8-9: Resuelve casos prácticos y el reto de cifrado.**
- [ ] **Parte 10: Repasa las páginas de preguntas frecuentes básicas y avanzadas.**
- [ ] **Parte 11: Explora 10 datos reales interesantes.**
- [ ] **Extra: reto Piensa rápido.**

Abre la guía de VPN de VPN.com

URL: https://www.vpn.com/es/vpn/

Tu hoja de ruta de aprendizaje sobre VPN

- Evalúa la jurisdicción del proveedor y sus políticas sin registros en materia de privacidad.
- Compara la velocidad de protocolos de tunelización como WireGuard y OpenVPN.
- Analiza funciones de seguridad como los kill switches y los nodos de servidores solo RAM.
- Identificar las auditorías de seguridad independientes y los planes de precios al elegir.
- Elige las ubicaciones de servidor según tus necesidades de velocidad y de desbloqueo geográfico.

INSTRUCCIONES DE LA HOJA DE TRABAJO DE SELECCIÓN

Responde a las preguntas de opción múltiple y de verdadero/falso, completa las frases con huecos usando el banco de palabras, relaciona las definiciones y resuelve el crucigrama y la sopa de letras. Aplica tus conocimientos a la elección de una infraestructura de VPN segura. Termina con la actividad extra Piensa rápido.

CÓMO ELEGIR UNA VPN (INTRODUCCIÓN)

Elegir la VPN adecuada exige mirar más allá de la publicidad. Un proveedor fiable debe tener una política de cero registros demostrada, protocolos de cifrado seguros y clientes de código abierto. Si evalúas las funciones de seguridad, las jurisdicciones y el rendimiento de velocidad, podrás elegir una VPN que se adapte a tus necesidades de protección digital.

LEE ATENTAMENTE CADA PUNTO DE CONTROL Y SELECCIONA O ESCRIBE LA RESPUESTA CORRECTA.

Punto de control 1: Reto de opción múltiple

1. ¿Cuál es el factor clave al elegir un proveedor de VPN seguro?

- A. El número de países con servidores
- B. Una política de no registros auditada de forma independiente
- C. El nivel de precio mensual más bajo
- D. Patrocinios publicitarios llamativos

2. ¿Qué protocolo VPN ofrece el mejor equilibrio entre velocidad y facilidad de auditoría?

- A. PPTP (heredado)
- B. L2TP/IPSec
- C. OpenVPN solo sobre TCP
- D. WireGuard

3. ¿Por qué los usuarios deberían evitar las VPN gratuitas para actividades delicadas?

- A. Están prohibidos en Estados Unidos
- B. A menudo venden tu historial de navegación web
- C. No admiten la navegación web básica
- D. Requieren hardware especial para conectarse

4. ¿Qué determina la jurisdicción legal de origen de un proveedor?

- A. La velocidad de la conexión al servidor
- B. Los tipos de dispositivos compatibles
- C. Leyes locales sobre conservación de datos y órdenes de registro
- D. El tema visual de la aplicación cliente

5. ¿Cuál es la finalidad principal de la función «kill switch» de un cliente VPN?

- A. Bloquear el acceso a internet si la conexión VPN se cae
- B. Eliminar todas las aplicaciones instaladas en el dispositivo
- C. Para duplicar la velocidad de la conexión con el servidor
- D. Para reiniciar el sistema operativo cuando está inactivo

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. Una VPN protege tu dispositivo de las descargas de malware y los archivos con virus.

○ Verdadero ○ Falso

7 Pregunta 7

7. Las auditorías independientes de empresas como Deloitte verifican las afirmaciones de cero registros.

○ Verdadero ○ Falso

8 Pregunta 8

8. Las leyes del país de origen de un proveedor no afectan a la privacidad de los datos de los usuarios.

○ Verdadero ○ Falso

9 Pregunta 9

9. El código base compacto de WireGuard es más fácil de auditar que el de OpenVPN.

○ Verdadero ○ Falso

10 Pregunta 10

10. Las VPN gratuitas a menudo venden anuncios o rastrean a los usuarios para cubrir los costes de los servidores.

○ Verdadero ○ Falso

Punto de control 3: Inserción de términos clave

Lee cada una de las frases siguientes y rellena el espacio en blanco con el término correcto del banco de palabras.

1. Una política _____ verificada de forma independiente compromete a un proveedor de VPN a no registrar tu historial en línea.

2. El moderno protocolo _____ ofrece alta velocidad y usa una base de código muy pequeña.

3. Una función de seguridad llamada _____ detiene todo el tráfico si la conexión VPN falla de repente.

4. Evaluar la _____ legal de un proveedor determina si está sujeto a tratados de vigilancia.

5. Proteger los servidores con almacenamiento _____ ayuda a evitar que los datos de los usuarios persistan tras un reinicio.

6. Verificar una política de conocimiento cero requiere una _____ de seguridad externa realizada por empresas de prestigio.

BANCO DE PALABRAS DE VOCABULARIO

AUDITORÍA CINCO OJOS JURISDICCIÓN KILL SWITCH SIN REGISTROS
SOLO RAM VPN GRATUITA WIREGUARD

Escribe aquí tus respuestas:

1. **2.**

3. **4.**

5. **6.**

Punto de control 4: Relación de conceptos de redes

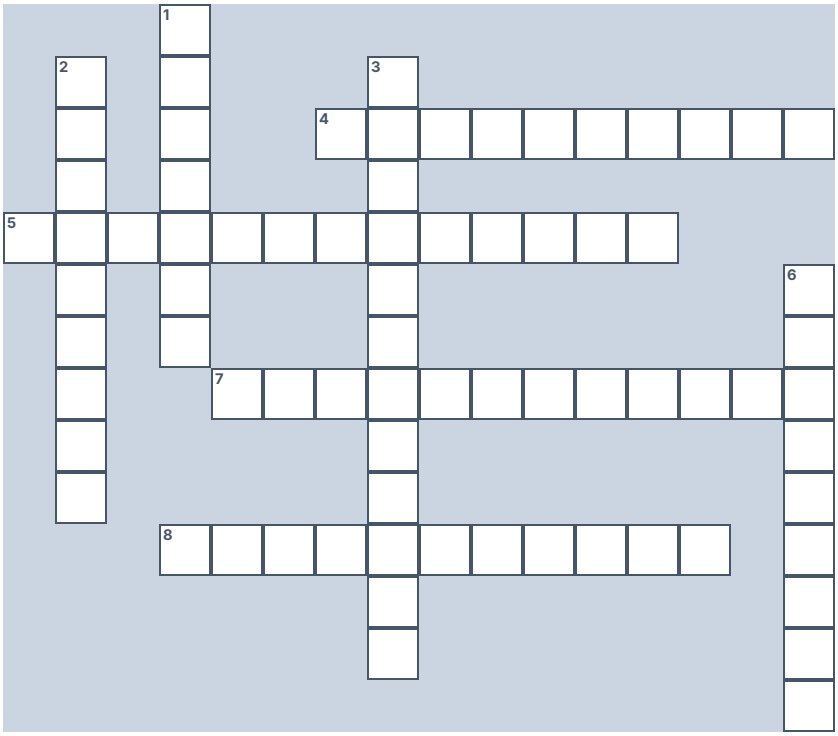
RELACIÓN DE DEFINICIONES

Relaciona cada término de vocabulario de la izquierda con su definición correcta de la derecha escribiendo la letra correspondiente (A-H) en la casilla rellenable.

☐	1. WireGuard	A	Servicio de conexión de alto riesgo que a menudo obtiene ingresos registrando y vendiendo datos de navegación.
☐	2. Registros auditados	B	Mecanismo de seguridad que bloquea el enrutamiento a internet si el túnel seguro se desconecta.
☐	3. Jurisdicción	C	Alianza internacional de intercambio de inteligencia entre EE. UU., Reino Unido, Canadá, Australia y Nueva Zelanda.
☐	4. Kill switch	D	Infraestructura de hardware que funciona con memoria volátil, de modo que los datos no se almacenan en disco.
☐	5. Cinco Ojos	E	La región geográfica que rige las obligaciones legales del proveedor de VPN.
☐	6. VPN gratuita	F	Protocolo moderno y rápido que utiliza unas 4.000 líneas de código muy fácil de auditar.
☐	7. Servidores solo RAM	G	Protocolo de código abierto maduro y ampliamente auditado, con una base de código mucho mayor que la de WireGuard.
☐	8. OpenVPN	H	Afirmación de privacidad verificada por empresas de ciberseguridad externas e independientes.

Punto de control 5: Crucigrama

Resuelve el crucigrama escribiendo letras en las casillas blancas activas. Los números corresponden a las pistas de abajo.



HORIZONTALES

4. Mecanismo de seguridad que bloquea el tráfico de internet si el túnel seguro se desconecta (10)

5. Infraestructura de hardware que funciona totalmente con memoria volátil, lo que impide almacenar datos (13)

7. Región geográfica cuyas leyes rigen las obligaciones legales del proveedor de VPN (12)

8. Servicio de conexión de alto riesgo que a menudo se monetiza registrando y vendiendo datos de navegación (11)

VERTICALES

1. Protocolo de código abierto maduro y muy auditado, con una base de código mucho mayor que la de WireGuard (7)

2. Protocolo moderno y rápido que usa unas 4000 líneas de código muy fácil de auditar (9)

3. Afirmación de privacidad verificada por empresas de ciberseguridad externas e independientes (12)

6. Alianza internacional de intercambio de inteligencia entre EE. UU., Reino Unido, Canadá, Australia y Nueva Zelanda (9)

Punto de control 5, alternativa: Pistas accesibles del crucigrama

Los usuarios de lectores de pantalla y de teclado pueden escribir las respuestas del crucigrama directamente en los campos de texto de abajo.

HORIZONTALES

4 horizontal: Mecanismo de seguridad que bloquea el tráfico de internet si el túnel seguro se desconecta (10 letras):

5 horizontal: Infraestructura de hardware que funciona totalmente con memoria volátil, lo que impide almacenar datos (13 letras):

7 horizontal: Región geográfica cuyas leyes rigen las obligaciones legales del proveedor de VPN (12 letras):

8 horizontal: Servicio de conexión de alto riesgo que a menudo se monetiza registrando y vendiendo datos de navegación (11 letras):

VERTICALES

1 vertical: Protocolo de código abierto maduro y muy auditado, con una base de código mucho mayor que la de WireGuard (7 letras):

2 vertical: Protocolo moderno y rápido que usa unas 4000 líneas de código muy fácil de auditar (9 letras):

3 vertical: Afirmación de privacidad verificada por empresas de ciberseguridad externas e independientes (12 letras):

6 vertical: Alianza internacional de intercambio de inteligencia entre EE. UU., Reino Unido, Canadá, Australia y Nueva Zelanda (9 letras):

Punto de control 6: Sopa de letras

Encuentra los 8 términos clave del vocabulario ocultos en la cuadrícula de abajo. Las palabras pueden estar en horizontal, en vertical o en diagonal.

S	K	Ñ	D	N	C	D	J	H	I	H	B	B	O	R
O	M	P	V	T	I	Y	U	F	C	Y	R	H	X	W
R	I	F	Q	T	Ñ	U	R	T	K	R	D	T	S	M
T	P	L	N	S	I	K	I	O	P	E	N	V	P	N
S	P	I	Y	O	M	W	S	W	U	Ñ	Y	Q	Q	B
I	A	L	O	N	S	B	D	L	I	F	J	Ñ	Y	C
G	B	Z	Z	L	Y	B	I	N	V	X	M	C	F	I
E	O	W	L	P	Q	X	C	H	E	Y	C	W	M	N
R	F	I	H	H	Z	W	C	C	O	Q	K	W	X	C
N	K	R	L	Z	A	N	I	R	Z	R	M	G	S	O
I	S	E	R	V	I	D	O	R	E	S	R	A	M	O
S	W	G	L	W	J	B	N	Y	C	C	Y	O	U	J
Z	O	V	P	N	G	R	A	T	U	I	T	A	Z	O
U	T	B	I	V	P	X	C	N	M	I	P	X	Y	S
D	R	A	U	G	E	R	I	W	Z	X	H	Ñ	J	Ñ

LISTA DE PALABRAS DE VOCABULARIO

WIREGUARD SINREGISTROS JURISDICCION KILLSWITCH CINCOOJOS
VPNGRATUITA SERVIDORESRAM OPENVPN

Punto de control 6, alternativa: Relación de vocabulario accesible

Relaciona cada uno de los 8 términos de vocabulario de la sopa de letras con su definición correcta escribiendo la letra (A-H) en el espacio en blanco.

TÉRMINOS DE VOCABULARIO

- **A. WIREGUARD**
- **B. SINREGISTROS**
- **C. JURISDICCION**
- **D. KILLSWITCH**
- **E. CINCOOJOS**
- **F. VPNGRATUITA**
- **G. SERVIDORESRAM**
- **H. OPENVPN**

DEFINICIONES Y CAMPOS DE RELACIÓN

_____ 1. Alianza internacional de intercambio de inteligencia entre EE. UU., Reino Unido, Canadá, Australia y Nueva Zelanda.

_____ 2. Protocolo moderno y rápido que usa unas 4000 líneas de código muy fácil de auditar.

_____ 3. Protocolo de código abierto maduro y muy auditado, con una base de código mucho mayor que la de WireGuard.

_____ 4. Servicio de conexión de alto riesgo que a menudo se monetiza registrando y vendiendo datos de navegación.

_____ 5. Mecanismo de seguridad que bloquea el tráfico de internet si el túnel seguro se desconecta.

_____ 6. Infraestructura de hardware que funciona totalmente con memoria volátil, lo que impide almacenar datos.

_____ 7. Región geográfica cuyas leyes rigen las obligaciones legales del proveedor de VPN.

_____ 8. Afirmación de privacidad verificada por empresas de ciberseguridad externas e independientes.

Punto de control 7: Reto de palabras desordenadas

Ordena las letras de abajo para descubrir conceptos y términos clave de las VPN. Escribe tus respuestas en los campos rellenables.

1. UGEIWARDR
2. NUSDJIORCCII
3. COOIJSCON
4. DAERRIMORSSEV
5. IRSISNETGSOR
6. CSLITKIWHL
7. URVPTAITNAG
8. PNNOPVE

Actividad extra: Piensa rápido

3 RESPUESTAS POR CATEGORÍA. GANA QUIEN COMPLETE PRIMERO LA LISTA.

1	Cosas que una VPN puede ocultar			
2	Cosas que importan más que el precio			
3	Lugares donde leer reseñas de VPN			
4	Cosas de las que una VPN no puede protegerte			
5	Preguntas para el equipo de ventas de una VPN			
6	Cosas que puede ver tu proveedor de internet			
7	Elementos de tu lista de comprobación al elegir una VPN			
8	Lugares en los que usarías una VPN			
9	Señales de alerta en un proveedor de VPN			
10	Palabras relacionadas con la privacidad			
11	Cosas que probarías primero			
12	Promesas que hace un buen proveedor de VPN			
13	Razones para usar una VPN cuando viajas			
14	Dispositivos que pueden usar una VPN			
15	Mitos sobre las VPN			

Punto de control 8: Casos prácticos de VPN

Aplica los conceptos que has aprendido para resolver los escenarios reales que aparecen a continuación.

SARAH (ESTUDIANTE EN LA CAFETERÍA)

👩‍💻 "¡Hola! Estoy en Coffee & Bytes. Hay una red pública no segura llamada 'Free_Wi-Fi_No_Password'. Quiero iniciar sesión en el correo electrónico de mi centro y subir mi trabajo, pero me preocupan los hackers. ¿Qué riesgos tiene usar esta red sin una VPN y cómo protege una VPN mis datos?"

ALEX (ESTUDIANTE VIAJERO)

👩‍💻 "¡Oh, no! Estoy de viaje en el extranjero por un proyecto e intento ver un documental de biología alojado en un servidor de mi país. Pero el sitio dice 'Este vídeo no está disponible en tu ubicación actual'. ¿Por qué estoy bloqueado y cómo puede ayudarme una VPN a verlo?"

Punto de control 9: Descifrar el código

Para completar tu formación con la guía de selección, descifra este mensaje oculto sobre cómo elegir una infraestructura segura.

CLAVE DE CIFRADO DE LETRAS A NÚMEROS

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9
J=10 K=11 L=12 M=13 N=14 Ñ=15 O=16 P=17 Q=18
R=19 S=20 T=21 U=22 V=23 W=24 X=25 Y=26 Z=27

3	16	13	17	1	19	1		21	22	20		9	14	6	16	19	13	5	20
3	16	14		22	14		20	9	20	21	5	13	1		20	5	7	22	19	16

Mensaje descifrado:

CONSEJO: CADA NÚMERO REPRESENTA LA POSICIÓN DE ESA LETRA EN EL ALFABETO (P. EJ., 1 = A, 2 = B, 27 = Z).

Punto de control 10: Preguntas frecuentes básicas sobre VPN (Parte A)

Repasa las preguntas y respuestas más habituales que tienen los posibles clientes sobre el uso de redes privadas virtuales.

Q1: ¿Qué es una VPN y cómo funciona?

Una red privada virtual (VPN) cifra tu conexión a internet y enruta tu tráfico a través de un servidor remoto seguro. Así se enmascara tu dirección IP pública y se limita lo que los observadores de la red local y tu ISP pueden ver del tráfico que pasa por el túnel VPN.

Q2: ¿Por qué debería usar una VPN?

Una VPN protege tu privacidad digital, asegura tu conexión en redes wifi públicas (como cafeterías o aeropuertos), puede reducir la limitación de velocidad basada en la actividad cuando el ISP no puede identificar el tipo de tráfico cifrado, elude las restricciones geográficas para acceder a contenido de todo el mundo y ayuda a proteger los recursos del teletrabajo.

Q3: ¿Me hace una VPN completamente anónimo en internet?

No. Aunque una VPN oculta tu dirección IP y cifra el tráfico, aún se te puede rastrear mediante las cookies del navegador, las cuentas activas (como Google o Facebook), la huella digital del navegador o si tu proveedor de VPN registra tus datos.

Q4: ¿Ralentizará una VPN mi velocidad de internet?

Sí, ligeramente. El proceso de cifrado y la distancia física hasta el servidor VPN añaden latencia y sobrecarga. El impacto varía según el proveedor, el protocolo, la distancia al servidor, el dispositivo y las condiciones de la red.

Q5: ¿Cómo gana dinero?

Revisa el modelo de negocio. Las suscripciones, los niveles freemium y la venta de datos influyen en cuánto puedes confiar en una VPN, y un servicio que nunca recopila tus datos no puede venderlos. Lee primero la política de privacidad. [1]

Punto de control 10: Preguntas frecuentes básicas sobre VPN (Parte B)

Repasa las preguntas y respuestas más habituales que tienen los posibles clientes sobre el uso de redes privadas virtuales.

Q6: ¿Puedo usar una VPN gratuita?

Las VPN gratuitas pueden basarse en publicidad, funciones limitadas, análisis de uso, límites de datos u otros modelos de monetización. Los usuarios deben revisar la política de privacidad, la titularidad, las auditorías y el modelo de negocio del proveedor antes de usarlas.

Q7: ¿Qué es una política de "no registros"?

Una política sin registros describe qué datos de actividad y de conexión afirma el proveedor que no conserva. El alcance exacto varía, por lo que conviene revisar la política y los resultados de las auditorías independientes.

Q8: ¿Cómo elijo la mejor VPN?

Busca políticas de no registros auditadas, protocolos sólidos (WireGuard, OpenVPN), ubicaciones de servidores seguras, velocidades altas, servidores solo RAM, una función de kill switch y una jurisdicción fuera de las alianzas de intercambio de inteligencia (como los 5/9/14 Ojos).

Q9: ¿Puedo usar una VPN en mi teléfono y en mi smart TV?

Sí. Los proveedores de VPN modernos ofrecen aplicaciones dedicadas para iOS, Android, macOS, Windows, Linux y televisores inteligentes, así como configuraciones para routers que protegen todos los dispositivos de tu red doméstica.

Q10: ¿Qué es un kill switch?

Un kill switch es una función de seguridad que desconecta automáticamente tu dispositivo de internet si la conexión VPN se cae. Así se evita que se filtren tus datos sin cifrar o tu dirección IP real.

Punto de control 10: Preguntas frecuentes avanzadas sobre VPN (Parte C)

Explora los aspectos técnicos y estructurales de las redes privadas virtuales y los protocolos de tunelización seguros.

Q1: ¿Qué diferencia hay entre WireGuard, OpenVPN e IKEv2?

WireGuard es un protocolo moderno y ligero (solo unas 4.000 líneas de código) que ofrece velocidades altas y tiempos de conexión cortos. OpenVPN es un protocolo de código abierto muy seguro y probado a fondo. IKEv2 es excelente para dispositivos móviles por su capacidad de reconectarse rápidamente al cambiar de red.

Q2: ¿Qué es la doble VPN o enrutamiento multisalto?

El multisalto enruta tu tráfico a través de dos o más servidores VPN en secuencia. Esto añade una segunda capa de cifrado y ayuda a mantener tu dirección IP real oculta al segundo salto si uno de los servidores se ve comprometido.

Q3: ¿Qué es la fuga de WebRTC y cómo la evita una VPN?

WebRTC es un protocolo del navegador que puede revelar tus direcciones IP local y pública reales incluso con una VPN activa. Las VPN premium bloquean o falsean las solicitudes WebRTC en sus aplicaciones de escritorio y móviles y en sus extensiones de navegador.

Q4: ¿Qué son los servidores solo RAM y por qué son importantes?

Los servidores tradicionales escriben los datos en discos duros, que pueden ser incautados o comprometidos. Los servidores solo RAM (sin disco) funcionan totalmente en memoria volátil (RAM). Cuando el servidor se reinicia o se apaga, los datos guardados en memoria se borran.

Q5: ¿Cómo elude la ofuscación los bloqueos de VPN?

La ofuscación (o «VPN sigilosa») disfraza los paquetes de tráfico VPN para que parezcan tráfico web HTTPS normal (puerto 443). Esto ayuda a sortear la inspección profunda de paquetes (DPI) que usan los gobiernos o las redes de centros educativos y oficinas para bloquear las VPN.

Punto de control 10: Preguntas frecuentes avanzadas sobre VPN (Parte D)

Explora los aspectos técnicos y estructurales de las redes privadas virtuales y los protocolos de tunelización seguros.

Q6: ¿Qué es el túnel dividido (split tunneling) y cuándo debo usarlo?

El túnel dividido te permite elegir qué apps pasan por el túnel VPN cifrado y cuáles se conectan directamente a internet. Úsalo para enrutar las apps bancarias sensibles a través de la VPN mientras los juegos locales se conectan directamente, evitando la latencia que añade la VPN.

Q7: ¿Cómo funciona el secreto hacia adelante (Perfect Forward Secrecy)?

El PFS garantiza que se genere una clave de cifrado temporal y única para cada sesión. Aunque una clave privada se vea comprometida en el futuro, no podrá usarse para descifrar sesiones pasadas ni futuras, porque estas usaron claves independientes.

Q8: ¿Qué son las alianzas de los 5/9/14 Ojos y por qué deberían importarme?

La jurisdicción puede influir en los procesos legales a los que puede enfrentarse un proveedor, pero el riesgo práctico para la privacidad también depende de los datos que conserva el proveedor, su arquitectura técnica, su titularidad, sus informes de transparencia y su historial de auditorías.

Q9: ¿Qué es la protección contra fugas de DNS?

La protección contra fugas de DNS obliga a tu dispositivo a enviar las consultas de búsqueda de sitios web (consultas DNS) a través de los servidores DNS privados y cifrados de la VPN en lugar de los servidores de tu ISP. Así se evita que tu ISP rastree qué sitios visitas.

Q10: ¿Por qué comprobar quién gestiona y respalda una VPN?

La reputación importa. Investiga a los propietarios y directivos de la empresa, busca auditorías públicas de terceros y comprueba lo que dicen los expertos en seguridad independientes y la prensa antes de confiar en ella. [1]

Parte 11: 10 datos interesantes sobre las VPN y aplicaciones reales

Repasa estos datos y conclusiones reales y muy valiosos sobre la historia, el mercado y la tecnología de las VPN.

1. PRIMER PROTOCOLO VPN

PPTP (protocolo de túnel punto a punto), uno de los primeros protocolos VPN, creado por un grupo liderado por Microsoft en la década de 1990, se considera hoy inseguro, por lo que las VPN modernas usan WireGuard u OpenVPN. [1]

2. VALORACIÓN DE MERCADO

El mercado mundial de las VPN ha crecido rápidamente, impulsado por las crecientes necesidades del teletrabajo y las exigencias de seguridad de las empresas.

3. LA REVOLUCIÓN DE WIREGUARD

WireGuard cuenta con un código base muy simplificado y diseñado para la eficiencia, lo que facilita auditar sus vulnerabilidades de seguridad en comparación con los protocolos tradicionales. [3]

4. ESTÁNDARES DE AUDITORÍA ESTRICTOS

Los principales proveedores de VPN contratan a firmas como Deloitte, KPMG o PwC para comprobar sus afirmaciones de no registros, y a empresas de seguridad como Cure53 para poner a prueba sus aplicaciones y servidores. [4]

5. ORÍGENES DE LA ALIANZA DE LOS 5 OJOS

La asociación de inteligencia Cinco Ojos, formada por EE. UU., Reino Unido, Canadá, Australia y Nueva Zelanda, surgió de la cooperación en inteligencia de señales entre los Aliados durante la Segunda Guerra Mundial.

6. INSPECCIÓN PROFUNDA DE PAQUETES

Los cortafuegos avanzados emplean la inspección profunda de paquetes (DPI) para analizar los metadatos de los paquetes de red y bloquear las características de las conexiones VPN estándar.

7. USO CORPORATIVO

Muchas organizaciones proporcionan una VPN a sus empleados remotos para acceder a sistemas internos como bases de datos, lo que hace de las VPN una herramienta de seguridad habitual en el trabajo.

8. VPN DESCENTRALIZADAS

Las VPN descentralizadas (dVPN) reparten el tráfico por una red de nodos gestionados por pares, lo que reduce la dependencia de un único proveedor centralizado.

9. ANONIMATO: TOR FRENTE A VPN

Una VPN canaliza el tráfico a través de un único proveedor, mientras que Tor (The Onion Router) lo envía a través de tres repetidores voluntarios (de guarda, intermedio y de salida) para maximizar la privacidad. [5]

10. COSTE DE LAS FILTRACIONES DE DATOS

Combinar una VPN con un modelo de acceso de confianza cero, que verifica cada usuario y dispositivo, ayuda a las organizaciones a proteger los datos y a limitar los daños de las filtraciones de datos.

Referencias técnicas y fuentes

Publicaciones citadas, especificaciones criptográficas y normas documentales oficiales utilizadas en esta hoja de trabajo.

REFERENCIAS ACADÉMICAS Y DEL SECTOR

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.
https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

Clave de respuestas: evaluación de proveedores de VPN, estándares de seguridad, auditorías y políticas de registros

1 **Política de registros auditada** PROTOCOLOS — **Respuesta correcta: B**

NOTA PARA DOCENTES

Una política sin registros auditada de forma independiente es la forma más práctica de comprobar las afirmaciones de privacidad de conocimiento cero de un proveedor. El marketing llamativo o las afirmaciones propias no bastan. Cita: Deloitte Advisory, Cure53 Audit.

2 **Superioridad de WireGuard** LATENCIA — **Respuesta correcta: D**

NOTA PARA DOCENTES

WireGuard ofrece un enrutamiento de conexiones moderno y rápido en el espacio del kernel con un código base compacto (~4.000 líneas), lo que hace que las auditorías sean muy eficientes. Cita: IETF Protocol RFC, WireGuard Project.

3 **Pregunta 3** — **Respuesta correcta: B**

NOTA PARA DOCENTES

Las VPN gratuitas también pagan los servidores, y la FTC advierte de que algunas apps de VPN comparten datos de los usuarios con terceros, por ejemplo para mostrar anuncios.

4 **Jurisdicciones legales** CONTROLES DE ENRUTAMIENTO — **Respuesta correcta: C**

NOTA PARA DOCENTES

La jurisdicción determina si la VPN está sujeta a leyes de vigilancia, a obligaciones locales de retención de datos y a citaciones judiciales secretas del gobierno. Cita: Privacy Rights Clearinghouse.

5 **Protección kill switch** PRIVACIDAD — **Respuesta correcta: A**

NOTA PARA DOCENTES

El kill switch corta de inmediato el enrutamiento del adaptador de red del sistema si el túnel se cae, lo que evita la exposición de la IP real y las fugas de DNS. Cita: IETF Tunnel RFC.

Clave de respuestas: Punto de control 2 – Verdadero o falso

6 **Limitaciones frente al malware** ENMASCARAMIENTO DE IP — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Una VPN ofrece un canal cifrado seguro, pero no analiza la carga útil ni los archivos. Para bloquear el malware se necesita un software antivirus. Cita: Deloitte Advisory.

7 **Auditoría independiente** VELOCIDADES — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Los informes de auditoría verifican las configuraciones del software de los servidores, el cumplimiento de la configuración solo RAM y la ausencia de bases de datos de registros. Cita: Deloitte Advisory, Cure53 Audit.

8 **Pregunta 8** — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Los proveedores deben cumplir las leyes de su país de origen, que pueden incluir normas de retención de datos y órdenes de entregar los datos que conservan.

9 **Tamaño del código del protocolo** CORTAFUEGOS — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Una base de código más pequeña reduce la superficie de ataque potencial y facilita que los equipos de seguridad verifiquen la integridad del protocolo. Cita: WireGuard Project.

10 **Monetización publicitaria** SIN REGISTROS — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Sin cuotas de suscripción, las VPN gratuitas dependen de la minería de datos, la elaboración de perfiles de tráfico y la inyección de anuncios en el navegador para generar ingresos. Cita: EDRi Retention Guidelines.

Claves de vocabulario y rúbrica de calificación

Rúbrica de calificación para docentes: concede 1 punto por cada relación correcta (8 puntos en total) y por cada término de contexto (6 puntos en total).

PUNTO DE CONTROL 4: SOLUCIÓN DE LA RELACIÓN DE CONCEPTOS

F 1. WireGuard	H 2. Registros auditados	E 3. Jurisdicción	B 4. Kill switch
C 5. Cinco Ojos	A 6. VPN gratuita	D 7. Servidores solo RAM	G 8. OpenVPN

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 SIN REGISTROS	2 WIREGUARD	3 KILL SWITCH	4 JURISDICCIÓN
5 SOLO RAM	6 AUDITORÍA		

PUNTO DE CONTROL 6, ALTERNATIVA: SOLUCIÓN DE LA RELACIÓN DE PALABRAS

1 E – CINCOOJOS	2 A – WIREGUARD	3 H – OPENVPN	4 F – VPNGRATUITA
5 D – KILLSWITCH	6 G – SERVIDORESRAM	7 C – JURISDICCION	8 B – SINREGISTROS

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar WireGuard, Registros auditados y Jurisdicción con sus propias palabras y dar un ejemplo de cada uno.

Casos prácticos:
Pide a los estudiantes que justifiquen sus recomendaciones con datos de la hoja de trabajo y no con suposiciones.

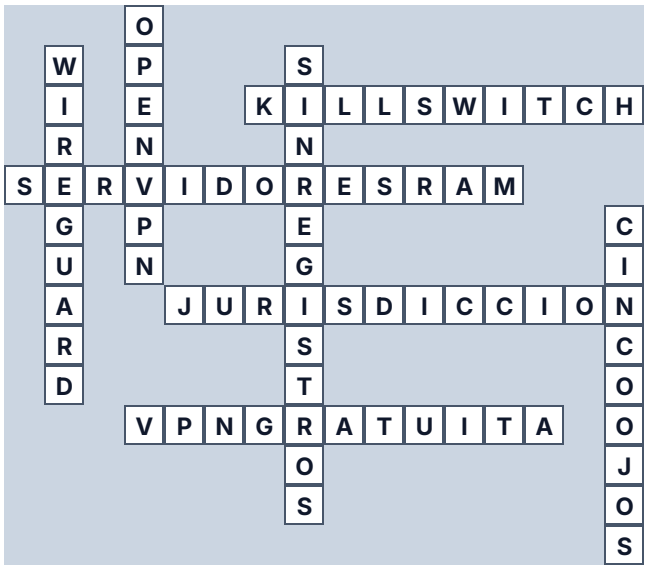
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

S	K	Ñ	D	N	C	D	J	H	I	H	B	B	O	R
O	M	P	V	T	I	Y	U	F	C	Y	R	H	X	W
R	I	F	Q	T	Ñ	U	R	T	K	R	D	T	S	M
T	P	L	N	S	I	K	I	O	P	E	N	V	P	N
S	P	I	Y	O	M	W	S	W	U	Ñ	Y	Q	Q	B
I	A	L	O	N	S	B	D	L	I	F	J	Ñ	Y	C
G	B	Z	Z	L	Y	B	I	N	V	X	M	C	F	I
E	O	W	L	P	Q	X	C	H	E	Y	C	W	M	N
R	F	I	H	H	Z	W	C	C	O	Q	K	W	X	C
N	K	R	L	Z	A	N	I	R	Z	R	M	G	S	O
I	S	E	R	V	I	D	O	R	E	S	R	A	M	O
S	W	G	L	W	J	B	N	Y	C	C	Y	O	U	J
Z	O	V	P	N	G	R	A	T	U	I	T	A	Z	O
U	T	B	I	V	P	X	C	N	M	I	P	X	Y	S
D	R	A	U	G	E	R	I	W	Z	X	H	Ñ	J	Ñ

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

4 horizontal: KILLSWITCH Mecanismo de seguridad que bloquea el tráfico de internet si el túnel seguro se desconecta (10 letras)

5 horizontal: SERVIDORESRAM Infraestructura de hardware que funciona totalmente con memoria volátil, lo que impide almacenar datos (13 letras)

7 horizontal: JURISDICCION Región geográfica cuyas leyes rigen las obligaciones legales del proveedor de VPN (12 letras)

8 horizontal: VPNGRATUITA Servicio de conexión de alto riesgo que a menudo se monetiza registrando y vendiendo datos de navegación (11 letras)

VERTICALES

1 vertical: OPENVPN Protocolo de código abierto maduro y muy auditado, con una base de código mucho mayor que la de WireGuard (7 letras)

2 vertical: WIREGUARD Protocolo moderno y rápido que usa unas 4000 líneas de código muy fácil de auditar (9 letras)

3 vertical: SINREGISTROS Afirmación de privacidad verificada por empresas de ciberseguridad externas e independientes (12 letras)

6 vertical: CINCOOJOS Alianza internacional de intercambio de inteligencia entre EE. UU., Reino Unido, Canadá, Australia y Nueva Zelanda (9 letras)

Clave de soluciones de palabras desordenadas y del cifrado

Clave de calificación de la actividad de ordenar letras del vocabulario y del Reto del código secreto.

CLAVE DE LAS PALABRAS DESORDENADAS

1. UGEIWARDR — **WIREGUARD**
2. NUSDJIORCCII — **JURISDICCION**
3. COOIJSCON — **CINCOOJOS**
4. DAERRIMORSSEV — **SERVIDORESRAM**
5. IRSISNETGSOR — **SINREGISTROS**
6. CSLITKIWHL — **KILLSWITCH**
7. URVPTAITNAG — **VPNGRATUITA**
8. PNNOPVE — **OPENVPN**

CLAVE DEL RETO DEL CÓDIGO SECRETO

"COMPARA TUS INFORMES CON UN SISTEMA SEGURO"

Clave de respuestas de los casos prácticos

A Escenario A: seguridad en redes públicas

SNIFFING Y CIFRADO | El dilema de Sarah

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Riesgos: rastreo de paquetes (sniffing), interceptación de datos y ataques de intermediario (man-in-the-middle). Alguien en la misma red de la cafetería podría capturar sus datos de inicio de sesión o su archivo de deberes.
- Protección VPN: cifra el contenido de los paquetes de red, de modo que el tráfico del túnel interceptado resulta ilegible para los espías pasivos de la red local cuando la VPN está bien configurada.

B Escenario B: Acceder a recursos bloqueados

GEOBLOQUEO E IP | El dilema de Alex

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Por qué se bloquea: el servicio de streaming usa bloqueo geográfico, que asocia la IP local del viajero a su país físico y la bloquea según las licencias territoriales.
- Cómo ayuda la VPN: ocultando su ubicación real al enrutar el tráfico a través de un servidor de su país de origen. El sitio ve la IP del país de origen y permite el acceso.