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

Cómo ocultar tu dirección IP Hoja de trabajo

Ocultar direcciones IP, enmascarar la ubicación, proxy, Tor y evitar fugas de DNS/WebRTC

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

- Explica cómo funcionan las direcciones IP y cómo revelan la ubicación.
- Contrasta los proxies, Tor y las VPN como formas de ocultar las direcciones de red.
- Identificar métodos para detectar y evitar las fugas de DNS y WebRTC.
- Comprende cómo los sitios web rastrean a los usuarios a través de su IP pública.
- Evalúa el enrutamiento multisalto y los túneles cifrados para proteger la IP.

INSTRUCCIONES DE LA HOJA DE TRABAJO SOBRE PROTECCIÓN DE LA IP

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 ocultación de tu dirección IP y la prevención de fugas. Termina con la actividad extra Piensa rápido.

OCULTAR TU IP (INTRODUCCIÓN)

Tu dirección IP es una dirección postal digital que expone tu ubicación física y tus hábitos en la red. Ocultar tu IP es la primera línea de defensa contra el rastreo en línea, la elaboración de perfiles y el bloqueo por geolocalización. Entender cómo ocultar tu dirección de forma segura ayuda a proteger tu privacidad en línea.

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

Punto de control 1: Reto de opción múltiple

1. ¿Qué revela la dirección IP pública de un dispositivo a los sitios web que visitas?

- A. El número de tarjeta de crédito del usuario
- B. Tu ubicación aproximada y el nombre de tu ISP
- C. El directorio completo de archivos locales
- D. La configuración de idioma del teclado

2. ¿Qué método oculta tu IP y cifra todo el tráfico de todo el sistema?

- A. Un proxy web estándar
- B. Borrar las cookies del navegador
- C. Una red privada virtual (VPN)
- D. Desactivar tu cortafuegos nativo

3. ¿Qué gran limitación de privacidad tiene usar un proxy web gratuito?

- A. No cifra el tráfico de datos en las redes públicas
- B. Requiere instalar un sistema operativo externo
- C. Es totalmente ilegal en Estados Unidos
- D. Requiere una conexión de línea telefónica dedicada

4. ¿Cómo proporciona la red Tor un alto grado de anonimato a los usuarios?

- A. Acelerando la velocidad de conexión
- B. Enrutando el tráfico a través de tres relés gestionados por voluntarios
- C. Registrando tu nombre en una base de datos mundial
- D. Restringiendo el acceso solo a organismos gubernamentales

5. ¿Qué es una fuga de DNS?

- A. Un error al enviar un correo electrónico a la dirección equivocada
- B. Cuando las consultas DNS eluden el túnel VPN y van al ISP
- C. Un fallo de hardware en la fuente de alimentación del router local
- D. Una actualización del controlador del adaptador de red local

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. Un servidor proxy cifra el tráfico en segundo plano del sistema operativo igual que una VPN.

- ◯ Verdadero
- ◯ Falso

7 Pregunta 7

7. El enrutamiento de Tor es muy seguro, pero reduce la velocidad de navegación.

- ◯ Verdadero
- ◯ Falso

8 Pregunta 8

8. Las fugas de WebRTC pueden exponer tu IP real durante una sesión de VPN activa.

- ◯ Verdadero
- ◯ Falso

9 Pregunta 9

9. Con una VPN activada y sin filtraciones, tu ISP no puede ver qué sitios web visitas.

- ◯ Verdadero
- ◯ Falso

10 Pregunta 10

10. Ocultar tu dirección IP bloquea el rastreo mediante la huella digital del navegador.

- ◯ 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 vía que elude el túnel seguro y expone tus consultas de dominio se denomina _____ .

2. Las API de comunicación _____ del navegador pueden filtrar por accidente tu dirección IP real.

3. Un _____ web redirige el tráfico del navegador, pero no cifra el contenido de los paquetes.

4. El cifrado de varias capas de la red _____ proporciona un alto nivel de anonimato.

5. Tu _____ pública la asigna tu operadora de telecomunicaciones y revela tu zona.

6. Los bloqueos regionales de contenidos se eluden mediante el enmascaramiento de la _____ .

BANCO DE PALABRAS DE VOCABULARIO

DIRECCIÓN IP ENMASCARAR FUGA DE DNS PROXY TOR TÚNEL VPN UBICACIÓN WEBRTC

Escribe aquí tus respuestas:

1. **2.**

3. **4.**

5. **6.**

Punto de control 4: Relación de conceptos de redes

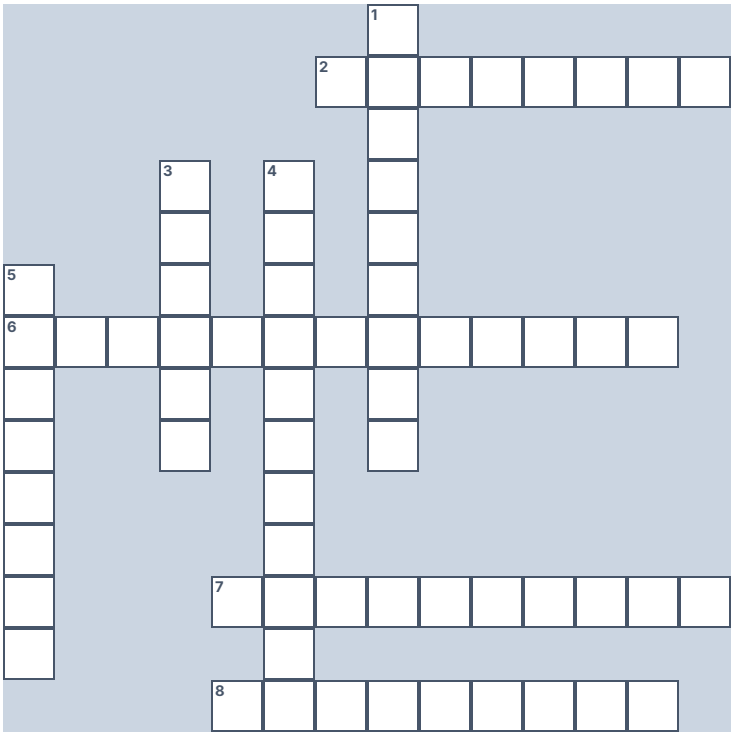
RELACIÓN DE DEFINICIONES

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. Dirección IP	A	Cifra todo el tráfico de un dispositivo y lo enruta a través de un servidor VPN.
☐	2. Túnel VPN	B	Enruta los datos a través de tres servidores voluntarios y cifra una capa en cada paso.
☐	3. Red Tor	C	Enrutar la conexión a través de un servidor de otro país para sortear los bloqueos geográficos.
☐	4. Proxy web	D	Etiqueta numérica única que identifica la interfaz de un dispositivo en internet.
☐	5. Fuga de DNS	E	Redirige el tráfico del navegador en la capa de aplicación sin cifrado del sistema.
☐	6. API WebRTC	F	El registro, por parte de tu operador de telecomunicaciones, de los destinos del tráfico de internet sin cifrar.
☐	7. Ocultación de la ubicación	G	Consultas que se resuelven fuera del túnel VPN y exponen los dominios visitados al ISP.
☐	8. Rastreo por parte del ISP	H	Función del navegador para voz/vídeo que puede eludir los túneles y exponer las direcciones IP reales.

Punto de control 5: Crucigrama

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



HORIZONTALES

2. Cifra todo el tráfico de un dispositivo y lo envía a través de un servidor VPN (8)

6. Registro por parte de tu operadora de los destinos del tráfico de internet sin cifrar (13)

7. Enrutar la conexión a través de un servidor de otro país para eludir los bloqueos geográficos (10)

8. Función del navegador para voz y vídeo que puede eludir los túneles y exponer direcciones IP reales (9)

VERTICALES

1. Consultas que se resuelven fuera del túnel VPN y exponen al ISP los dominios visitados (9)

3. Envía los datos a través de tres servidores voluntarios y cifra una capa en cada paso (6)

4. Etiqueta numérica única que identifica la interfaz de un dispositivo en internet (11)

5. Redirige el tráfico del navegador en la capa de aplicación sin cifrado a nivel de sistema (8)

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

2 horizontal: Cifra todo el tráfico de un dispositivo y lo envía a través de un servidor VPN (8 letras):

6 horizontal: Registro por parte de tu operadora de los destinos del tráfico de internet sin cifrar (13 letras):

7 horizontal: Enrutar la conexión a través de un servidor de otro país para eludir los bloqueos geográficos (10 letras):

8 horizontal: Función del navegador para voz y vídeo que puede eludir los túneles y exponer direcciones IP reales (9 letras):

VERTICALES

1 vertical: Consultas que se resuelven fuera del túnel VPN y exponen al ISP los dominios visitados (9 letras):

3 vertical: Envía los datos a través de tres servidores voluntarios y cifra una capa en cada paso (6 letras):

4 vertical: Etiqueta numérica única que identifica la interfaz de un dispositivo en internet (11 letras):

5 vertical: Redirige el tráfico del navegador en la capa de aplicación sin cifrado a nivel de sistema (8 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.

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

LISTA DE PALABRAS DE VOCABULARIO

DIRECCIONIP TUNELVPN REDTOR PROXYWEB FUGADEDNS APIWEBRTC ENMASCARAR RASTREODELISP

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. DIRECCIONIP**
- **B. TUNELVPN**
- **C. REDTOR**
- **D. PROXYWEB**
- **E. FUGADEDNS**
- **F. APIWEBRTC**
- **G. ENMASCARAR**
- **H. RASTREODELISP**

DEFINICIONES Y CAMPOS DE RELACIÓN

_____ 1. Redirige el tráfico del navegador en la capa de aplicación sin cifrado a nivel de sistema.

_____ 2. Enrutar la conexión a través de un servidor de otro país para eludir los bloqueos geográficos.

_____ 3. Función del navegador para voz y vídeo que puede eludir los túneles y exponer direcciones IP reales.

_____ 4. Etiqueta numérica única que identifica la interfaz de un dispositivo en internet.

_____ 5. Envía los datos a través de tres servidores voluntarios y cifra una capa en cada paso.

_____ 6. Registro por parte de tu operadora de los destinos del tráfico de internet sin cifrar.

_____ 7. Consultas que se resuelven fuera del túnel VPN y exponen al ISP los dominios visitados.

_____ 8. Cifra todo el tráfico de un dispositivo y lo envía a través de un servidor VPN.

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. **CIIICODNRPE** _____
2. **RRDOTE** _____
3. **FEDUDSANG** _____
4. **CASRARAENM** _____
5. **LVUNETPN** _____
6. **EBXWPYRO** _____
7. **BATCRWPEI** _____
8. **ESREIDPROASLT** _____

Actividad extra: Piensa rápido

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

1	Razones para usar una VPN cuando viajas			
2	Navegadores que conoces			
3	Cosas que una VPN puede ocultar			
4	Palabras relacionadas con la privacidad			
5	Palabras de esta hoja de trabajo que quieres recordar			
6	Cosas que un sitio web puede deducir de tu IP			
7	Números o símbolos de una dirección IP			
8	Mitos sobre las VPN			
9	Servicios VPN que conoces			
10	Cosas que puede ver tu proveedor de internet			
11	Promesas que hace un buen proveedor de VPN			
12	Cosas que pueden filtrar tu IP real			
13	Razones para ocultar tu ubicación			
14	Formas de ocultar tu dirección IP			
15	Dispositivos que pueden usar una 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 sobre el enmascaramiento de IP, descifra este mensaje secreto sobre cómo ocultar tus huellas digitales.

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

16	3	22	12	21	1		21	22		4	9	19	5	3	3	9	16	14
3	16	14		22	14		20	9	20	21	5	13	1		16	3	22	12	21	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: ¿Oculta un proxy web mi dirección IP?

Sí, pero solo para el tráfico que se envía a través de él, normalmente el de tu navegador. La mayoría de los proxies web no cifran tus datos, por lo que tu ISP o el operador de la red aún pueden ver lo que envías y recibes.

Q5: ¿Es legal ocultar mi IP?

En muchos países, sí, pero algunos restringen o prohíben las VPN y otras herramientas para ocultar la dirección IP. Ocultar tu IP nunca convierte en legal un acto ilegal, así que consulta las leyes locales antes de usar una.

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: ¿Oculta Tor mi IP?

Sí. Tor envía tu tráfico a través de tres repetidores voluntarios (de guarda, intermedio y de salida), de modo que los sitios web ven la dirección del repetidor de salida y ningún repetidor sabe a la vez quién eres y adónde vas. [1]

Q7: ¿Qué revela mi IP?

Tu IP pública suele revelar tu ISP y una ubicación aproximada, como tu país o ciudad. Los sitios también pueden usarla para vincular tus visitas entre sí y para aplicar bloqueos geográficos.

Q8: ¿Cómo compruebo que está oculta?

Conéctate a tu VPN y, después, visita un sitio de comprobación de IP y haz pruebas de fugas de DNS y WebRTC. La IP y los servidores DNS que aparezcan deben ser los de la VPN, no los de tu ISP. Si aparece tu IP real, activa la protección contra fugas.

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: ¿Por qué pueden seguir rastreándome los sitios web después de ocultar mi dirección IP?

Ocultar tu IP no impide la huella digital del navegador. Los rastreadores pueden combinar datos como la resolución de pantalla, las fuentes instaladas y la configuración del navegador en un identificador, y las cookies o las cuentas con sesión iniciada también pueden identificarte, así que utiliza también un navegador centrado en la privacidad. [3]

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: ¿Puede el tráfico IPv6 filtrar mi dirección IP real?

Sí, si tu VPN solo canaliza IPv4. En ese caso, tu dispositivo puede enviar tráfico IPv6 fuera del túnel y exponer una dirección asignada por tu ISP. Usa una VPN que canalice o bloquee IPv6 y compruébalo con una prueba de fugas de IPv6.

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: ¿Expone el túnel dividido mi dirección IP real?

Sí, en el caso de las aplicaciones que excluyas. El tráfico enviado fuera del túnel usa tu IP real, y el RFC 8828 señala que WebRTC puede revelar la dirección del ISP por debajo de una VPN con túnel dividido, a menos que el navegador lo limite. [2]

Q7: ¿Qué es una dirección IP compartida y cómo ayuda a la privacidad?

Con una IP compartida, muchos usuarios de la VPN aparecen en internet con la misma dirección al mismo tiempo. Eso hace que a un sitio web le resulte mucho más difícil vincular una visita concreta contigo que con una IP dedicada que solo usas tú.

Q8: ¿Puede mi ISP ver que uso una VPN para ocultar mi IP?

Normalmente, sí. Tu ISP puede ver que te conectas a la dirección IP de un servidor VPN, cuándo te conectas y cuántos datos envías, pero no los sitios web que visitas ni el contenido del túnel cifrado.

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: ¿Qué es mejor para ocultar mi IP, un proxy o una VPN?

Normalmente es mejor una VPN. Oculta tu IP en todas las aplicaciones del dispositivo y cifra el tráfico, mientras que un proxy web suele cubrir solo el navegador y a menudo no añade cifrado.

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.

2. HUELLA DIGITAL (FINGERPRINTING)

Ocultar tu IP no impide la huella digital del navegador, que puede identificarte a partir de datos como la resolución de pantalla y las fuentes instaladas. [3]

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.

4. EXPOSICIÓN DE LA DIRECCIÓN POR WEBRTC

El RFC 8828 advierte que WebRTC puede descubrir tanto la dirección pública de una VPN como la dirección del ISP sobre la que funciona la VPN, a menos que el navegador lo limite. [2]

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. REUTILIZACIÓN DE CIRCUITOS TOR

Tor reutiliza el mismo circuito durante unos diez minutos y después crea uno nuevo, lo que hace más difícil relacionar entre sí tus actividades de navegación. [1]

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. [1]

10. PROXIES FRENTE A TÚNELES VPN

Un proxy web cambia la dirección IP que ve un sitio para el tráfico de tu navegador, pero, a diferencia de una VPN, normalmente no cifra ese tráfico ni cubre otras aplicaciones de tu dispositivo. [5]

Referencias técnicas y fuentes

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

REFERENCIAS ACADÉMICAS Y DEL SECTOR

[1] Tor Project. (n.d.). Overview.

https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.

https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.

https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] 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

Clave de respuestas: ocultar direcciones IP, enmascarar la ubicación, proxy, Tor y prevenir fugas de DNS/WebRTC

1 Pregunta 1

Respuesta correcta: B

NOTA PARA DOCENTES

¿Qué revela la dirección IP pública de un dispositivo a los sitios web que visitas? → Tu ubicación aproximada y el nombre de tu ISP

2 Cifrado del sistema VPN LATENCIA

Respuesta correcta: C

NOTA PARA DOCENTES

A diferencia de los proxies, que solo redirigen el tráfico del navegador, una VPN crea un túnel cifrado para todo el sistema que protege las aplicaciones en segundo plano, los juegos y las consultas del sistema operativo. Cita: Tor Project Relays, W3C WebRTC API.

3 Falta de cifrado del proxy SEGURIDAD WIFI

Respuesta correcta: A

NOTA PARA DOCENTES

Los proxies web solo reenvían el tráfico del navegador sin cifrar la carga útil de los paquetes, por lo que tu operador de red o tu ISP aún pueden rastrear el contenido de tu tráfico. Cita: IETF Proxy Vulnerabilities.

4 Pregunta 4

Respuesta correcta: B

NOTA PARA DOCENTES

¿Cómo proporciona la red Tor un alto grado de anonimato a los usuarios? → Enrutando el tráfico a través de tres relés gestionados por voluntarios

5 Fugas de DNS del túnel PRIVACIDAD

Respuesta correcta: B

NOTA PARA DOCENTES

Una fuga de DNS se produce cuando las solicitudes de resolución de nombres de dominio eluden el túnel VPN y van directamente a los resolutores de tu ISP, lo que expone los registros de los dominios visitados. Cita: DNSSEC Tunnel Testing, EFF Tracking Evasion.

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

6 **Detalles de las limitaciones del proxy** ENMASCARAMIENTO DE IP — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Los proxies funcionan en la capa de aplicación y carecen de la integración con el controlador de red de todo el sistema que tiene un túnel VPN. Cita: IETF Proxy Vulnerabilities.

7 **Pregunta 7** — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Retransmitir el tráfico a través de tres relés de voluntarios con cifrado por capas añade latencia, por lo que Tor suele ser más lento que una conexión directa.

8 **Pregunta 8** — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

WebRTC puede revelar direcciones locales y, con algunas configuraciones de VPN, la IP pública asignada por el ISP bajo el túnel (RFC 8828).

9 **Pregunta 9** — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Sin filtraciones de DNS ni de WebRTC, el ISP solo ve tráfico cifrado hacia el servidor VPN, no los sitios que visitas.

10 **Límites frente a la huella digital** SIN REGISTROS — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

La huella digital (fingerprinting) se basa en métricas de configuración del dispositivo (resolución de pantalla, fuentes, complementos) que siguen siendo visibles aunque la IP esté oculta. Cita: EFF Tracking Evasion.

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

D 1. Dirección IP	A 2. Túnel VPN	B 3. Red Tor	E 4. Proxy web
G 5. Fuga de DNS	H 6. API WebRTC	C 7. Ocultación de la ubicación	F 8. Rastreo por parte del ISP

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 FUGA DE DNS	2 WEBRTC	3 PROXY	4 TOR
5 DIRECCIÓN IP	6 UBICACIÓN		

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

1 D – PROXYWEB	2 G – ENMASCARAR	3 F – APIWEBRTC	4 A – DIRECCIONIP
5 C – REDTOR	6 H – RASTREODELISP	7 E – FUGADEDNS	8 B – TUNELVPN

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar Dirección IP, Túnel VPN y Red Tor 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.

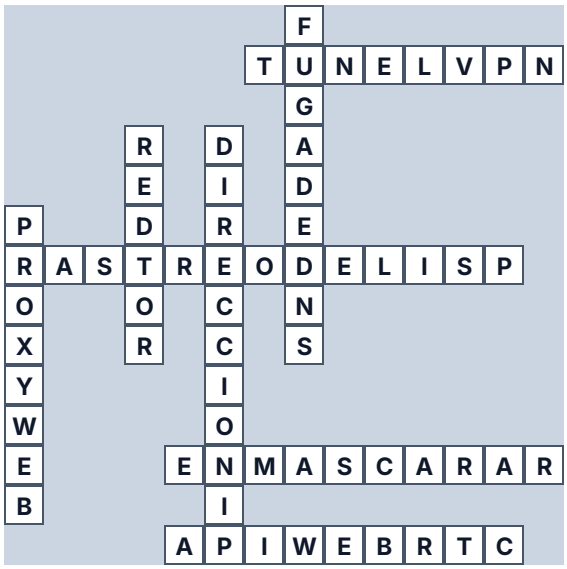
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

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

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

2 horizontal: TUNELVPN Cifra todo el tráfico de un dispositivo y lo envía a través de un servidor VPN (8 letras)

6 horizontal: RASTREODELISP Registro por parte de tu operadora de los destinos del tráfico de internet sin cifrar (13 letras)

7 horizontal: ENMASCARAR Enrutar la conexión a través de un servidor de otro país para eludir los bloqueos geográficos (10 letras)

8 horizontal: APIWEBRTC Función del navegador para voz y vídeo que puede eludir los túneles y exponer direcciones IP reales (9 letras)

VERTICALES

1 vertical: FUGADEDNS Consultas que se resuelven fuera del túnel VPN y exponen al ISP los dominios visitados (9 letras)

3 vertical: REDTOR Envía los datos a través de tres servidores voluntarios y cifra una capa en cada paso (6 letras)

4 vertical: DIRECCIONIP Etiqueta numérica única que identifica la interfaz de un dispositivo en internet (11 letras)

5 vertical: PROXYWEB Redirige el tráfico del navegador en la capa de aplicación sin cifrado a nivel de sistema (8 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. C I I I C O D N R P E — **DIRECCIONIP**
2. R R D O T E — **REDTOR**
3. F E D U D S A N G — **FUGADEDNS**
4. C A S R A R A E N M — **ENMASCARAR**
5. L V U N E T P N — **TUNELVPN**
6. E B X W P Y R O — **PROXYWEB**
7. B A T C R W P E I — **APIWEBRTC**
8. E S R E I D P R O A S L T — **RASTREODELISP**

CLAVE DEL RETO DEL CÓDIGO SECRETO

"OCULTA TU DIRECCION CON UN SISTEMA OCULTO"

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.