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

Qué es una VPN Hoja de trabajo

Ejercicios prácticos sobre protocolos de red, tunelización y controles de seguridad.

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 el concepto de tunelización y encapsulación de datos.
- Identificar las configuraciones de protocolo estándar y los métodos de cifrado.
- Analiza el papel de los servidores y del enmascaramiento de la IP en las redes privadas virtuales.
- Comprende cómo rastrean los ISP la navegación y cómo lo impide una VPN.
- Distingue los límites operativos de la topología de red virtual.

INSTRUCCIONES DE LA GUÍA ¿QUÉ ES UNA VPN?

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 los escenarios reales de la sección de casos prácticos. Termina con la actividad extra Piensa rápido.

¿QUÉ ES UNA VPN? (INTRODUCCIÓN)

Una red privada virtual es mucho más que un interruptor de privacidad. Es un túnel cifrado que enruta tu tráfico de internet a través de un servidor remoto. Así oculta tu dirección IP, impide que tu ISP elabore registros de tu actividad en línea y protege tus datos en las redes públicas. Comprender la terminología es esencial para mantener la seguridad 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 la función principal de una red privada virtual (VPN)?

- A. Aumentar la velocidad de renderizado del navegador web
- B. Cifrar los paquetes de datos y enmascarar tu IP pública
- C. Para almacenar localmente las bases de datos de cookies del sitio web
- D. Para sustituir el hardware físico de tu ordenador

2. ¿Qué es la tunelización de red en el contexto de una VPN?

- A. Eliminar archivos de registro de red duplicados
- B. Instalar archivos de almacenamiento de bases de datos locales
- C. Compartir archivos con otros ordenadores locales
- D. Encapsular un paquete de red dentro de otro paquete seguro

3. ¿Qué estándar de cifrado se usa ampliamente para proteger el tráfico VPN?

- A. Cifrado DES heredado
- B. Estándar moderno AES-256
- C. Codificación base64 en texto plano
- D. Cifrado rot13 estándar

4. ¿Qué componente de tu tráfico de red cifra una VPN?

- A. Solo los trabajos de impresión de la red del dispositivo local
- B. La ruta física del cable Ethernet
- C. Toda la parte de carga útil de datos del paquete de red
- D. Solo los historiales de búsqueda de tu navegador web

5. ¿Qué significa el término «cifrado» en redes?

- A. Convertir datos en texto plano en texto cifrado ilegible
- B. Eliminar registros de comunicaciones antiguos
- C. Aumentar los límites de velocidad de tu ancho de banda local
- D. Compartir públicamente las claves de acceso a la base de datos

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. Una VPN cifra tu tráfico para impedir que te espíen localmente en una red wifi pública.

○ Verdadero ○ Falso

7 Pregunta 7

7. Una VPN cambia físicamente la configuración del hardware de tu router.

○ Verdadero ○ Falso

8 Pregunta 8

8. Los protocolos de túnel envuelven los paquetes de datos en una capa de transporte cifrada.

○ Verdadero ○ Falso

9 Pregunta 9

9. El cifrado simétrico usa la misma clave para cifrar y descifrar el tráfico.

○ Verdadero ○ Falso

10 Pregunta 10

10. Usar una VPN hace que tu conexión a internet sea físicamente inmune a cualquier corte de luz.

○ 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. Para proteger tu tráfico, la VPN envuelve tus paquetes de datos dentro de otro protocolo, un proceso llamado _____ .

2. Si la velocidad de descarga es lenta mientras ves contenido en streaming, puede deberse a un _____ de red limitado.

3. Un servicio de streaming que solo está disponible en un país concreto usa un _____ para restringir a los usuarios de otros lugares.

4. Las reglas de conexión que definen los parámetros de cifrado y de conexión se llaman el _____ de la VPN.

5. Tu ordenador usa un _____ local para supervisar el tráfico de red y bloquear las conexiones inseguras.

6. Cuando te conectas a una VPN, tus datos pasan por un _____ remoto que oculta tu IP pública.

BANCO DE PALABRAS DE VOCABULARIO

ANCHO DE BANDA CORTAFUEGOS GEOBLOQUEO PRIVACIDAD PROTOCOLO
PROVEEDOR SERVIDOR TUNELIZACIÓN

Escribe aquí tus respuestas:

1. **2.**

3. **4.**

5. **6.**

Punto de control 4: Relación de conceptos de redes

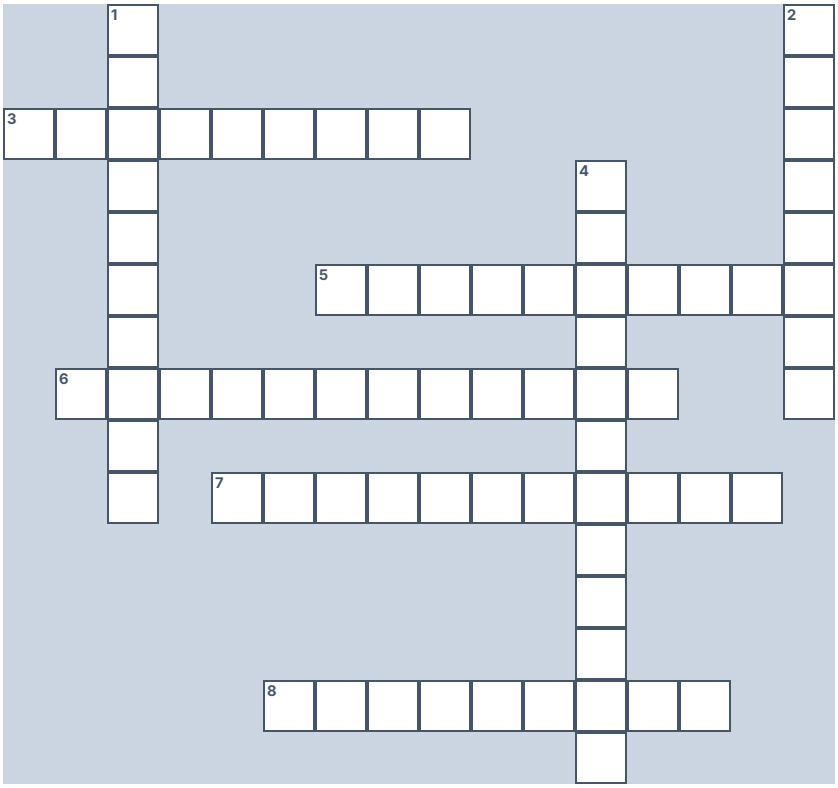
RELACIÓN DE DEFINICIONES

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. Tunelización	A	Un ordenador remoto que enruta tu tráfico y enmascara tu IP.
☐	2. Protocolo	B	Proveedor de servicios de internet que transporta tu tráfico y puede ver la actividad no cifrada.
☐	3. Ancho de banda	C	Una restricción que impide el acceso web en función de la ubicación física.
☐	4. Servidor	D	Un sistema de seguridad que supervisa y bloquea el tráfico no autorizado.
☐	5. Bloqueo geográfico	E	Un conjunto de reglas que determina cómo se transmiten los datos por la red.
☐	6. Cortafuegos	F	El estado de estar libre de rastreo o de vigilancia pública.
☐	7. Privacidad	G	La velocidad máxima de transferencia de datos a través de una conexión.
☐	8. ISP	H	Encapsulación de paquetes de datos dentro de otro paquete para un tránsito seguro.

Punto de control 5: Crucigrama

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



HORIZONTALES

3. Conjunto de reglas que determina cómo se transmiten los datos por la red (9)

5. Estado de estar libre de rastreo o de vigilancia pública (10)

6. Encapsulación de paquetes de datos dentro de otro paquete para transportarlos de forma segura (12)

7. Sistema de seguridad que supervisa y bloquea el tráfico no autorizado (11)

8. Empresa que te da acceso a internet (ISP) y que registra tu tráfico si no está cifrado (9)

VERTICALES

1. Restricción que impide el acceso web según la ubicación física (10)

2. Ordenador remoto que enruta tu tráfico y oculta tu IP (8)

4. Velocidad máxima de transferencia de datos de una conexión (12)

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

3 horizontal: Conjunto de reglas que determina cómo se transmiten los datos por la red (9 letras):

5 horizontal: Estado de estar libre de rastreo o de vigilancia pública (10 letras):

6 horizontal: Encapsulación de paquetes de datos dentro de otro paquete para transportarlos de forma segura (12 letras):

7 horizontal: Sistema de seguridad que supervisa y bloquea el tráfico no autorizado (11 letras):

8 horizontal: Empresa que te da acceso a internet (ISP) y que registra tu tráfico si no está cifrado (9 letras):

VERTICALES

1 vertical: Restricción que impide el acceso web según la ubicación física (10 letras):

2 vertical: Ordenador remoto que enruta tu tráfico y oculta tu IP (8 letras):

4 vertical: Velocidad máxima de transferencia de datos de una conexión (12 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.

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

LISTA DE PALABRAS DE VOCABULARIO

TUNELIZACION PROTOCOLO ANCHODEBANDA SERVIDOR GEOBLOQUEO
CORTAFUEGOS PRIVACIDAD PROVEEDOR

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. TUNELIZACION**
- **B. PROTOCOLO**
- **C. ANCHODEBANDA**
- **D. SERVIDOR**
- **E. GEOBLOQUEO**
- **F. CORTAFUEGOS**
- **G. PRIVACIDAD**
- **H. PROVEEDOR**

DEFINICIONES Y CAMPOS DE RELACIÓN

_____ 1. Conjunto de reglas que determina cómo se transmiten los datos por la red.

_____ 2. Restricción que impide el acceso web según la ubicación física.

_____ 3. Sistema de seguridad que supervisa y bloquea el tráfico no autorizado.

_____ 4. Estado de estar libre de rastreo o de vigilancia pública.

_____ 5. Empresa que te da acceso a internet (ISP) y que registra tu tráfico si no está cifrado.

_____ 6. Encapsulación de paquetes de datos dentro de otro paquete para transportarlos de forma segura.

_____ 7. Ordenador remoto que enruta tu tráfico y oculta tu IP.

_____ 8. Velocidad máxima de transferencia de datos de una conexión.

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. CIALUZITONNE
2. ANODANDCBAEH
3. GOEQELOBUO
4. CAADVDIPRI
5. OOROCTPLO
6. ORVDSIER
7. EACOUSGORFT
8. REOPVREDO

Actividad extra: Piensa rápido

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

1	Cosas que puede revelar una dirección IP			
2	Mitos sobre las VPN			
3	Cosas que viajan por internet			
4	Promesas que hace un buen proveedor de VPN			
5	Secretos que cifrarías			
6	Cosas de las que una VPN no puede protegerte			
7	Formas de detectar una red Wi-Fi falsa			
8	Palabras relacionadas con la privacidad			
9	Dispositivos que pueden usar una VPN			
10	Cosas que ocurren cuando pulsas 'Conectar'			
11	Lugares en los que usarías una VPN			
12	Razones para usar una VPN cuando viajas			
13	Cosas de la vida real que parecen un túnel			
14	Palabras de esta hoja de trabajo que quieres recordar			
15	Palabras para explicar una VPN a un niño			

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

Una VPN cifra tu tráfico para protegerlo. Usa la clave de letras y números de abajo para descifrar el mensaje de ciberseguridad escribiendo las letras correspondientes en los espacios en blanco.

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

17	19	16	21	5	7	5		21	22		17	19	9	23	1	3	9	4	1	4

3	16	14		22	14		21	22	14	5	12		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: ¿Es legal usar una VPN?

El uso de VPN es legal en muchos países, pero algunas jurisdicciones restringen, regulan o bloquean los servicios VPN. Los usuarios deben comprobar la legislación local vigente antes de usarlas. Para más información, consulta las guías de legalidad de VPN.com.

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. [4]

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 el tráfico VPN para que parezca tráfico HTTPS normal (puerto 443). Esto puede ayudar 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: ¿Puede una VPN eludir la limitación de velocidad de internet de un ISP?

A veces. Una VPN puede ayudar cuando un ISP ralentiza selectivamente actividades identificables, pero no resolverá la congestión, los límites de datos, los límites de velocidad de la cuenta ni la mala calidad de la red.

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) fue desarrollado por un grupo de fabricantes que incluía a Microsoft y se publicó como RFC 2637 en julio de 1999 para dar soporte a las VPN de acceso remoto. [6]

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. [4]

4. ESTÁNDARES DE AUDITORÍA ESTRICTOS

Los principales proveedores de VPN contratan a auditores externos (como Cure53 o PwC) para que realicen revisiones de código independientes y verifiquen que no registran la actividad de los usuarios.

5. ORÍGENES DE LA ALIANZA DE LOS 5 OJOS

La alianza Cinco Ojos surgió del acuerdo UKUSA de inteligencia de señales de 1946 entre EE. UU. y Reino Unido, al que más tarde se unieron Canadá, Australia y Nueva Zelanda.

6. INSPECCIÓN PROFUNDA DE PAQUETES

La inspección profunda de paquetes (DPI) examina el contenido de los paquetes y los patrones de tráfico, no solo los encabezados, y algunos cortafuegos la usan para detectar y bloquear los protocolos VPN habituales.

7. USO CORPORATIVO

Un gran porcentaje de los empleados de empresas de todo el mundo usa VPN seguras para iniciar sesión en las bases de datos internas, lo que las convierte en un estándar de seguridad clave.

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), de modo que ningún repetidor conoce ambos extremos.

10. COSTE DE LAS FILTRACIONES DE DATOS

Emplear un modelo de acceso seguro de confianza cero con una VPN ayuda a las organizaciones a proteger su propiedad intelectual y a mitigar el impacto económico 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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

Clave de respuestas: hoja de trabajo «Qué es una VPN»

1 **Función principal** PROTOCOLOS — **Respuesta correcta: B**

NOTA PARA DOCENTES

La función principal de una VPN es establecer un túnel cifrado que protege la carga útil de los paquetes y enmascara la dirección IP pública del usuario. Cita: IETF Tunnel RFC.

2 **Tunelización de red** LATENCIA — **Respuesta correcta: D**

NOTA PARA DOCENTES

Los protocolos de túnel encapsulan los paquetes de datos originales dentro de paquetes portadores externos para que atraviesen de forma segura las redes públicas. Cita: IETF Tunnel RFC.

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

NOTA PARA DOCENTES

¿Qué estándar de cifrado se usa ampliamente para proteger el tráfico VPN? → Estándar moderno AES-256

4 **Componentes cifrados** CONTROLES DE ENRUTAMIENTO — **Respuesta correcta: C**

NOTA PARA DOCENTES

Una VPN cifra el segmento completo de carga útil de los paquetes de datos IP, de modo que el contenido de la transmisión se mantiene confidencial. Cita: IETF Tunnel RFC.

5 **Pregunta 5** — **Respuesta correcta: A**

NOTA PARA DOCENTES

El cifrado usa un algoritmo y una clave para convertir el texto plano en texto cifrado ilegible.

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

6 **Bloqueo de escuchas** ENMASCARAMIENTO DE IP — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Los túneles cifrados garantizan que las cargas útiles de los paquetes sigan siendo ilegibles para quienes intercepten datos en redes Wi-Fi locales. Cita: Deloitte Advisory.

7 **Cambios de hardware** VELOCIDADES — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Las VPN son túneles de red basados en software y no modifican físicamente el hardware de tu router. Cita: Cure53 Audit.

8 **Tunelización de paquetes** RIESGO DE SNIFFING — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

La tunelización consiste en envolver los paquetes de red originales dentro de encabezados de transporte para su tránsito. Cita: IETF Tunnel RFC.

9 **Claves simétricas** CORTAFUEGOS — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

La criptografía simétrica usa una clave compartida tanto para cifrar como para descifrar los flujos de red. Fuente: WireGuard Project.

10 **Inmunidad ante cortes de energía** SIN REGISTROS — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Una VPN solo cifra las señales de la conexión activa; no puede evitar los cortes de servicio causados por apagones locales. 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

H 1. Tunelización	E 2. Protocolo	G 3. Ancho de banda	A 4. Servidor
C 5. Bloqueo geográfico	D 6. Cortafuegos	F 7. Privacidad	B 8. ISP

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 TUNELIZACIÓN	2 ANCHO DE BANDA	3 GEOBLOQUEO	4 PROTOCOLO
5 CORTAFUEGOS	6 SERVIDOR		

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

1 B – PROTOCOLO	2 E – GEOBLOQUEO	3 F – CORTAFUEGOS	4 G – PRIVACIDAD
5 H – PROVEEDOR	6 A – TUNELIZACION	7 D – SERVIDOR	8 C – ANCHODEBANDA

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar Tunelización, Protocolo y Ancho de banda 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.

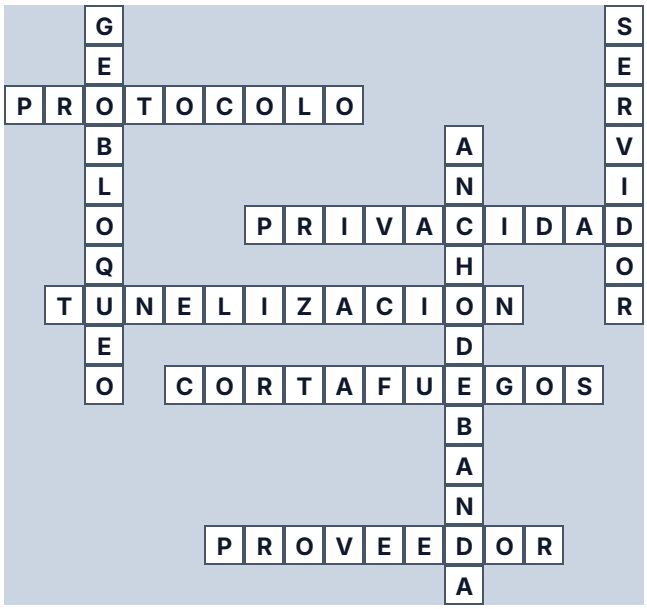
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

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

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

3 horizontal: PROTOCOLO Conjunto de reglas que determina cómo se transmiten los datos por la red (9 letras)

5 horizontal: PRIVACIDAD Estado de estar libre de rastreo o de vigilancia pública (10 letras)

6 horizontal: TUNELIZACION Encapsulación de paquetes de datos dentro de otro paquete para transportarlos de forma segura (12 letras)

7 horizontal: CORTAFUEGOS Sistema de seguridad que supervisa y bloquea el tráfico no autorizado (11 letras)

8 horizontal: PROVEEDOR Empresa que te da acceso a internet (ISP) y que registra tu tráfico si no está cifrado (9 letras)

VERTICALES

1 vertical: GEOBLOQUEO Restricción que impide el acceso web según la ubicación física (10 letras)

2 vertical: SERVIDOR Ordenador remoto que enruta tu tráfico y oculta tu IP (8 letras)

4 vertical: ANCHODEBANDA Velocidad máxima de transferencia de datos de una conexión (12 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. CIALUZITONNE — **TUNELIZACION**
2. ANODANDCBAEH — **ANCHODEBANDA**
3. GOEQELOBUO — **GEOBLOQUEO**
4. CAADVDIPRI — **PRIVACIDAD**
5. OOROCTPLO — **PROTOCOLO**
6. ORVDSIER — **SERVIDOR**
7. EACOUSGORFT — **CORTAFUEGOS**
8. REOPVREDO — **PROVEEDOR**

CLAVE DEL RETO DEL CÓDIGO SECRETO

"PROTEGE TU PRIVACIDAD CON UN TUNEL 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.