Nombre: _____ Fecha: _____ Puntuación: _____

Seguridad de Surfshark

Análisis de las funciones de seguridad de Surfshark, incluidos el bloqueo de anuncios CleanWeb, el enrutamiento dinámico MultiHop, la arquitectura SDN Nexus, la flota de servidores solo RAM y el modo Camouflage.

VISIÓN GENERAL DEL APRENDIZAJE: SEGURIDAD DE SURFSHARK

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 la arquitectura de seguridad de Surfshark. Explorarás el hardware de servidores solo en RAM, la rotación dinámica de IP de Nexus SDN, los bloqueadores de anuncios CleanWeb y el enrutamiento MultiHop.

PUNTOS DE CONTROL DE LA HOJA DE TRABAJO

- [ ] **Partes 1-4: Domina las configuraciones de VPN y de seguridad de redes.**
- [ ] **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 las mejores VPN de VPN.com

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

Tu hoja de ruta de aprendizaje sobre la seguridad de Surfshark

- Analiza la arquitectura técnica y las reglas de configuración de la seguridad de Surfshark.
- Configura los ajustes del cliente para evitar fugas de tráfico de IP, DNS y WebRTC.
- Compara los precios personalizados, la prueba y las funciones de rendimiento con los modelos estándar.

INSTRUCCIONES DE LA GUÍA DE SEGURIDAD DE SURFSHARK

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 infraestructura solo RAM, la SDN Nexus y CleanWeb. Termina con la actividad extra Piensa rápido.

FLOTA DE SERVIDORES SOLO RAM, NEXUS SDN Y ARQUITECTURA CLEANWEB (INTRODUCCIÓN)

Surfshark protege la privacidad de los usuarios con una flota de servidores que funcionan solo en RAM, la red definida por software Nexus con IP Rotator, el bloqueo de anuncios CleanWeb y rutas de cifrado Dynamic MultiHop.

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

Punto de control 1: Reto de opción múltiple

1. ¿Cómo se llama el bloqueador integrado de anuncios y malware de Surfshark?

- A) AdGuard
- B) CleanWeb
- C) ThreatShield
- D) NetBlocker

2. ¿Qué arquitectura de hardware usa Surfshark en todos sus servidores?

- A) Discos duros
- B) 100 % solo RAM
- C) Almacenamiento óptico
- D) Cinta magnética

3. ¿Qué función enruta el tráfico a través de dos servidores VPN distintos?

- A) Bypasser
- B) MultiHop (Double VPN)
- C) Red Nexus
- D) IP estática

4. ¿Qué función de ofuscación disfraza el tráfico VPN como datos web normales?

- A) Kill switch
- B) Modo camuflaje
- C) CleanWeb 2.0
- D) Túnel dividido

5. ¿Cuál es la función de la herramienta Bypasser de Surfshark?

- A) Speed Booster
- B) Túnel dividido (split tunneling)
- C) Gestor de contraseñas
- D) Resolutor DNS

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. Los servidores solo RAM borran todos los datos operativos inmediatamente al reiniciarse.

- ◯ Verdadero
- ◯ Falso

7 Pregunta 7

7. El modo camuflaje impide que los ISP detecten que estás usando una VPN.

- ◯ Verdadero
- ◯ Falso

8 Pregunta 8

8. CleanWeb 2.0 funciona dentro de extensiones del navegador para bloquear las ventanas emergentes de consentimiento de cookies.

- ◯ Verdadero
- ◯ Falso

9 Pregunta 9

9. Surfshark guarda marcas de tiempo temporales de conexión y registros de uso del ancho de banda.

- ◯ Verdadero
- ◯ Falso

10 Pregunta 10

10. La red Nexus rota periódicamente las direcciones IP de los usuarios sin desconectarlos.

- ◯ 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. Los molestos anuncios web, los scripts de rastreo y los enlaces de phishing se bloquean con los filtros _____ .
2. La actividad del usuario no deja rastro forense porque los servidores son _____ .
3. El envío de datos a través de dos saltos de servidor cifrados distintos se consigue con túneles _____ .
4. Para ocultar el uso de la VPN a los proveedores de internet, los usuarios activan el modo _____ .
5. Permitir que las apps bancarias eludan el túnel VPN se gestiona en la configuración de _____ .
6. La arquitectura SDN de nueva generación que conecta la flota de servidores es el sistema _____ .

BANCO DE PALABRAS DE VOCABULARIO

BYPASSER CAMUFLAJE CLEANWEB IP ROTATIVA KILL SWITCH MULTI-HOP NEXUS SOLO RAM

Escribe aquí tus respuestas:

1.
2.
3.
4.
5.
6.

Punto de control 4: Relación de conceptos de VPN y redes

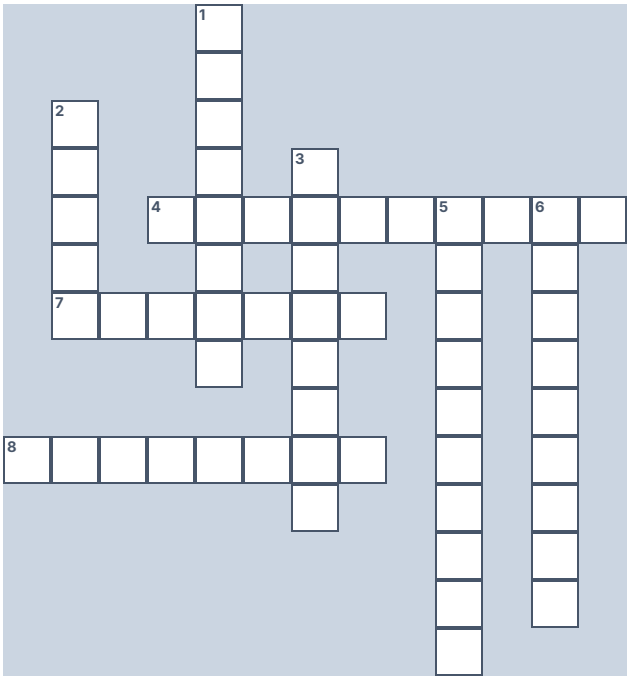
RELACIÓN DE DEFINICIONES

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. CLEANWEB	A	Una función de seguridad automática que bloquea el tráfico de red cuando la VPN se cae.
☐	2. SOLO RAM	B	Función de túnel dividido que permite que determinadas aplicaciones no pasen por la VPN.
☐	3. MULTISALTO	C	Un filtro avanzado que bloquea anuncios, malware y avisos de consentimiento de cookies.
☐	4. CAMUFLAJE	D	Hardware de servidores de memoria volátil que borra todos los datos en cada ciclo de encendido.
☐	5. HERRAMIENTA DE ELUSIÓN	E	Una función que cambia periódicamente tu dirección IP externa sin interrumpir los túneles.
☐	6. KILL SWITCH	F	Tecnología de ofuscación que oculta las firmas de la VPN para imitar el tráfico HTTPS normal.
☐	7. RED NEXUS	G	Una función de enrutamiento doble VPN que cifra el tráfico a través de dos nodos de servidor distintos.
☐	8. ROTATIVO	H	Una red propia definida por software que conecta todos los servidores en una malla unificada.

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. Función de seguridad automática que bloquea el tráfico de red cuando se cae la VPN (10)

7. Hardware de servidor con memoria volátil que borra todos los datos en cada reinicio (7)

8. Función de túnel dividido que permite que ciertas aplicaciones eludan la VPN (8)

VERTICALES

1. Función de doble VPN que cifra el tráfico a través de dos nodos de servidor distintos (8)

2. Red definida por software propia que conecta todos los servidores en una malla unificada (5)

3. Filtro avanzado que bloquea anuncios, malware y avisos de consentimiento de cookies (8)

5. Función que cambia periódicamente tu dirección IP externa sin interrumpir los túneles (10)

6. Tecnología de ofuscación que oculta las firmas de la VPN para imitar el tráfico HTTPS normal (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: Función de seguridad automática que bloquea el tráfico de red cuando se cae la VPN (10 letras):

7 horizontal: Hardware de servidor con memoria volátil que borra todos los datos en cada reinicio (7 letras):

8 horizontal: Función de túnel dividido que permite que ciertas aplicaciones eludan la VPN (8 letras):

VERTICALES

1 vertical: Función de doble VPN que cifra el tráfico a través de dos nodos de servidor distintos (8 letras):

2 vertical: Red definida por software propia que conecta todos los servidores en una malla unificada (5 letras):

3 vertical: Filtro avanzado que bloquea anuncios, malware y avisos de consentimiento de cookies (8 letras):

5 vertical: Función que cambia periódicamente tu dirección IP externa sin interrumpir los túneles (10 letras):

6 vertical: Tecnología de ofuscación que oculta las firmas de la VPN para imitar el tráfico HTTPS normal (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.

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

LISTA DE PALABRAS DE VOCABULARIO

CLEANWEB SOLORAM MULTIHOP CAMUFLAJE BYPASSER KILLSWITCH
NEXUS IPROTATIVA

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. CLEANWEB**
- **B. SOLORAM**
- **C. MULTIHOP**
- **D. CAMUFLAJE**
- **E. BYPASSER**
- **F. KILLSWITCH**
- **G. NEXUS**
- **H. IPROTATIVA**

DEFINICIONES Y CAMPOS DE RELACIÓN

_____ 1. Tecnología de ofuscación que oculta las firmas de la VPN para imitar el tráfico HTTPS normal.

_____ 2. Función de seguridad automática que bloquea el tráfico de red cuando se cae la VPN.

_____ 3. Filtro avanzado que bloquea anuncios, malware y avisos de consentimiento de cookies.

_____ 4. Función de túnel dividido que permite que ciertas aplicaciones eludan la VPN.

_____ 5. Hardware de servidor con memoria volátil que borra todos los datos en cada reinicio.

_____ 6. Función que cambia periódicamente tu dirección IP externa sin interrumpir los túneles.

_____ 7. Función de doble VPN que cifra el tráfico a través de dos nodos de servidor distintos.

_____ 8. Red definida por software propia que conecta todos los servidores en una malla unificada.

Punto de control 7: Reto de palabras desordenadas

Ordena las letras de abajo para descubrir conceptos y términos clave de las redes privadas virtuales (VPN). Escribe tus respuestas en los campos proporcionados.

1. **EANCWLBE** _____
2. **TMPUOHIL** _____
3. **AYBSSREP** _____
4. **XSUNE** _____
5. **RMOLSAO** _____
6. **JUAALCFEM** _____
7. **ILKIWTCHSL** _____
8. **VOAAITPTIR** _____

Actividad extra: Piensa rápido

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

1	Funciones de seguridad de Surfshark			
2	Señales de que tu conexión VPN es lenta			
3	Protocolos VPN que conoces			
4	Cosas que protege el cifrado			
5	Amenazas en las redes Wi-Fi públicas			
6	Países conocidos por sus estrictas leyes de privacidad			
7	Formas de crear una contraseña segura			
8	Dispositivos en los que instalarías Surfshark			
9	Preguntas para el soporte al cliente de Surfshark			
10	Ajustes que activas para tener más seguridad			
11	Cosas que Surfshark puede ocultar a tu red			
12	Tipos de filtraciones de una VPN			
13	Datos que una VPN nunca debería guardar			
14	Palabras que describen una buena app de VPN			
15	Cosas que puede comprobar una auditoría			

Punto de control 8: Casos prácticos de VPN y redes

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

CASO PRÁCTICO 1: SORTEAR LOS FILTROS DEL CAMPUS Y DEL TRABAJO



Escenario: Un estudiante descubre que la red Wi-Fi del campus de su universidad bloquea todos los puertos estándar de OpenVPN y WireGuard.

Pregunta de debate: ¿Qué función de Surfshark permite al estudiante conectarse sin que lo detecten los administradores de la red?

CASO PRÁCTICO 2: INVESTIGACIÓN PERIODÍSTICA DE ALTO RIESGO



Escenario: Una periodista de investigación necesita protección adicional frente a la vigilancia mientras investiga registros corporativos confidenciales.

Pregunta de debate: ¿Cómo ofrece Dynamic MultiHop una privacidad superior al enrutamiento a través de un solo servidor?

Punto de control 9: Descifrar el código

Un ingeniero de redes protege los canales de enrutamiento y los túneles de los clientes. Usa la clave de letras y números de abajo para descifrar el mensaje 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

12 1 9 17 19 16 21 1 21 9 23 1 4 5

14 5 25 22 20 13 5 10 16 19 1 21 22

17 19 9 23 1 3 9 4 1 4

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 sobre las redes privadas virtuales (VPN) y la tunelización.

Q1: ¿Qué es Surfshark CleanWeb?

CleanWeb es una función de seguridad integrada que bloquea anuncios, rastreadores, malware y sitios de phishing.

Q2: ¿Qué son los servidores solo RAM?

Los servidores solo RAM funcionan con memoria volátil, lo que significa que los datos guardados en la memoria se borran cada vez que los servidores se reinician.

Q3: ¿Qué es Surfshark MultiHop?

MultiHop (Double VPN) enruta y cifra tu conexión a internet a través de dos ubicaciones de servidor diferentes.

Q4: ¿Cómo funciona el modo camuflaje (Camouflage Mode)?

El modo camuflaje ofusca el tráfico de la VPN para que tu ISP no pueda saber que estás usando una VPN.

Q5: ¿Qué es la función Bypasser?

Bypasser es la herramienta de túnel dividido de Surfshark que permite que determinadas aplicaciones o sitios web eludan la VPN.

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

Repasa las preguntas y respuestas más habituales sobre las redes privadas virtuales (VPN) y la tunelización.

Q6: ¿Tiene Surfshark un kill switch?

Sí, el Kill Switch te desconecta de internet si la VPN se cae de forma inesperada.

Q7: ¿Qué estándar de cifrado utiliza Surfshark?

Surfshark usa AES-256-GCM y ChaCha20, además de AEGIS-256X2 en su nuevo protocolo Dausos.

Q8: ¿Se ha auditado la política de no registros de Surfshark?

Sí, Deloitte verificó la política de no registros de Surfshark en 2023 y de nuevo en 2025.

Q9: ¿Qué es Surfshark Nexus?

Nexus es una arquitectura SDN avanzada que conecta todos los servidores en una red unificada para lograr un enrutamiento más fluido.

Q10: ¿Qué es la función IP Rotator?

IP Rotator cambia automáticamente tu dirección IP cada pocos minutos sin desconectar tu sesión VPN.

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

Explora aspectos técnicos avanzados de los protocolos de tunelización VPN, las integraciones con clientes móviles y el despliegue empresarial.

Q1: ¿En qué se diferencia Dynamic MultiHop de la doble VPN tradicional?

Dynamic MultiHop te permite personalizar cualquier combinación de servidores de entrada y salida de todo el mundo.

Q2: ¿Funciona CleanWeb 2.0 en las extensiones del navegador?

Sí, CleanWeb 2.0 bloquea los anuncios en vídeo, las ventanas emergentes de consentimiento de cookies y los banners de alerta en Chrome/Firefox.

Q3: ¿Qué es Alternative ID en la suite de seguridad?

Alternative ID genera seudónimos personales únicos, direcciones de correo electrónico y máscaras de teléfono.

Q4: ¿Cómo evita Surfshark las fugas de DNS?

Surfshark enruta todas las solicitudes de dominio a través de sus propios servidores DNS privados en cada nodo.

Q5: ¿Admite Surfshark el cifrado ChaCha20 en el móvil?

Sí, WireGuard en Android e iOS usa ChaCha20-Poly1305 para lograr una mayor eficiencia en dispositivos móviles.

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

Explora aspectos técnicos avanzados de los protocolos de tunelización VPN, las integraciones con clientes móviles y el despliegue empresarial.

Q6: ¿Qué es el modo NoBorders en Surfshark?

NoBorders detecta automáticamente los entornos de red restrictivos y proporciona servidores especializados.

Q7: ¿Quién realizó las auditorías de seguridad de las extensiones de navegador de Surfshark?

La empresa de ciberseguridad independiente Cure53 completó auditorías de las extensiones de navegador y de los sistemas de servidores.

Q8: ¿Cómo protege Surfshark contra las fugas de IPv6?

Surfshark enruta el tráfico IPv6 de forma segura o lo restringe de forma segura para evitar cualquier fuga sin cifrar.

Q9: ¿Dónde se encuentra la jurisdicción legal de Surfshark?

Surfshark se rige por la legislación de los Países Bajos y cumple las estrictas normas europeas de privacidad del RGPD (GDPR).

Q10: ¿Surfshark admite la autenticación de dos factores (2FA)?

Sí, y Surfshark One añade un bloqueo con 2FA para que solo tú puedas cambiar los ajustes de las funciones.

Parte 11: 10 datos reales sobre las VPN y su aplicación

Repasa datos reales sobre velocidades de cifrado de VPN, auditorías de protocolos, conectividad móvil y teletrabajo en empresas.

1. PERSPECTIVA SOBRE VPN

1. Surfshark afirma que toda su red de más de 4,500 servidores funciona con hardware sin disco que usa solo memoria RAM volátil.

2. PERSPECTIVA SOBRE VPN

2. Deloitte, firma de las Big Four, verificó la política de no registros de Surfshark en 2023 y de nuevo en noviembre de 2025.

3. PERSPECTIVA SOBRE VPN

3. La arquitectura propietaria Nexus conecta todos los servidores del mundo en una red dinámica definida por software.

4. PERSPECTIVA SOBRE VPN

4. Rotating IP cambia tu dirección IP aproximadamente cada cinco minutos sin interrumpir la conexión VPN.

5. PERSPECTIVA SOBRE VPN

5. CleanWeb 2.0 bloquea los molestos avisos de consentimiento de cookies y los anuncios de vídeo directamente en los navegadores.

6. PERSPECTIVA SOBRE VPN

6. Dynamic MultiHop permite a los usuarios crear rutas de cifrado personalizadas de doble servidor en 100 países.

7. PERSPECTIVA SOBRE VPN

7. El modo Camuflaje elimina las firmas de las cabeceras VPN, de modo que el tráfico no se distingue del HTTPS normal.

8. PERSPECTIVA SOBRE VPN

8. Alternative ID genera seudónimos desechables y alias de correo electrónico para proteger a los usuarios de las filtraciones de bases de datos.

9. PERSPECTIVA SOBRE VPN

9. Surfshark aplica el cifrado simétrico AES-256-GCM junto con ChaCha20 en los protocolos WireGuard.

10. PERSPECTIVA SOBRE VPN

10. El modo NoBorders se activa automáticamente en redes restringidas para ofrecer un acceso por túnel resistente.

Referencias técnicas y fuentes

La guía de estudio y los pasatiempos interactivos se han elaborado a partir de estándares técnicos, especificaciones y marcos normativos internacionales.

REFERENCIAS ACADÉMICAS Y DEL SECTOR

[1] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

Clave de respuestas: Punto de control 1 – Opción múltiple

1 **Bloqueador de contenido integrado** DEFENSA CONTRA ANUNCIOS Y MALWARE — **Respuesta correcta: B**

NOTA PARA DOCENTES

CleanWeb es el filtro de seguridad integrado de Surfshark que bloquea anuncios, dominios de rastreo, sitios web de phishing y scripts de URL maliciosos a nivel de red. Cita: CleanWeb Security Specs.

2 **Infraestructura 100 % solo RAM** ARQUITECTURA RAM — **Respuesta correcta: B**

NOTA PARA DOCENTES

Surfshark usa servidores solo en RAM, por lo que los datos guardados en la memoria del servidor se borran cuando el servidor se apaga o se reinicia. Fuente: Cure53 Infrastructure Audit.

3 **Doble tunelización MultiHop** VPN MULTISALTO — **Respuesta correcta: B**

NOTA PARA DOCENTES

MultiHop (Double VPN) cifra el tráfico a través de dos nodos de servidor distintos en países diferentes para evitar ataques de correlación de tráfico. Cita: Surfshark MultiHop Guide.

4 **Ofuscación con el modo camuflaje** OFUSCACIÓN — **Respuesta correcta: B**

NOTA PARA DOCENTES

El modo camuflaje modifica las cabeceras de los paquetes de OpenVPN para disfrazar el tráfico de la VPN como tráfico HTTPS estándar, lo que permite sortear los bloqueos de cortafuegos restrictivos. Cita: Surfshark Stealth Whitepaper.

5 **Túnel dividido Bypasser** TUNELIZACIÓN DIVIDIDA — **Respuesta correcta: B**

NOTA PARA DOCENTES

Bypasser es la herramienta de túnel dividido de Surfshark que permite a los usuarios seleccionar aplicaciones o sitios web concretos para enrutarlos directamente a través de su conexión habitual del ISP. Cita: Surfshark Client Features.

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

6 **Borrado de datos de la memoria volátil** — SEGURIDAD DEL SERVIDOR — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Los servidores solo RAM no almacenan ningún dato en discos duros permanentes; reiniciar el hardware purga de inmediato toda la memoria operativa. Cita: RAM Server Architecture.

7 **Ocultación ante el ISP con el modo camuflaje** — OCULTACIÓN DEL TRÁFICO — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

El modo camuflaje elimina las firmas del protocolo OpenVPN, lo que impide que los ISP detecten que el usuario está conectado a un túnel VPN. Cita: Deep Packet Inspection Guide.

8 **Extensiones de navegador de CleanWeb 2.0** — EXTENSIÓN DEL NAVEGADOR — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

CleanWeb 2.0 funciona dentro de extensiones del navegador para bloquear en tiempo real ventanas emergentes de consentimiento de cookies, anuncios en vídeo y scripts de redirección maliciosos. Cita: CleanWeb 2.0 Release Notes.

9 **Cero retención de registros de conexión** — POLÍTICA DE NO REGISTROS — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Surfshark mantiene una estricta política de cero registros auditada de forma independiente: no registra direcciones IP, marcas de tiempo de conexión ni registros de ancho de banda. Fuente: Deloitte No-Logs Audit.

10 **Rotación dinámica de IP de Nexus** — RED NEXUS — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

La red definida por software Nexus de Surfshark rota dinámicamente las direcciones IP de los usuarios cada pocos minutos sin cortar la conexión VPN activa. Cita: Surfshark Nexus Architecture.

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

C 1. CLEANWEB	D 2. SOLO RAM	G 3. MULTISALTO	F 4. CAMUFLAJE
B 5. HERRAMIENTA DE ELUSIÓN	A 6. KILL SWITCH	H 7. RED NEXUS	E 8. ROTATIVO

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 CLEANWEB	2 SOLO RAM	3 MULTI-HOP	4 CAMUFLAJE
5 BYPASSER	6 NEXUS		

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

1 D – CAMUFLAJE	2 F – KILLSWITCH	3 A – CLEANWEB	4 E – BYPASSER
5 B – SOLORAM	6 H – IPROTATIVA	7 C – MULTIHOP	8 G – NEXUS

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar CLEANWEB, SOLO RAM y MULTISALTO 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.

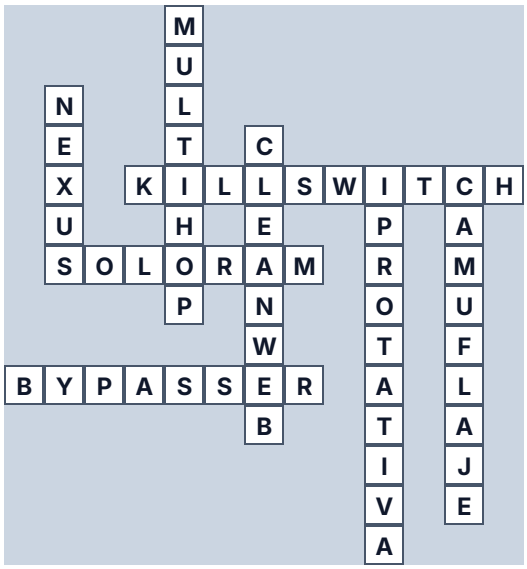
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

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

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

4 horizontal: KILLSWITCH Función de seguridad automática que bloquea el tráfico de red cuando se cae la VPN (10 letras)

7 horizontal: SOLORAM Hardware de servidor con memoria volátil que borra todos los datos en cada reinicio (7 letras)

8 horizontal: BYPASSER Función de túnel dividido que permite que ciertas aplicaciones eludan la VPN (8 letras)

VERTICALES

1 vertical: MULTIHOP Función de doble VPN que cifra el tráfico a través de dos nodos de servidor distintos (8 letras)

2 vertical: NEXUS Red definida por software propia que conecta todos los servidores en una malla unificada (5 letras)

3 vertical: CLEANWEB Filtro avanzado que bloquea anuncios, malware y avisos de consentimiento de cookies (8 letras)

5 vertical: IPROTATIVA Función que cambia periódicamente tu dirección IP externa sin interrumpir los túneles (10 letras)

6 vertical: CAMUFLAJE Tecnología de ofuscación que oculta las firmas de la VPN para imitar el tráfico HTTPS normal (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. E A N C W L B E — **CLEANWEB**
2. T M P U O H I L — **MULTIHOP**
3. A Y B S S R E P — **BYPASSER**
4. X S U N E — **NEXUS**
5. R M O L S A O — **SOLORAM**
6. J U A A L C F E M — **CAMUFLAJE**
7. I L K I W T C H S L — **KILLSWITCH**
8. V O A A I T P T I R — **IPROTATIVA**

CLAVE DEL RETO DEL CÓDIGO SECRETO

"LA IP ROTATIVA DE NEXUS MEJORA TU PRIVACIDAD"

Clave de respuestas de los casos prácticos

A CASO PRÁCTICO 1: SORTEAR LOS FILTROS DEL CAMPUS Y DEL TRABAJO

Solución para docentes

RÚBRICA DE CALIFICACIÓN Y PAUTAS DE SOLUCIÓN

- Análisis del escenario: una estudiante descubre que la wifi del campus universitario bloquea todos los puertos estándar de OpenVPN y WireGuard.
- Pregunta clave: ¿Qué función de Surfshark permite al estudiante conectarse sin que los administradores de red lo detecten?
- Estrategia y solución recomendadas: activar el modo camuflaje (Camouflage Mode) (OpenVPN), que oculta los metadatos de la VPN para que los cortafuegos vean una navegación HTTPS normal.

B CASO PRÁCTICO 2: INVESTIGACIÓN PERIODÍSTICA DE ALTO RIESGO

Solución para docentes

RÚBRICA DE CALIFICACIÓN Y PAUTAS DE SOLUCIÓN

- Análisis de escenario: Un periodista de investigación necesita protección adicional contra la vigilancia mientras investiga registros corporativos confidenciales.
- Pregunta clave: ¿Por qué Dynamic MultiHop ofrece más privacidad que el enrutamiento a través de un solo servidor?
- Estrategia y solución recomendadas: Dynamic MultiHop enruta el tráfico a través de servidores de entrada y de salida en dos países, de modo que ningún servidor por sí solo puede exponer al usuario.