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

Guía de la VPN más segura

Análisis técnico del diseño de VPN de alta seguridad: servidores solo en memoria RAM volátil, seguridad de acceso Zero Trust, defensas contra fugas con DNS privado cifrado y configuraciones de WireGuard auditadas.

RESUMEN DE APRENDIZAJE: GUÍA DE LA VPN MÁS SEGURA

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 estándares técnicos de las VPN de alta seguridad. Explorarás el hardware de servidores solo RAM, la seguridad de acceso de confianza cero, los resolvedores DNS privados y cifrados y las configuraciones de WireGuard auditadas.

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/vpn-mas-seguro/

Tu hoja de ruta de aprendizaje sobre la VPN más segura

- Analiza la arquitectura técnica y los estándares de cifrado que se tratan en la guía de las VPN más seguras.
- Configura los ajustes del cliente para evitar fugas de tráfico de IP, DNS y WebRTC.
- Compara los protocolos de tunelización propietarios con las implementaciones estándar.

INSTRUCCIONES DE LA GUÍA DE LA VPN MÁS SEGURA

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 el hardware de servidores solo RAM y los sistemas de confianza cero (Zero Trust). Termina con la actividad extra Piensa rápido.

INFRAESTRUCTURAS SOLO RAM Y REDES DE CONFIANZA CERO (INTRODUCCIÓN)

Una VPN realmente segura se basa en un marco Zero Trust, servidores solo RAM que impiden que la incautación de discos exponga registros, resolutores DNS privados cifrados y protocolos auditados como WireGuard. En conjunto, estos controles defienden los activos digitales de alto valor frente a las amenazas de interceptación.

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

Punto de control 1: Reto de opción múltiple

1. ¿Qué arquitectura es fundamental para garantizar la máxima seguridad en los servidores VPN modernos?

- A) Infraestructura de servidores solo RAM
- B) Almacenamiento en disco
- C) Enrutamiento de DNS dinámico
- D) Activación del reenvío de puertos

2. ¿Qué protocolo se recomienda ampliamente para las configuraciones de VPN más seguras y modernas?

- A) WireGuard
- B) PPTP
- C) L2TP/IPSec
- D) SSTP

3. ¿Qué marco de seguridad exige verificar continuamente cada conexión sin excepción?

- A) Arquitectura Zero Trust
- B) Cortafuegos perimetrales
- C) Enrutamiento dinámico
- D) Claves secretas compartidas

4. ¿Cuál es la función principal de la protección contra fugas de DNS de un cliente VPN?

- A) Enrutar todas las solicitudes DNS a través de resolutores privados cifrados
- B) Ofuscar los paquetes IP
- C) Almacenar en caché las consultas DNS localmente
- D) Desactivar los servidores de nombres

5. ¿Cómo aumenta el enrutamiento multisalto (Multi-Hop) la seguridad general de un túnel VPN?

- A) Enruta los datos a través de dos servidores distintos en serie
- B) Aumenta la velocidad de compresión
- C) Cifra los datos con cifrados de baja seguridad
- D) Sortea los cortafuegos

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. Los servidores solo RAM almacenan los archivos de registro en memoria efímera, que se borra al reiniciar.

- ○ Verdadero
- ○ Falso

7 Pregunta 7

7. WireGuard usa algoritmos criptográficos modernos que son menos propensos a provocar cuellos de botella de velocidad.

- ○ Verdadero
- ○ Falso

8 Pregunta 8

8. Un kill switch de VPN funciona bloqueando todo el tráfico de red si el túnel se cae.

- ○ Verdadero
- ○ Falso

9 Pregunta 9

9. Las auditorías independientes de terceros son irrelevantes para verificar los compromisos de seguridad.

- ○ Verdadero
- ○ Falso

10 Pregunta 10

10. Los modelos de confianza cero asumen que todas las conexiones de la red interna son seguras de forma predeterminada.

- ○ 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 administradores refuerzan la seguridad desplegando un marco estricto de _____ .

2. Enviar los paquetes a través de varios puntos de entrada requiere una configuración _____ segura.

3. Para evitar fugas de datos por robo de discos, usamos un diseño de _____ .

4. El secuestro por parte del ISP se mitiga configurando funciones nativas de _____ .

5. Para bloquear el tráfico durante los fallos de conexión, activa el mecanismo _____ .

6. Para minimizar los registros almacenados en bases de datos, elige un proveedor totalmente _____ .

BANCO DE PALABRAS DE VOCABULARIO

AUDITADO CIFRADO CONFIANZA CERO KILL SWITCH MULTI-HOP
PROTECCIÓN DNS PROTOCOLO SERVIDOR RAM

Escribe aquí tus respuestas:

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

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

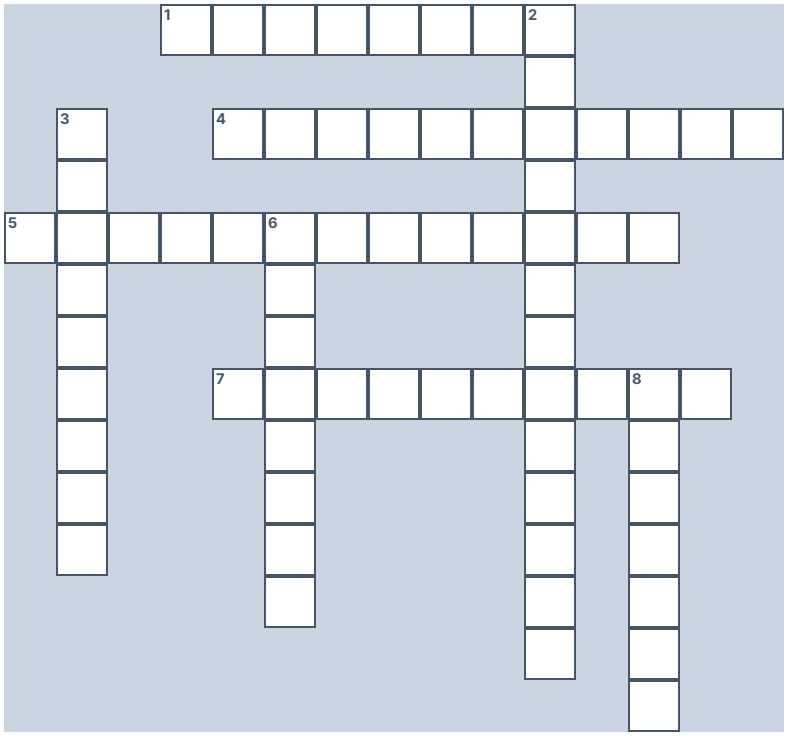
RELACIÓN DE DEFINICIONES

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. Confianza cero	A	Configuración inspeccionada de forma independiente que confirma que no se almacena ningún registro.
☐	2. Multisalto	B	Codificación criptográfica de la carga útil de datos para proteger el tránsito.
☐	3. Servidor solo RAM	C	Marco de seguridad que exige la autenticación continua de todos los usuarios.
☐	4. Protección de DNS	D	Conjunto de reglas técnicas que determinan cómo se empaquetan y envían los datos.
☐	5. Kill switch	E	Enrutamiento de VPN en cascada que encadena dos nodos de servidor.
☐	6. Sistema auditado	F	Arquitectura de servidor que usa memoria volátil para almacenar las cargas de datos.
☐	7. Cifrado	G	Forzar consultas DNS privadas para proteger las búsquedas en los servidores de nombres.
☐	8. Protocolo	H	Mecanismo a prueba de fallos que bloquea el tráfico si la VPN falla.

Punto de control 5: Crucigrama

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



HORIZONTALES

1. Enrutamiento VPN en cascada que encadena dos nodos de servidor (8)

4. Arquitectura de servidor que usa memoria volátil para almacenar las cargas de datos (11)

5. Marco de seguridad que exige la autenticación continua de todos los usuarios (13)

7. Mecanismo de seguridad que bloquea el tráfico si la VPN falla (10)

VERTICALES

2. Uso obligatorio de consultas DNS privadas para proteger las búsquedas en los servidores de nombres (13)

3. Conjunto de reglas técnicas que determina cómo se empaquetan y envían los datos (9)

6. Configuración inspeccionada de forma independiente que confirma que no se almacenan registros (8)

8. Codificación criptográfica de las cargas de datos para protegerlas en tránsito (7)

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

1 horizontal: Enrutamiento VPN en cascada que encadena dos nodos de servidor (8 letras):

4 horizontal: Arquitectura de servidor que usa memoria volátil para almacenar las cargas de datos (11 letras):

5 horizontal: Marco de seguridad que exige la autenticación continua de todos los usuarios (13 letras):

7 horizontal: Mecanismo de seguridad que bloquea el tráfico si la VPN falla (10 letras):

VERTICALES

2 vertical: Uso obligatorio de consultas DNS privadas para proteger las búsquedas en los servidores de nombres (13 letras):

3 vertical: Conjunto de reglas técnicas que determina cómo se empaquetan y envían los datos (9 letras):

6 vertical: Configuración inspeccionada de forma independiente que confirma que no se almacenan registros (8 letras):

8 vertical: Codificación criptográfica de las cargas de datos para protegerlas en tránsito (7 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 E R V I D O R R A M R Y B H
N M Z G P O H I T L U M K Ñ C
D P Ñ W C M Z Y G Y O W U I L
N U P B Ñ V T M H U D Y F U K
O H C T I W S L L I K R R B W
I Z Y M R Q X I O D A A D K Q
C V W W L J I T I D G B F I L
C T R V Q Z E I O F R C A L P
E C Z M K V R U A S W K M M H
T H N I O D A T I D U A Q G L
O C O N F I A N Z A C E R O T
R L R W H B U F Y Ñ Y W S H T
P X P R O T O C O L O A P U Ñ
Ñ Z O I P T I O U U O U T K A
E O N L A Ñ V G G P Q X Y K K

LISTA DE PALABRAS DE VOCABULARIO

CONFIANZACERO MULTIHOP SERVIDORRAM PROTECCIONDNS KILLSWITCH
AUDITADO CIFRADO PROTOCOLO

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. CONFIANZACERO**
- **B. MULTIHOP**
- **C. SERVIDORRAM**
- **D. PROTECCIONDNS**
- **E. KILLSWITCH**
- **F. AUDITADO**
- **G. CIFRADO**
- **H. PROTOCOLO**

DEFINICIONES Y CAMPOS DE RELACIÓN

_____ 1. Mecanismo de seguridad que bloquea el tráfico si la VPN falla.

_____ 2. Uso obligatorio de consultas DNS privadas para proteger las búsquedas en los servidores de nombres.

_____ 3. Enrutamiento VPN en cascada que encadena dos nodos de servidor.

_____ 4. Conjunto de reglas técnicas que determina cómo se empaquetan y envían los datos.

_____ 5. Codificación criptográfica de las cargas de datos para protegerlas en tránsito.

_____ 6. Arquitectura de servidor que usa memoria volátil para almacenar las cargas de datos.

_____ 7. Configuración inspeccionada de forma independiente que confirma que no se almacenan registros.

_____ 8. Marco de seguridad que exige la autenticación continua de todos los usuarios.

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. NNARAOZCCE OIF
2. IMESADRRRO V
3. KWCIISHLTL
4. OIARDCF
5. IHUPTMOL
6. ENCCDONOPR IST
7. AOTADUID
8. OOLPTRCOO

Actividad extra: Piensa rápido

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

1	Cerraduras o llaves que usas todos los días			
2	Cosas que una VPN puede ocultar			
3	Cosas que hacen que una VPN sea segura			
4	Mitos sobre las VPN			
5	Razones para usar una VPN cuando viajas			
6	Lugares seguros del mundo real			
7	Palabras que significan 'protegido'			
8	Promesas que hace un buen proveedor de VPN			
9	Palabras relacionadas con la privacidad			
10	Tipos de auditoría o inspección			
11	Palabras de esta hoja de trabajo que quieres recordar			
12	Cosas que un hacker quiere robar			
13	Formas de detectar una red Wi-Fi falsa			
14	Lugares en los que usarías una VPN			
15	Cosas que puede ver tu proveedor de internet			

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: REFUERZO DE LA INFRAESTRUCTURA EMPRESARIAL



Escenario: Un banco corporativo está rediseñando su topología de acceso remoto. Necesita una arquitectura Zero Trust que conecte todos los dispositivos cliente con servidores seguros.

Pregunta de debate: ¿Cuál es la principal ventaja de la microsegmentación de la red en un modelo de VPN Zero Trust?

CASO PRÁCTICO 2: PROTECCIONES DE LOS SERVIDORES SOLO RAM



Escenario: Un proveedor de VPN centrado en la seguridad está actualizando sus servidores para evitar que la incautación física de un servidor exponga los historiales de registros de los usuarios.

Pregunta de debate: Explica cómo las configuraciones de hardware solo RAM impiden la extracción forense de datos durante las incautaciones físicas de servidores.

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	20	23	17	14	20	5	7	22	19	1	20

17	19	16	21	5	7	5	14	1	3	21	9	23	16	20

23	1	12	9	16	20	16	20

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 hace que una VPN sea «la más segura»?

Una combinación de Zero Trust, servidores solo RAM y protocolos auditados.

Q2: ¿Qué son los servidores solo RAM?

Servidores que funcionan en memoria volátil, diseñados para no almacenar registros en disco.

Q3: ¿Qué es una VPN de confianza cero (Zero Trust)?

Un marco que verifica de forma continua cada solicitud de acceso y cada conexión.

Q4: ¿Por qué se considera seguro WireGuard?

Tiene una base de código pequeña y fácil de auditar, y utiliza cifrados modernos.

Q5: ¿Cómo evitan las VPN seguras las fugas de DNS?

Enrutando todas las consultas a través de resolutores DNS privados y cifrados.

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: ¿Requiere auditorías una VPN segura?

Sí, las auditorías independientes verifican las afirmaciones de no registros y la seguridad del código.

Q7: ¿Qué papel desempeña un kill switch?

Detiene inmediatamente el tráfico de red si se cae la conexión VPN.

Q8: ¿Qué cifrado se utiliza en las VPN seguras?

AES-256 y ChaCha20 son los estándares del sector en materia de cifrado.

Q9: ¿Es seguro el enrutamiento Multi-Hop?

Sí, encadena dos o más servidores para evitar el análisis del tráfico.

Q10: ¿Cómo ayuda una jurisdicción extraterritorial?

Puede limitar qué leyes se aplican, pero no ofrece inmunidad absoluta.

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: ¿Cómo evitan los servidores solo RAM los riesgos de incautación de datos?

Como funcionan en RAM, desenchufarlos borra los datos que hay en la memoria.

Q2: ¿Cómo sustituye Zero Trust a la seguridad perimetral estándar?

Trata a cada cliente como hostil y exige una autenticación continua.

Q3: ¿Qué hace que el código base de WireGuard sea más fácil de auditar?

Su código para Linux tiene menos de 4.000 líneas, mucho menos que las pilas VPN habituales. [4]

Q4: ¿Cómo protege DNSSEC las consultas DNS?

Firma los registros DNS para que los resolutores puedan detectar respuestas falsificadas o manipuladas.

Q5: ¿Cómo dificulta Multi-Hop la correlación del tráfico?

Separando las IP de entrada y de salida entre distintos proveedores de alojamiento.

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: ¿Por qué las jurisdicciones de los Cinco Ojos (Five Eyes) son arriesgadas para las VPN?

Los Estados miembros comparten inteligencia y pueden recurrir a órdenes judiciales para solicitar datos de los usuarios.

Q7: ¿Cómo se implementa un kill switch a nivel del kernel?

Utiliza reglas del cortafuegos del sistema (como iptables o WFP) para bloquear el tráfico de salida.

Q8: ¿Qué es el secreto hacia adelante en los protocolos de enlace (handshakes) de las VPN?

Genera claves de sesión únicas para que las sesiones anteriores no puedan descifrarse.

Q9: ¿Cómo mitigan las VPN seguras las fugas de WebRTC?

Bloqueando las solicitudes WebRTC o enrutándolas a través del túnel.

Q10: ¿Cómo garantizan las auditorías independientes el cumplimiento en materia de privacidad?

Los auditores realizan pruebas de penetración e inspeccionan las configuraciones de los servidores.

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

Los servidores solo RAM cargan su sistema operativo en la memoria al arrancar, por lo que nada persiste en el disco tras un reinicio.

2. PERSPECTIVA SOBRE VPN

WireGuard usa el marco Noise con Curve25519, ChaCha20, Poly1305, BLAKE2s y HKDF. [3]

3. PERSPECTIVA SOBRE VPN

La confianza cero concede el acceso por recurso y no otorga ninguna confianza implícita en función de la ubicación en la red (NIST SP 800-207). [1]

4. PERSPECTIVA SOBRE VPN

La alianza de inteligencia Cinco Ojos incluye a EE. UU., Reino Unido, Canadá, Australia y Nueva Zelanda.

5. PERSPECTIVA SOBRE VPN

Las fugas de WebRTC se producen cuando los navegadores revelan la dirección IP pública real del cliente mediante consultas STUN.

6. PERSPECTIVA SOBRE VPN

El secreto perfecto hacia adelante (PFS) garantiza que el compromiso de una clave a largo plazo no exponga las claves de sesiones anteriores. [3]

7. PERSPECTIVA SOBRE VPN

Cure53, una empresa de seguridad con sede en Berlín, ha publicado auditorías de varios proveedores de VPN.

8. PERSPECTIVA SOBRE VPN

Las fugas de DNS se producen cuando las consultas DNS eluden el túnel VPN y van a los servidores de nombres del ISP local.

9. PERSPECTIVA SOBRE VPN

Los chips de RAM volátil necesitan alimentación eléctrica constante para conservar los datos y pierden su contenido al apagarse.

10. PERSPECTIVA SOBRE VPN

Los sistemas empresariales de confianza cero imponen comprobaciones del estado del dispositivo antes de permitir la conexión a recursos protegidos. [1]

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] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

Clave de respuestas: Punto de control 1 – Opción múltiple

1 **Servidor solo RAM** SOLO RAM — **Respuesta correcta: A**

NOTA PARA DOCENTES

Los servidores solo RAM no almacenan registros en disco y borran los datos al reiniciar. Cita: Most Secure VPN.

2 **Pregunta 2** — **Respuesta correcta: A**

NOTA PARA DOCENTES

WireGuard combina una base de código pequeña y auditable con cifrados modernos.

3 **Modelo de confianza cero** CONFIANZA CERO — **Respuesta correcta: A**

NOTA PARA DOCENTES

Los modelos de confianza cero verifican continuamente el cumplimiento de los dispositivos antes de conceder el acceso. Cita: Most Secure VPN.

4 **Protección de DNS** PROTECCIÓN DE DNS — **Respuesta correcta: A**

NOTA PARA DOCENTES

La protección contra fugas de DNS dirige las consultas de resolución a través de resolutores privados. Cita: Most Secure VPN.

5 **Túneles multisalto** MULTISALTO — **Respuesta correcta: A**

NOTA PARA DOCENTES

El enrutamiento multisalto encadena dos nodos de servidor distintos en serie. Cita: Most Secure VPN.

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

6 **Servidor solo RAM** SOLO RAM — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

El hardware de servidor solo RAM no escribe datos en disco y se borra al reiniciar. Cita: Most Secure VPN.

7 **Velocidad de WireGuard** WIREGUARD — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

WireGuard usa criptografía moderna que evita los cuellos de botella de procesamiento. Cita: Most Secure VPN.

8 **Kill switch** INTERRUPTOR DE SEGURIDAD — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Un kill switch bloquea todo el tráfico si la conexión VPN se cae. Cita: Most Secure VPN.

9 **Auditorías de terceros** AUDITORÍAS ESENCIALES — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Las auditorías de terceros son esenciales para verificar las afirmaciones de privacidad de las empresas. Cita: Most Secure VPN.

10 **Pregunta 10** — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Zero Trust no concede confianza implícita en función de la ubicación en la red. [1]

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. Confianza cero	E 2. Multisalto	F 3. Servidor solo RAM	G 4. Protección de DNS
H 5. Kill switch	A 6. Sistema auditado	B 7. Cifrado	D 8. Protocolo

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 CONFIANZA CERO	2 MULTI-HOP	3 SERVIDOR RAM	4 PROTECCIÓN DNS
5 KILL SWITCH	6 AUDITADO		

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

1 E – KILLSWITCH	2 D – PROTECCIONDNS	3 B – MULTIHOP	4 H – PROTOCOLO
5 G – CIFRADO	6 C – SERVIDORRAM	7 F – AUDITADO	8 A – CONFIANZACERO

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar Confianza cero, Multisalto y Servidor solo RAM 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.

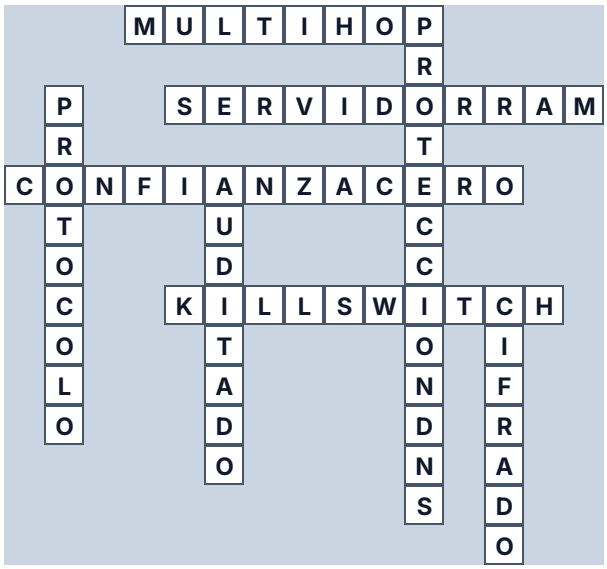
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

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

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

1 horizontal: MULTIHOP Enrutamiento VPN en cascada que encadena dos nodos de servidor (8 letras)

4 horizontal: SERVIDORRAM Arquitectura de servidor que usa memoria volátil para almacenar las cargas de datos (11 letras)

5 horizontal: CONFIANZACERO Marco de seguridad que exige la autenticación continua de todos los usuarios (13 letras)

7 horizontal: KILLSWITCH Mecanismo de seguridad que bloquea el tráfico si la VPN falla (10 letras)

VERTICALES

2 vertical: PROTECCIONDNS Uso obligatorio de consultas DNS privadas para proteger las búsquedas en los servidores de nombres (13 letras)

3 vertical: PROTOCOLO Conjunto de reglas técnicas que determina cómo se empaquetan y envían los datos (9 letras)

6 vertical: AUDITADO Configuración inspeccionada de forma independiente que confirma que no se almacenan registros (8 letras)

8 vertical: CIFRADO Codificación criptográfica de las cargas de datos para protegerlas en tránsito (7 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.	NNARAOZCCEOIF	CONFIANZACERO	5.	IHUPTMOL	MULTIHOP
2.	IMESADRRROV	SERVIDORRAM	6.	ENCCDONOPRIST	PROTECCIONDNS
3.	KWCIISHLTL	KILLSWITCH	7.	AOTADUID	AUDITADO
4.	OIARDCF	CIFRADO	8.	OOLPTRCOO	PROTOCOLO

CLAVE DEL RETO DEL CÓDIGO SECRETO

"LAS VPN SEGURAS PROTEGEN ACTIVOS VALIOSOS"

Clave de respuestas de los casos prácticos

A CASO PRÁCTICO 1: REFUERZO DE LA INFRAESTRUCTURA EMPRESARIAL

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: un banco corporativo está rediseñando su topología de acceso remoto. Necesita una arquitectura de confianza cero que conecte todos los dispositivos cliente con servidores seguros.
- Estrategia y solución recomendadas: Pautas de evaluación: explicar que la microsegmentación limita el acceso a recursos concretos, lo que impide el movimiento lateral de amenazas si un dispositivo se ve comprometido.

B CASO PRÁCTICO 2: PROTECCIONES DE LOS SERVIDORES SOLO RAM

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: un proveedor de VPN centrado en la seguridad está actualizando sus servidores para evitar que una incautación física exponga el historial de registros de los usuarios.
- Estrategia y solución recomendadas: Pautas de evaluación: detallar que los servidores solo RAM carecen de almacenamiento físico en disco. Un corte de corriente borra automáticamente todos los datos efímeros de la memoria volátil.