Nombre: _____ Fecha: _____ Puntuación: _____

WireGuard frente a OpenVPN Hoja de trabajo

Comparación de los protocolos WireGuard y OpenVPN, el tamaño de su código, su velocidad y sus estándares criptográficos

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

- Compara la complejidad del código y la velocidad de auditoría de los protocolos.
- Analiza las mejoras de rendimiento de ejecutarse en el espacio del kernel.
- Contrasta los cifrados de OpenSSL con la criptografía moderna de WireGuard.
- Configurar pares de claves pública y privada para el handshake entre pares.
- Enruta el tráfico VPN a través de los puertos TCP y UDP del cortafuegos.

INSTRUCCIONES DE LA HOJA DE COMPARACIÓN DE PROTOCOLOS

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 auditoría de protocolos modernos. Termina con la actividad extra Piensa rápido.

WIREGUARD FRENTE A OPENVPN (INTRODUCCIÓN)

Elegir un protocolo VPN requiere equilibrar la velocidad y las opciones de configuración. OpenVPN ha sido el estándar durante décadas y ofrece flexibilidad de configuración TCP/UDP. WireGuard es un sustituto moderno que se ejecuta directamente en el espacio del kernel con solo 4,000 líneas de código. Entender las diferencias entre protocolos es clave para optimizar tus redes seguras.

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

Punto de control 1: Reto de opción múltiple

1. ¿Cuál es el tamaño aproximado del código base del protocolo WireGuard?

- A. Unas 70.000 líneas
- B. Más de 100,000 líneas
- C. Menos de 1,000 líneas
- D. Unas 4,000 líneas

2. ¿En qué espacio del sistema operativo se ejecuta WireGuard?

- A. Espacio de usuario
- B. Espacio del kernel
- C. Espacio de aplicación
- D. Espacio virtual

3. ¿En qué biblioteca criptográfica se basa principalmente OpenVPN?

- A. ChaCha20-Poly1305
- B. Biblioteca criptográfica OpenSSL
- C. Marco de protocolo Noise
- D. Codificación DES en texto plano

4. ¿Qué ventaja clave de rendimiento tiene WireGuard frente a OpenVPN?

- A. Negociaciones de conexión más rápidas y menor latencia
- B. Evitando la necesidad de direcciones IP públicas
- C. Compatibilidad nativa integrada con el acceso telefónico antiguo
- D. Ninguna sobrecarga de batería en los dispositivos móviles

5. ¿Cómo autentica WireGuard las conexiones entre pares?

- A. Intercambiando contraseñas de usuario estándar
- B. Verificando los certificados de registro del dominio
- C. Usando pares de claves públicas y privadas estáticas
- D. Comprobando los números de serie del hardware

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. El código base compacto de WireGuard hace que sea mucho más fácil de auditar.

- ○ Verdadero
- ○ Falso

7 Pregunta 7

7. OpenVPN suele ser más rápido que WireGuard porque se ejecuta en el espacio del kernel.

- ○ Verdadero
- ○ Falso

8 Pregunta 8

8. OpenVPN es muy configurable y admite tanto el protocolo UDP como el TCP.

- ○ Verdadero
- ○ Falso

9 Pregunta 9

9. WireGuard usa criptografía moderna como ChaCha20 para cifrar los paquetes con rapidez.

- ○ Verdadero
- ○ Falso

10 Pregunta 10

10. WireGuard requiere complejas configuraciones de autoridad de certificación para autenticarse.

- ○ 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. El moderno protocolo _____ funciona directamente dentro del kernel del sistema operativo.

2. El protocolo tradicional _____ se basa en la biblioteca criptográfica OpenSSL.

3. Ejecutar código en el _____ reduce la sobrecarga por cambios de contexto.

4. OpenVPN funciona en el _____ y enruta los paquetes a través de interfaces virtuales.

5. WireGuard usa _____ , públicas y privadas, para identificar a los nodos de la conexión.

6. Una base de código pequeña facilita la _____ de la seguridad del software.

BANCO DE PALABRAS DE VOCABULARIO

AUDITABILIDAD CÓDIGO COMPACTO ESPACIO DE KERNEL ESPACIO DE USUARIO
OPENSSL OPENVPN PARES DE CLAVES WIREGUARD

Escribe aquí tus respuestas:

1. **2.**

3. **4.**

5. **6.**

Punto de control 4: Relación de conceptos de redes

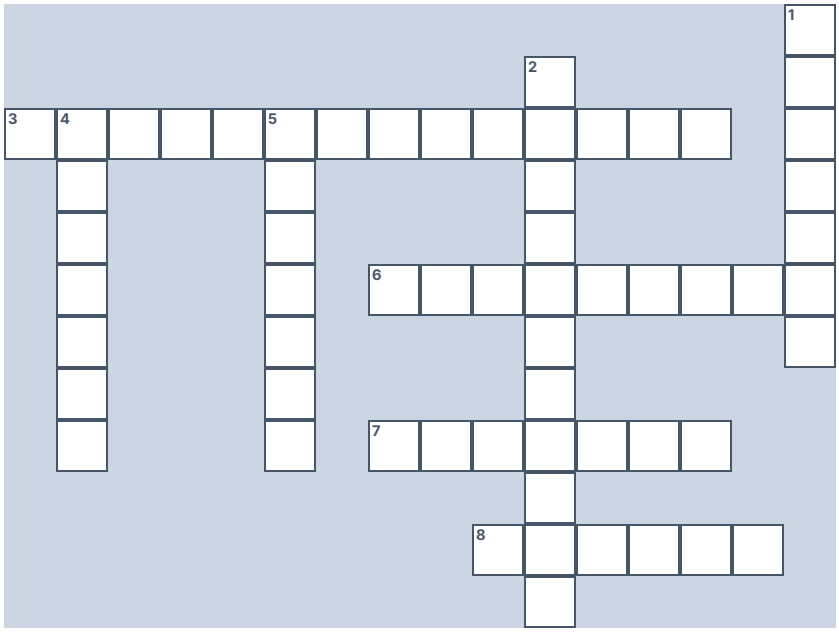
RELACIÓN DE DEFINICIONES

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

☐	1. WireGuard	A	Área de ejecución donde funciona OpenVPN, lo que genera la sobrecarga de los cambios de contexto.
☐	2. OpenVPN	B	El tamaño compacto de la base de código de WireGuard, que hace que sea mucho más fácil de auditar.
☐	3. Espacio del kernel	C	Biblioteca criptográfica de la que depende OpenVPN para los algoritmos de cifrado.
☐	4. Espacio de usuario	D	Protocolos de transporte que admite OpenVPN; WireGuard en sí solo funciona sobre UDP.
☐	5. 4,000 líneas	E	Área de ejecución del sistema operativo donde se ejecuta WireGuard para ganar velocidad.
☐	6. OpenSSL	F	Tokens asimétricos que WireGuard usa para verificar las conexiones entre pares.
☐	7. Par de claves	G	Protocolo VPN moderno diseñado para una alta velocidad y una auditoría sencilla del código.
☐	8. TCP/UDP	H	Protocolo heredado robusto que usa una base de código de configuración grande y compleja.

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. Tamaño reducido de la base de código de WireGuard, que la hace mucho más fácil de auditar (14)

6. Protocolo VPN moderno diseñado para ofrecer alta velocidad y un código fácil de auditar (9)

7. Espacio de ___: área de ejecución donde funciona OpenVPN, lo que genera sobrecarga por cambios de contexto (7)

8. Espacio de ___: área de ejecución del sistema operativo donde funciona WireGuard para ganar velocidad (6)

VERTICALES

1. Protocolos de transporte que admite OpenVPN; WireGuard solo funciona sobre UDP (7)

2. Claves asimétricas que usa WireGuard para verificar las conexiones entre pares (11)

4. Biblioteca criptográfica en la que se basa OpenVPN para los algoritmos de cifrado (7)

5. Protocolo tradicional y robusto que usa una base de código de configuración grande y compleja (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

3 horizontal: Tamaño reducido de la base de código de WireGuard, que la hace mucho más fácil de auditar (14 letras):

6 horizontal: Protocolo VPN moderno diseñado para ofrecer alta velocidad y un código fácil de auditar (9 letras):

7 horizontal: Espacio de ___: área de ejecución donde funciona OpenVPN, lo que genera sobrecarga por cambios de contexto (7 letras):

8 horizontal: Espacio de ___: área de ejecución del sistema operativo donde funciona WireGuard para ganar velocidad (6 letras):

VERTICALES

1 vertical: Protocolos de transporte que admite OpenVPN; WireGuard solo funciona sobre UDP (7 letras):

2 vertical: Claves asimétricas que usa WireGuard para verificar las conexiones entre pares (11 letras):

4 vertical: Biblioteca criptográfica en la que se basa OpenVPN para los algoritmos de cifrado (7 letras):

5 vertical: Protocolo tradicional y robusto que usa una base de código de configuración grande y compleja (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.

O P E N S S L W I D R Q M E I

S R Z S F Q V I F A O A Q O N

E O P T X Q K R R T P R D N Y

V I B G K R X E W J E A R Z Y

A R Y L E G I G N Q N K M M T

L A O H R P Q U H Z V A O V G

C U U C N Y R A Y B P H M Z G

E S K Ñ E P Ñ R W C N M Z Y G

D U Y O L W U D L U P B Ñ V T

R M H U D Y U K R B W Z Y M R

A C O D I G O C O M P A C T O

P Q X I O D A D K Q V W W L J

I T T C P Y U D P I G B F I L

T R V Q Z E I F R C A L P C Z

M K V R U A S W K M M H H N I

LISTA DE PALABRAS DE VOCABULARIO

WIREGUARD OPENVPN KERNEL USUARIO CODIGOCOMPACTO OPENSSL PARDECLAVES TCPYUDP

Punto de control 6, alternativa: Relación de vocabulario accesible

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

TÉRMINOS DE VOCABULARIO

- **A. WIREGUARD**
- **B. OPENVPN**
- **C. KERNEL**
- **D. USUARIO**
- **E. CODIGOCOMPACTO**
- **F. OPENSSL**
- **G. PARDECLAVES**
- **H. TCPYUDP**

DEFINICIONES Y CAMPOS DE RELACIÓN

_____ 1. Biblioteca criptográfica en la que se basa OpenVPN para los algoritmos de cifrado.

_____ 2. Espacio de ___: área de ejecución del sistema operativo donde funciona WireGuard para ganar velocidad.

_____ 3. Protocolo tradicional y robusto que usa una base de código de configuración grande y compleja.

_____ 4. Claves asimétricas que usa WireGuard para verificar las conexiones entre pares.

_____ 5. Protocolos de transporte que admite OpenVPN; WireGuard solo funciona sobre UDP.

_____ 6. Tamaño reducido de la base de código de WireGuard, que la hace mucho más fácil de auditar.

_____ 7. Protocolo VPN moderno diseñado para ofrecer alta velocidad y un código fácil de auditar.

_____ 8. Espacio de ___: área de ejecución donde funciona OpenVPN, lo que genera sobrecarga por cambios de contexto.

Punto de control 7: Reto de palabras desordenadas

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

1. **UGEIWARDR** _____

2. **LKRENE** _____

3. **CMOTOOPADCGOCI** _____

4. **LESCREVAPAD** _____

5. **VNNEOPP** _____

6. **IURUAOS** _____

7. **OSSLPNE** _____

8. **CYPTDUP** _____

Actividad extra: Piensa rápido

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

1	Razones para elegir WireGuard			
2	Promesas que hace un buen proveedor de VPN			
3	Razones para elegir OpenVPN			
4	Razones para usar una VPN cuando viajas			
5	Cosas que puede ver tu proveedor de internet			
6	Formas de detectar una red Wi-Fi falsa			
7	Mitos sobre las VPN			
8	Lugares en los que usarías una VPN			
9	Cosas rápidas de la vida cotidiana			
10	Cosas de las que una VPN no puede protegerte			
11	Cosas que hacen que el código sea más fácil de revisar			
12	Cosas que una VPN puede ocultar			
13	Diferencias entre WireGuard y OpenVPN			
14	Palabras relacionadas con la privacidad			
15	Nombres de cifrados que conoces			

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 conectada al wifi de la cafetería y mi aplicación VPN me deja elegir WireGuard u OpenVPN. Mis videollamadas se cortan cada vez que paso de la red de la cafetería a la zona wifi de mi móvil. ¿Qué protocolo debería elegir y por qué gestionaría mejor el cambio?"

ALEX (ESTUDIANTE VIAJERO)

👩‍💻 "Estoy en el extranjero, en la red de un hotel que parece bloquear la mayor parte del tráfico VPN. WireGuard no se conecta en absoluto, pero necesito acceder a los recursos de mi centro de estudios en mi país. ¿Qué es probable que se esté bloqueando y cómo podría ayudarme OpenVPN a superarlo?"

Punto de control 9: Descifrar el código

Para completar tu formación sobre auditoría de protocolos, descifra este mensaje oculto sobre la ejecución en el espacio del kernel.

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

13	5	10	16	19	1		21	22		16	17	5	14	23	17	14		3	16	14
22	14		21	22	14	5	12		13	1	20		19	1	17	9	4	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 importan los protocolos?

El protocolo decide cómo construye tu VPN su túnel, qué criptografía protege tus datos y con qué rapidez se conecta y se vuelve a conectar. WireGuard y OpenVPN son los dos protocolos de código abierto que ofrecen la mayoría de las aplicaciones VPN, y cada uno equilibra de forma distinta la sencillez, la velocidad y la capacidad de configuración.

Q3: ¿Es uno de ellos más privado que el otro?

Ninguno de los dos protocolos te hace anónimo. Ambos cifran el tráfico del túnel con cifrados sólidos; tu privacidad depende sobre todo de lo que registra el proveedor de VPN y de cómo gestiona las claves, las cuentas y los servidores.

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: ¿Son ambos de código abierto?

Sí. Tanto WireGuard como la edición comunitaria de OpenVPN publican su código fuente, de modo que investigadores independientes pueden revisarlos. El reducido código base de WireGuard hace que una revisión completa sea mucho más rápida.

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: ¿Cuál es más rápido?

WireGuard suele ser más rápido: se ejecuta en el kernel, usa el cifrado ligero ChaCha20-Poly1305 y completa los handshakes rápidamente. OpenVPN tiene más sobrecarga, pero la velocidad real también depende de la carga del servidor y de la distancia.

Q7: ¿Pueden ambos funcionar sobre TCP y UDP?

No. OpenVPN puede funcionar sobre UDP o TCP, y el modo TCP ayuda en redes que bloquean UDP. WireGuard envía sus paquetes solo por UDP, por lo que puede fallar en redes que solo permiten TCP. [4]

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 WireGuard y OpenVPN en mi teléfono?

Sí. WireGuard es multiplataforma, con aplicaciones para Windows, macOS, Linux, iOS y Android, y existen clientes de OpenVPN para los mismos sistemas. La mayoría de las aplicaciones VPN te permiten elegir cualquiera de los dos. [1]

Q10: ¿Por qué WireGuard es tan pequeño?

WireGuard admite un único conjunto fijo de cifrados modernos en lugar de muchas opciones. Su implementación para Linux necesita menos de 4.000 líneas de código, lo que facilita auditarlo en comparación con códigos base de VPN más grandes. [3]

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

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

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

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

Q2: ¿Qué cifrados utiliza WireGuard?

WireGuard usa ChaCha20 con Poly1305 para el cifrado, Curve25519 para el intercambio de claves, BLAKE2s para el hash y el marco Noise para su handshake. No hay negociación de cifrados, por lo que los usuarios no pueden elegir una opción débil. [2]

Q3: ¿Qué cifrados y bibliotecas puede utilizar OpenVPN?

OpenVPN está estrechamente integrado con la biblioteca OpenSSL y usa TLS para intercambiar claves. Los administradores pueden elegir cifrados del canal de datos como AES-256-GCM, lo que aporta flexibilidad pero también deja margen para configuraciones débiles. [4]

Q4: ¿Cómo autentica cada protocolo a los pares?

Los pares de WireGuard se identifican entre sí mediante claves públicas estáticas, de forma muy parecida al intercambio de claves SSH, y cada clave se asocia a las IP de túnel permitidas. OpenVPN suele basarse en una autoridad de certificación con certificados X.509, a menudo combinada con un nombre de usuario y una contraseña.

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 ocurre cuando cambio de Wi-Fi a datos móviles?

WireGuard no mantiene conexiones: envía los paquetes desde la nueva dirección y el túnel continúa tras un breve handshake. OpenVPN mantiene el estado de la sesión, por lo que un cambio de red puede requerir una reconexión que tarda algo más.

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: ¿Sigue siendo OpenVPN una buena opción si WireGuard es más rápido?

Sí. OpenVPN es un protocolo maduro y ampliamente implantado, funciona sobre TCP cuando UDP está bloqueado y admite configuraciones empresariales basadas en certificados. Muchos proveedores ofrecen ambos protocolos para que los usuarios puedan cambiar si uno está bloqueado o es lento.

Q9: ¿Qué puertos utilizan?

El puerto estándar de OpenVPN es el 1194, pero puede trasladarse a cualquier puerto UDP o TCP, incluido el 443. WireGuard escucha en un puerto UDP definido en su configuración; 51820 es el puerto que se usa en sus ejemplos oficiales.

Q10: ¿Qué protocolo es más fácil de configurar a mano?

WireGuard suele ser más sencillo: generas un par de claves, intercambias las claves públicas y enumeras las IP permitidas. OpenVPN necesita certificados, una CA y más opciones, aunque los perfiles .ovpn los agrupan en un solo archivo.

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. DOS TRANSPORTES

OpenVPN puede transportar su túnel por UDP o TCP y, en modo TLS, sus canales de control y de datos comparten un único puerto. [4]

3. LA REVOLUCIÓN DE WIREGUARD

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

4. CRIPTOGRAFÍA MODERNA

WireGuard combina ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 y HKDF dentro del marco del protocolo Noise, sin opciones de cifrado que los usuarios puedan configurar mal. [2]

5. OPENSSL DENTRO DE OPENVPN

OpenVPN está estrechamente integrado con la biblioteca OpenSSL y obtiene de ella muchas de sus capacidades criptográficas, incluido el TLS que se usa para intercambiar claves. [4]

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. CLAVES DE TIPO SSH

Las conexiones WireGuard se establecen intercambiando claves públicas sencillas, de forma muy parecida al intercambio de claves SSH, sin necesidad de una autoridad de certificación. [1]

8. MULTIPLATAFORMA

WireGuard se publicó primero para el kernel de Linux y ahora está disponible para Windows, macOS, BSD, iOS y Android, por lo que el mismo protocolo funciona en la mayoría de los dispositivos. [1]

9. SECRETO HACIA ADELANTE

WireGuard repite su handshake Noise_IK cada pocos minutos para rotar las claves de sesión simétricas, lo que proporciona confidencialidad directa perfecta (perfect forward secrecy) aunque más adelante se filtre una clave a largo plazo. [2]

10. INTERFACES TUN/TAP

OpenVPN está diseñado para funcionar con la interfaz de red virtual TUN/TAP, disponible en la mayoría de las plataformas, que transporta los paquetes del túnel. [4]

Referencias técnicas y fuentes

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

REFERENCIAS ACADÉMICAS Y DEL SECTOR

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

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

[3] 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/

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

[5] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

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

Clave de respuestas: comparación de los protocolos WireGuard y OpenVPN, el tamaño de su código, la velocidad y los estándares criptográficos

1 **Tamaño del código de WireGuard** PROTOCOLOS — **Respuesta correcta: D**

NOTA PARA DOCENTES

WireGuard es extremadamente compacto: funciona con unas 4.000 líneas de código. Esto mantiene reducida la superficie de ataque y facilita las auditorías. Cita: WireGuard Project.

2 **Velocidad en el espacio del kernel** LATENCIA — **Respuesta correcta: B**

NOTA PARA DOCENTES

Al ejecutarse directamente en el espacio del kernel, WireGuard evita la sobrecarga de los cambios de contexto, lo que permite un alto rendimiento. Cita: WireGuard Project.

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

NOTA PARA DOCENTES

OpenVPN está estrechamente integrado con OpenSSL, que aporta cifrados como AES-GCM y lo hace muy configurable, pero más complejo. [4]

4 **Rendimiento del protocolo** CONTROLES DE ENRUTAMIENTO — **Respuesta correcta: A**

NOTA PARA DOCENTES

WireGuard establece los handshakes en milisegundos y responde al instante a los cambios de red (por ejemplo, al pasar de wifi a datos móviles). Cita: Microsoft Native Gateway, Apple Support.

5 **Criptografía asimétrica** PRIVACIDAD — **Respuesta correcta: C**

NOTA PARA DOCENTES

WireGuard usa Cryptokey Routing, que asocia las claves públicas con las direcciones IP de túnel permitidas, de forma similar a las configuraciones de SSH. Cita: WireGuard Project.

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

6 **Pregunta 6** — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

La implementación de WireGuard para Linux tiene menos de 4,000 líneas, por lo que los equipos de seguridad pueden revisarla mucho más rápido que bases de código VPN mucho mayores, como la de OpenVPN.

7 **Latencia en el espacio de usuario** VELOCIDADES — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

OpenVPN se ejecuta en el espacio de usuario y pasa los paquetes de un lado a otro desde la interfaz virtual del kernel, lo que añade sobrecarga por cambios de contexto (salvo que se use una descarga al kernel como OpenVPN DCO). Cita: DD-WRT custom firmware.

8 **Configuración de OpenVPN** RIESGO DE SNIFFING — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

OpenVPN puede funcionar sobre TCP (para mayor fiabilidad o para sortear cortafuegos) o sobre UDP (para mayor velocidad), lo que lo hace compatible con cortafuegos empresariales complejos. Cita: IETF Cryptographic Protocols.

9 **Criptografía moderna** CORTAFUEGOS — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

WireGuard descarta los cifrados heredados en favor de primitivas modernas y seguras como ChaCha20 y Poly1305, que se ejecutan con rapidez en las CPU móviles. Cita: WireGuard Project.

10 **Simplificación mediante pares de claves** SIN REGISTROS — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

WireGuard no usa certificados ni complejas jerarquías de CA; se basa en simples pares de claves pública/privada intercambiados entre pares. Cita: WireGuard Project.

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

G 1. WireGuard	H 2. OpenVPN	E 3. Espacio del kernel	A 4. Espacio de usuario
B 5. 4,000 líneas	C 6. OpenSSL	F 7. Par de claves	D 8. TCP/UDP

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 WIREGUARD	2 OPENVPN	3 ESPACIO DE KERNEL	4 ESPACIO DE USUARIO
5 PARES DE CLAVES	6 AUDITABILIDAD		

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

1 F – OPENSSL	2 C – KERNEL	3 B – OPENVPN	4 G – PARDECLAVES
5 H – TCPYUDP	6 E – CODIGOCOMPACTO	7 A – WIREGUARD	8 D – USUARIO

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar WireGuard, OpenVPN y Espacio del kernel 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.

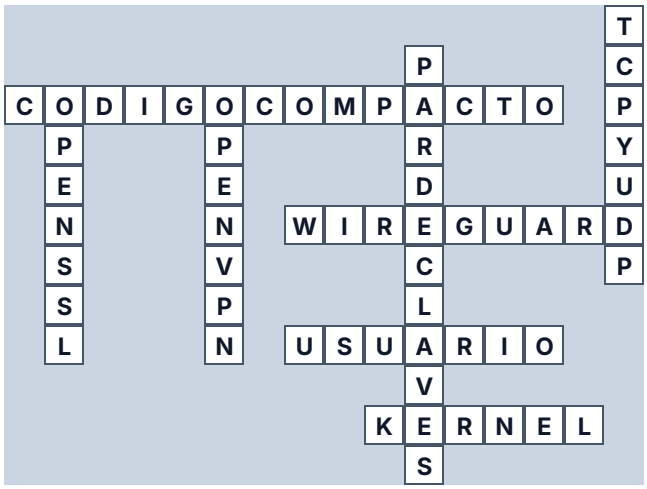
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

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

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

3 horizontal: CODIGOCOMPACTO Tamaño reducido de la base de código de WireGuard, que la hace mucho más fácil de auditar (14 letras)

6 horizontal: WIREGUARD Protocolo VPN moderno diseñado para ofrecer alta velocidad y un código fácil de auditar (9 letras)

7 horizontal: USUARIO Espacio de ___: área de ejecución donde funciona OpenVPN, lo que genera sobrecarga por cambios de contexto (7 letras)

8 horizontal: KERNEL Espacio de ___: área de ejecución del sistema operativo donde funciona WireGuard para ganar velocidad (6 letras)

VERTICALES

1 vertical: TCPYUDP Protocolos de transporte que admite OpenVPN; WireGuard solo funciona sobre UDP (7 letras)

2 vertical: PARDECLAVES Claves asimétricas que usa WireGuard para verificar las conexiones entre pares (11 letras)

4 vertical: OPENSSL Biblioteca criptográfica en la que se basa OpenVPN para los algoritmos de cifrado (7 letras)

5 vertical: OPENVPN Protocolo tradicional y robusto que usa una base de código de configuración grande y compleja (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. UGEIWARDR — **WIREGUARD**
2. LKRENE — **KERNEL**
3. CMOTOOPADCGOCI — **CODIGOCOMPACTO**
4. LESCREVAPAD — **PARDECLAVES**
5. VNNEOPP — **OPENVPN**
6. IURUAOS — **USUARIO**
7. OSSLPNE — **OPENSSL**
8. CYPTDUP — **TCPYUDP**

CLAVE DEL RETO DEL CÓDIGO SECRETO

"MEJORA TU OPENVPN CON UN TUNEL MAS RAPIDO"

Clave de respuestas de los casos prácticos

A Escenario A: elegir un protocolo

SNIFFING Y CIFRADO · El dilema de Sarah

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Recomendación: WireGuard. Su diseño ligero y sin conexión permite que el túnel se recupere rápidamente cuando cambia su red, y ChaCha20-Poly1305 mantiene un cifrado rápido.
- Seguridad: ambos protocolos cifran su tráfico en el wifi de la cafetería, así que cualquiera de los dos protege sus inicios de sesión si está bien configurado; la elección afecta sobre todo a la velocidad y la estabilidad.

B Escenario B: Sortear los bloqueos de VPN

GEOBLOQUEO E IP · El dilema de Alex

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Por qué se bloquea: WireGuard solo usa UDP, y es probable que el cortafuegos del hotel bloquee UDP o reconozca los paquetes de WireGuard mediante filtrado o inspección profunda de paquetes.
- Cómo ayuda OpenVPN: puede funcionar sobre TCP, incluido el puerto 443 que usa HTTPS, que los cortafuegos de los hoteles rara vez bloquean por completo porque la navegación web depende de él.