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

PUNTO DE CONTROL 10

Preguntas frecuentes sobre VPN

Hoja de trabajo interactiva y guía de estudio

Basado en la guía de VPN de VPN.com: **https://www.vpn.com/es/vpn/**

Hoja de trabajo: ¿Qué es una VPN?

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.

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