

¿Qué es una VPN (Virtual Private Network)?

Una red privada virtual (RPV) (en inglés, Virtual Private Network, VPN) es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

Permite que el ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo o bien que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

Características de una red privada virtual

- Autenticación y autorización: ¿quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.
- Integridad: de que los datos enviados no han sido alterados. Para ello se utilizan funciones de Hash. Los algoritmos de hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).
- Confidencialidad/Privacidad: dado que solamente puede

ser interpretada por los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).

- No repudio: es decir, un mensaje tiene que ir firmado, y quien lo firma no puede negar que envió el mensaje.
- Control de acceso: se trata de asegurar que los participantes autenticados tienen acceso únicamente a los datos a los que están autorizados.
- Auditoría y registro de actividades: se trata de asegurar el correcto funcionamiento y la capacidad de recuperación.
- Calidad del servicio: se trata de asegurar un buen rendimiento, que no haya una degradación poco aceptable en la velocidad de transmisión.