



# VPN

acceso al

# Teletrabajo

seguro



Llevamos mucho tiempo implementando sistemas y soluciones de teletrabajo para nuestros clientes. Cubrimos todo el ciclo de puesta en marcha del sistema: instalación de redes informáticas, instalación de redes privadas encriptadas (VPN), configuración de la red informática, administración de usuarios, sistemas de almacenamiento en la nube, copias de seguridad, escritorios virtuales, Proporcionamos además mantenimiento informático, asistencia telefónica, en remoto o en local, mantenimiento de las redes informáticas y soporte técnico, para garantizar la máxima fiabilidad del sistema, y que todos los empleados de la empresa puedan teletrabajar sin contratiempos ni incidencias. En resumen, ponemos a su disposición la ventaja competitiva que supone contar con las últimas innovaciones tecnológicas sin tener que gestionarlas directamente, una total flexibilidad a nivel de trabajo remoto, y todo ello con la tranquilidad de contar con un asistente tecnológico de confianza, que se encarga de todo lo relacionado con la informática, redes y telecomunicaciones en estos momentos tan complicados.

Las organizaciones estamos cada vez más conectadas a la red. Casi toda la información que manejamos es importante para el desarrollo de nuestro negocio y por eso ha de estar siempre bien protegida; pero no solo cuando la mantenemos almacenada, sino también cuando accedemos a ella. En la actualidad el constante uso de dispositivos en entornos corporativos, hace necesario que se tengan que establecer mecanismos de acceso remoto seguro a la información de nuestras empresas, como son las Redes Privadas Virtuales comúnmente conocidas por sus siglas en inglés VPN.

Hoy en día se habla mucho de habilitar los accesos a la red interna de gestión y a su información de una forma segura a través de implementación de VPN, pero puede que en algunos casos no se entienda bien cómo funciona y cuáles son sus principales ventajas e inconvenientes.

Una VPN es un servicio que permite el acceso remoto a la red interna de nuestra empresa y a los recursos de la misma, como pueden ser el correo electrónico, el servidor de ficheros o incluso aplicaciones de «escritorio» como el CRM, ERP o cualquier otra aplicación departamental. Este acceso a través de internet de forma segura, permite la movilidad o el teletrabajo del empleado o incluso interconectar sedes separadas geográficamente. Una VPN crea un túnel a través de internet mediante cifrado seguro, de forma que podemos acceder desde cualquier lugar a los servicios y documentos internos de nuestra compañía

## Pero, ¿cuáles son las ventajas que nos proporciona implementar una VPN?

1. **Acceso remoto seguro.** Se establece una comunicación cifrada entre el cliente o sede y el servidor VPN de la oficina. Este acceso aumenta la productividad, permite ahorrar costes y genera nuevas oportunidades de negocio.
2. **Publicamos un servicio único (VPN)** en vez de publicar varios que pueden ser punto de mira de ataques de fuerza bruta (FTP, Web Login, Paneles de administración, etc.)
3. **Teletrabajo:** Permite a nuestros empleados conectarse de forma segura remotamente a los recursos corporativos. De esta forma se fomenta la flexibilidad laboral y la conciliación familiar y profesional.
4. **Control de accesos:** Saber en cada momento quién y desde dónde se ha conectado y qué ha hecho.

Sin embargo, no todos son ventajas cuando implementamos una VPN, también conlleva una serie de desventajas como las que planteamos a continuación:

1. **Coste económico y temporal** que supondría instalar, configurar y poner en marcha un servicio VPN.
2. **Reestructuración a nivel de red** (filtrados, rutas, etc.) que se han de llevar a cabo por parte del equipo de comunicaciones.
3. **Configuración de los clientes** (móviles, PC, etc.) de los empleados para que puedan acceder a través de VPN haciendo uso de las aplicaciones correspondientes. Para ello, se ha de generar un certificado y una contraseña de acceso para cada uno de los empleados.

Entonces, llegados a este punto, ¿por qué deberíamos utilizar una conexión VPN?

Las VPN nos garantizan que toda la información que transmitamos va a estar segura. Concretamente su confidencialidad, ya que en caso que fuese interceptada durante la transmisión, no podría ser decodificada; su integridad, ya que la información viaja cifrada, por lo que no pueden ser modificada o alterada durante la transmisión. Además, nos garantiza que la información está siendo transmitida solo desde dispositivos autorizados.

Como se ha indicado anteriormente y teniendo en cuenta la necesidad de que nuestros empleados puedan acceder a la información corporativa desde cualquier lugar del mundo hace que asegurar el acceso y la transmisión de la información sea una tarea primordial.

Es importante que los accesos remotos a los recursos internos se hagan de una forma segura y totalmente controlada. Utilizando una VPN podemos garantizar las dos cosas: seguridad; por el cifrado que se aplica a la conexión y a la información que se remite a través del túnel, y control; ya que permite conocer en todo momento quién ha accedido, cuándo, desde dónde y las acciones que ha realizado.

Por lo tanto, y a modo de resumen debemos valorar la necesidad real de nuestra empresa de que los empleados necesiten acceder a los recursos y servicios corporativos desde sitios remotos (por motivos de viaje, teletrabajo, ...). Si realmente es necesario, debemos valorar otros aspectos como, el coste temporal y de recursos humanos que supondría desplegar e implementar un servicio VPN. En nuestro catálogo de soluciones podrás encontrar distintas aplicaciones VPN para implementar en el entorno corporativo.

Ahora que ya conoces todas las ventajas e inconvenientes que tiene implementar una VPN, ¡tú decides! Haz lo que hagas, hazlo siempre con ciberseguridad.