MICROAREA

TELETRABAJO

Guía para configurar el servidor y poder teletrabajar.

MANUAL CONFIGURACIÓN DEL SERVIDOR PARA TELETRABAJAR

MICROAREA DESARROLLOS INFORMÁTICOS, S.L.U.

info@microareanext.com | www.microarea.es

Índice General

Preámbulo

El presente manual tiene como naturaleza configurar el equipo que actúa como servidor y el rúter (red local) para poder teletrabajar, es decir, que la información, y por tanto la base de datos, sea accesible desde otra ubicación que no sea la habitual (oficina/despacho/hogar), de manera que se pueda trabajar con el programa desde cualquier lugar como si estuviera allí mismo mediante una conexión internet.

En términos generales, no hay diferencia alguna entre trabajar en una red local o doméstica (despacho, empresa, oficina o casa) y una red pública (Internet) aunque lógicamente la eficacia, eficiencia y rapidez vendrá siempre determinada y condicionada por la calidad y velocidad de la conexión, los dispositivos y la distancia entre los puntos.

En cualquier caso, el programa graba la información en la base de datos del ordenador que actúa como servidor mediante el SQL Server (Motor de base de datos perteneciente a Microsoft) de tal manera que ésta pueda ser accesible desde los distintos ordenadores que trabajan con las aplicaciones. Esta característica recibe el nombre técnico «Cliente-Servidor». Por defecto y por motivos de seguridad, Microsoft limitará la conexión a dicha base de datos a la red local, por lo no será posible conectar desde internet.

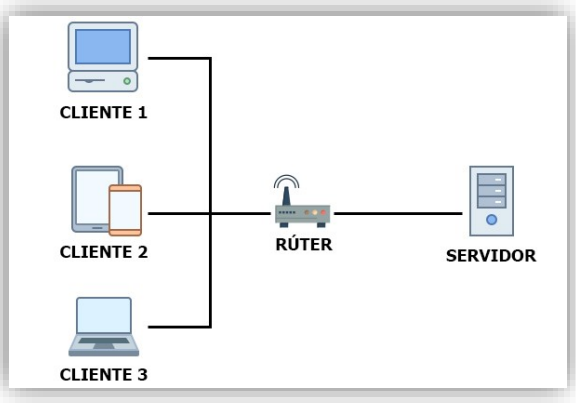

Ilustración 1: Esquema de la típica red local.

En la *ilustración 1*, podremos comprobar cómo funciona una típica red local en la que no hay acceso desde «fuera» a la base de datos. Cada dispositivo conectado a la red local (ordenador, portátil, Tablet, etc.), denominados clientes en la jerga informática, podrán recibir y enviar información al servidor mediante el rúter. Dicha conexión puede hacerse mediante una red Wifi, por cable de red o ambas a la vez. Este sería el comportamiento por defecto al realizar la instalación.

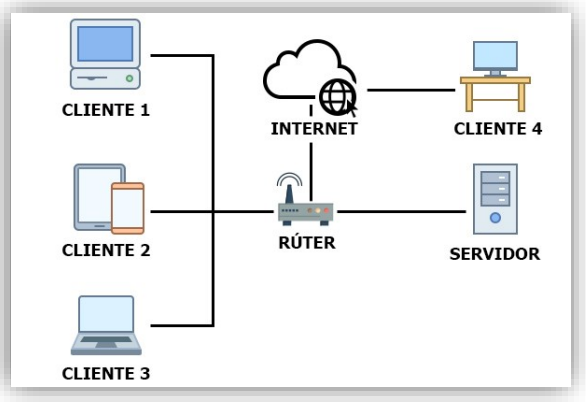

Ilustración 2: Esquema de la típica red local, pero con conexión a internet.

Por el contrario, en la *ilustración 2*, tendríamos la misma situación que la ilustración 1, pero permitiendo el acceso a la base de datos, no sólo a los dispositivos (clientes) de la red local, sino que además podría conectarse otros clientes desde fuera de la misma mediante una conexión de internet. Al igual que en el caso anterior, el punto de acceso, y filtrado, se realizaría mediante el rúter de la oficina/despacho. Del mismo modo, la conexión podría realizarse mediante cable de red, Wifi o una situación mixta.

Tal y como queda reflejada en las *ilustraciones 1 y 2*, deberíamos tener acceso al rúter con los privilegios adecuados para poder realizar modificaciones (En caso de duda, contacte con su compañía proveedora de internet o informático).

Consideraciones previas

Antes de continuar habrá que considerar o aclarar ciertos aspectos puesto que, aunque la configuración es relativamente sencilla, hay muchos factores a tener en consideración.

¿Podré trabajar en la nube?

Según la octava definición de la RAE[1], la nube es «*un espacio de almacenamiento y procesamiento de datos y archivos ubicado en internet, al que puede acceder el usuario desde cualquier dispositivo*». Por lo que técnicamente la respuesta es afirmativa. Con esta solución lo que se está haciendo es «transformar» su servidor local en servidor nube. Deberá tener presente ciertas cuestiones, al no ser una solución comercial, como la disponibilidad o seguridad del mismo. Para más información consulte la sección cuestiones sobre el servidor.

¿Podré trabajar en remoto?

No, trabajar de forma remota es otra solución totalmente distinta y diferente. Esta solución no está orientada a trabajar conectándose de un ordenador a otro mediante una tercera aplicación (control remoto, escritorio remoto, VPN, etc.). Esta solución brinda el acceso directamente a la base de datos para que, con el programa instalado fuera de la red local, o corporativa, pueda trabajar como si estuviera físicamente en la oficina/despacho.

Sobre la necesidad de una IP pública fija

La IP pública es la dirección IP del rúter, la cual es asignada automáticamente por el ISP (proveedor de internet), que permite el acceso de los dispositivos de esa red a internet (y viceversa). Técnicamente no es necesaria disponer de una IP fija para trabajar, no obstante, dado que actualmente casi todas las compañías de internet proveen IP dinámicas (cada cierto tiempo son reasignadas) es posible que, tras un reinicio/actualización del rúter, o simplemente, de un día para otro, la IP haya cambiado y no pueda conectar para trabajar con la IP antigua. En tal caso, debería averiguar[2] la nueva IP de un modo u otro. Si se dispone de una IP fija este problema desaparece, pero podría aplicarse algún cargo por el servicio. Deberá consultar a su proveedor de internet.

Cuestiones sobre el servidor

Si seguimos todos los pasos del manual, habremos expuesto la base de datos a internet, con todas las ventajas e inconvenientes que implica. A diferencia de una nube comercial, deberemos extremar las precauciones ya que será su responsabilidad asegurar su correcto funcionamiento, su debida accesibilidad, gestionar su seguridad y cumplir con la normativa en protección de datos (LOPD-GDD[3] y RGPD[3]).

Con esta opción, será el usuario el que tendrá el control total del servidor, de forma que será usted quién decida la disponibilidad del mismo (como que no esté disponible el fin de semana) o limitar el acceso a un número determinado de usuarios/IP. Adicionalmente, no será necesaria la cesión de los datos de carácter personal a una tercera empresa.

Esta personalización será a nivel de rúter y de ordenador, por lo que deberá contactar con su informático para establecer las condiciones que considere necesarias.

Accesibilidad 24/7 o 365

Si queremos trabajar siempre y en todo lugar, el ordenador que actúa como servidor deberá estar siempre encendido, así como el rúter. Si alguno de estos dos dispositivos no lo estuviera, no podría realizarse la conexión. Deberemos asegurarnos de que nunca se apaguen o que alguien pueda acercarse a su ubicación y encenderlos en caso de necesidad.

---

[1] Nube.

[2] Si hubiera alguien en la oficina, despacho u hogar sería posible contactar con ella para que se la comunique.

[3] Ley Orgánica de Protección de datos y garantía de derechos digitales y Reglamento General de Protección de Datos.

Velocidad de conexión

Hoy en día, casi todas las compañías ofrecen un buen ancho de banda, tanto de subida como de descarga, a velocidades decentes para cánones europeos gracias a la fibra. Sin embargo, es posible que en localidades algo lejanas a las capitales o de difícil acceso, la fibra no esté disponible o sea muy limitada. En estos casos, para no sufrir desconexiones fortuitas y maximizar la fluidez del programa, deberemos intentar disponer de la mayor velocidad simétrica disponible con la menor latencia posible.

Seguridad ampliada

Dado que la base de datos y el servidor han «salido» a internet siempre existirá cierto riesgo de ataque, evidentemente no tiene porqué ocurrir ninguna desgracia, pero habrá que extremar las precauciones y tomar **nuevas medidas de seguridad**. Entre ellas, y las que más afectan al programa, será el **cambio de las contraseñas** (en especial si se usan las claves por defecto) por otras de mayor robustez[4] (esto es, longitud mayor de 8 caracteres que incluyan mayúsculas, minúsculas, números y símbolos especiales**), su actualización de forma reiterada** y la realización periódica de **copias de seguridad.**

La seguridad informática es como la seguridad de cualquier tipo. Si se ponen las cosas fáciles, la posibilidad de sufrir un incidente siempre será más alta. Por ejemplo, en el verano del 2021 un joven accedió a los datos de más de 50 millones de usuarios de T-Mobile[5] al encontrar un rúter Wifi empresarial desprotegido. A modo de símil automovilístico, entre un coche de alta gama debidamente cerrado y sin elementos a la vista y otro coche de gama media, pero con la ventanilla bajada o el móvil en el salpicadero, el ladrón irá por este último porque le resultará más rápido, fácil o suculento que el de gama alta.

IP servidor

Para poder realizar la conexión desde internet es necesario conocer la dirección pública de la oficina/despacho. Dicha IP puede ser consultada en el propio rúter, o mediante alguna web, como por ejemplo ¿Cuál es mi IP? Para la configuración, además también deberá conocer la IP privada el servidor, también podrá consultarse en el rúter, en la lista de dispositivos conectados.

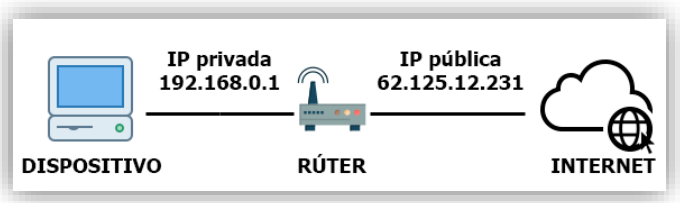

Ilustración 3: Tipos de IP según la red.

Como se desprende la de la *ilustración 3*, la IP pública se utiliza prácticamente para realizar cualquier operación por internet, como navegar, interactuar con la administración pública o presentar impuestos. Por el contrario, la IP privada se limita básicamente a la red local y de esta forma poder interactuar entre dispositivos de la misma red, como compartir información (carpetas compartidas, unidades de red, bases de datos, etc.).

En función de la configuración de la red local, la IP privada podrá ser siempre la misma para un mismo dispositivo (fija) o se le asignará una libre cada vez este se conecte a la red (como cuando se enciende el ordenador). Por este mismo motivo, es de necesidad imperiosa, que la IP privada del servidor sea fija y no cambie en ninguna circunstancia (a expensas de repetir la configuración del rúter).

[4] Consulte la guía publicada por el Incibe (instituto Nacional de Ciberseguridad de España).

[5] La tercera operadora de internet más grande de los Estados Unidos.

Configuración

Para poder conectar desde cualquier ubicación mediante una conexión a internet habrá que realizar dos configuraciones totalmente diferenciadas, una en el rúter, para poder redirigir el tráfico de datos, y otra en el ordenador servidor, para permitir el acceso a la base de datos desde el exterior. Adicionalmente, tendremos una tercera configuración que simplemente se limita a indicar la nueva conexión en el ordenador cliente que esté fuera de le red local.

Antes de poder continuar, será necesario conocer la IP privada del servidor y los puertos que estén siendo utilizados por la base de datos (SQL Server). Ambas acciones **deberán ser llevadas a cabo** de forma **exclusiva** en el ordenador **servidor**, de lo contrario los datos obtenidos no serán válidos.

¿Cuál es la IP privada?

Para saber la IP, no hay que más indicar «CMD» (sin comillas) en el buscador de Windows.

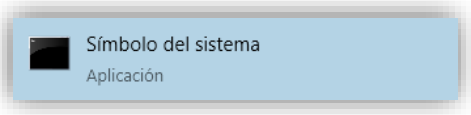

Ilustración 4: Línea de comando «CMD«.

En la ventana (negra) que se habrá abierto únicamente deberemos teclear «ipconfig» (**1**) (sin comillas) y pulsar la INTRO (tecla «INTRO»).

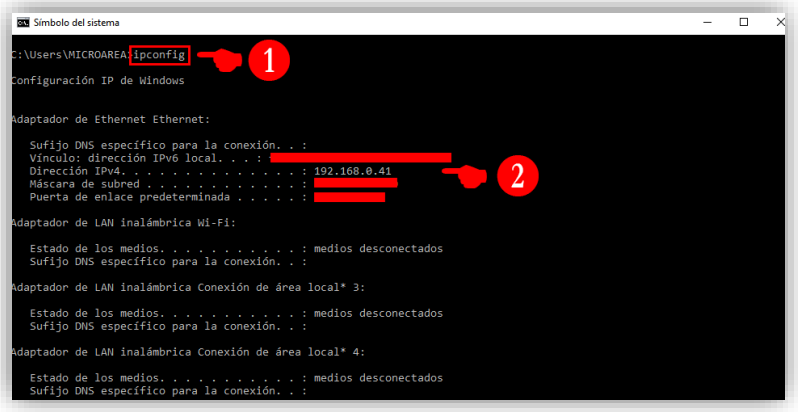

Ilustración 5: Localización de la IP privada.

Aparecerán una serie de datos, *ilustración 5*, con todos los adaptadores de red de los que disponga el ordenador. Habrá que centrarse en el que esté conectado a la red, y por tanto tenga información. Deberemos localizar la entrada «Dirección IPV4» (**2**) que comenzará generalmente por 192.168 seguido por dos bloques más de números. Todo ese conjunto será la IP privada (por ejemplo, 198.168.X.X), la cual necesitaremos para continuar con la configuración.

NOTA INFORMATIVA:

En algunos casos, si la red local ha sido configurada por un especialista para gestionar redes medianas o grandes, es posible que la IP comience por 10.0.X.X o por 172.16.X.X. Son IP privadas totalmente válidas, por lo que no cambiará nada la configuración.

¿Qué puertos utiliza el SQL Server?

Los **puertos** por **defecto** son **1433** y **1434**, no obstante, si en el servidor hay más de una instancia en la base de datos (SQL Server) deberemos consultar los puertos de la instancia que deseamos hacer accesible desde internet. Para ello, solo hay que indicar «SQL Server configuration manager» (Sin comillas) en la búsqueda de Windows para abrir la configuración del SQL Server.

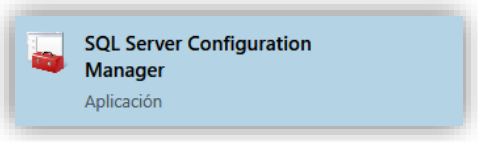

Ilustración 6: Aplicación que permite configurar el SQL Server.

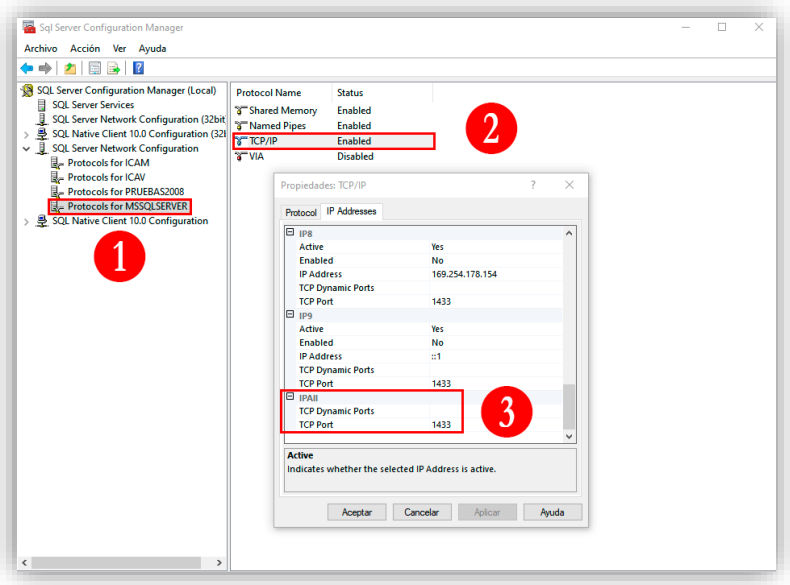

Ilustración 7: Configuración del SQL Server.

En la nueva ventana abierta, deberemos pulsar sobra la instancia que deseamos saber los puertos (**1**), para seleccionar (con doble clic izquierdo) la opción «TCP/IP» (**2**). A continuación, habrá que elegir la pestaña «IP Addresses» y bajar hasta abajo del todo para encontrar la opción «IPAII» y localizar el puerto (**3**).

El **puerto 1434** siempre **será común** para todas las instancias, por lo que este puerto no variará.

AVISO IMPORTANTE:

En ninguna circunstancia deberemos realizar algún cambio. alteración o modificación. Solo nos limitaremos a consultar la información para poder usarla. Para cerrar las ventanas podremos pulsar sobre el botón «Cancelar» si fuera preciso.

Rúter

Para esta configuración se necesitarán de los conocimientos informáticos necesarios para manipular el rúter o contar con el soporte de la compañía suministradora de internet[6], puesto que la configuración del mismo queda más allá de las competencias de Microarea.

Una vez conocidos tanto los puertos de la base de datos, como la IP privada, sólo habrá que abrir los puertos en el rúter (recodemos, siempre el 1434 y el que corresponda al SQL Server) tanto en TCP como UDP. Adicionalmente, deberemos redirigir el tráfico de esos puertos a la IP privada del servidor.

Las opciones de apertura de puertos y direccionamientos de IP pueden variar bastante de un rúter a otro, por lo que se recomienda la asistencia de un informático o la propia operadora.

NOTA INFORMATIVA:

Recuerde, esta configuración puede ser realizada por su operadora, podrá llamarles indicándoles lo que quiere hacer y con los puertos anteriormente indicados ellos le harán la configuración del rúter.

Servidor

En el servidor únicamente hay que configurar el cortafuegos de Windows (o del antivirus con cortafuegos que tenga instalado) para añadir a la lista de exclusiones (o lista blanca) dos ficheros pertenecientes al SQL server (base de datos) de forma que desde el exterior pueda realizarse la conexión.

Estos ficheros son:

- **SQLBrowser.exe**
- **SQLServr.exe**

En caso de emplear el cortafuegos nativo de Windows, deberemos permitirlos en la lista de aplicaciones permitidas de la red pública (si trabaja en la red local, además estaría marcada la opción «Red privada»).

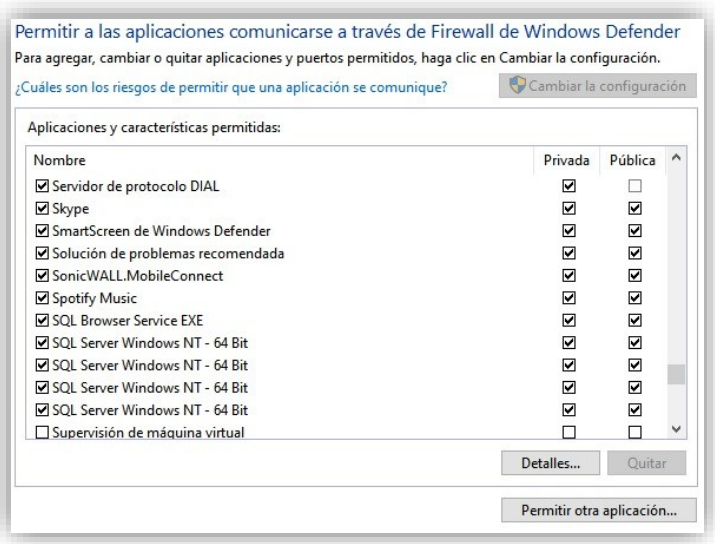

Ilustración 8: Ejemplo de la lista blanca del cortafuegos de Windows con el acceso del SQL server a la red pública y privada.

Para más información puede consultar el manual sobre como configurar cortafuegos de Windows

[6] De hecho, es posible llamarles y ellos harán los cambios pertinentes de forma remota.

Puesto de Red (dispositivo cliente)

No hay que realizar ninguna configuración en los puestos de red. La única diferencia será que, para acceder al programa, habrá que indicar en la casilla de «Servidor» la IP pública de la oficina/despacho o lugar donde se encuentre el PC que hace de servidor (Y el nombre de instancia si existiera más de una). Con respecto al usuario y contraseña, podrá indicarse el que venga utilizándose con asiduidad.

Ilustración 9: Ejemplo de teletrabajo con MaGest (instancia por defecto o única).

Ilustración 10: Ejemplo de teletrabajo para la versión comercial con instancia predeterminada o única y con más de una instancia.

Por ejemplo, si utilizamos la versión comercial de alguno de nuestros programas o el servidor de SQL Server cuenta con una única instancia predeterminada, bastará con indicar únicamente la IP pública o el nombre del ordenador servidor (ver *ilustraciones 9 y 10a).* En cambio, si en el servidor existieran varias instancias de SQL Server o alguna versión distribuida por un Colegio u otra entidad (como en el ejemplo, instancia con nombre «*MICROAREA*»), será necesario indicar la IP pública, o el nombre del equipo servidor, seguida de una barra invertida («\») y el nombre de la instancia correspondiente (ver *ilustración 10b*).

Ilustración 11: Descripción gráfica para poder escribir la barra invertida o contra barra.

Preguntas frecuentes

¿Es posible revertir la configuración?

Sí, no hay problema alguno. Es tan sencillo como deshabilitar el acceso de la base de datos en la red pública en el cortafuegos de Windows o desactivar la redirección en el rúter. Por motivos de seguridad se recomienda hacer ambos cambios. De esta forma, al deshabilitar, y no borrar, podremos alternar sin problema según las necesidades del momento.

¿Puedo trabajar de forma mixta?

Si, la gente podrá trabajar en la red local (oficina/despacho) con total normalidad a la vez que una, o más personas, trabajan desde casa (u otro lugar) sin que el sistema se resienta.

¿Tiene algún coste?

No, puesto que se trata de una configuración relativamente sencilla y no se adquiere ningún servicio extraordinario.

¿Podéis hacer vosotros la configuración?

Lamentablemente no, Microarea no tiene las competencias como para gestionar su red o su rúter. No obstante, con la presente guía puede hacer la parte relativa al servidor y su compañía de internet la gestión del rúter.

¿Podré conectarme desde una Tablet o un móvil?

El programa no ha cambiado, sólo que ahora la información será accesible desde internet, por lo que seguiremos necesitando tener el programa instalado. Lamentablemente aún no hay versión Android o IOS de nuestros programas.

¿Podré trabajar desde la web mediante el navegador?

No, esta solución no es una opción web. Necesitaremos tener un ordenador (o Tablet con sistema operativo Windows) con el programa instalado.

¿Es posible conectarse con un USB Wifi o compartiendo los datos con el móvil?

Sí, es posible. Cualquiera de nuestros programas no discrimina entre conexiones de internet, no obstante, lógicamente podrán darse una serie de limitaciones en función de las capacidades del USB Wifi o los datos del móvil, como pudieran ser la velocidad, la latencia o la cantidad de datos disponibles que podrán hacer que el programa vaya más lento o inestable de lo habitual.

Información de utilidad

Teléfonos y correos electrónicos

Teléfono Soporte Técnico: 96 338 79 20

Teléfono Departamento Comercial: 96 338 79 21

Correo Soporte Técnico: soporte.tecnico@microareanext.com

Correo Departamento Comercial: info@microareanext.com

Redes sociales:

Glosario

Base de datos	*Información almacenada en un soporte físico para poder ser tratada por uno o más usuarios.*
Cable (conexión red)	*La conexión a la red se hace directamente mediante un cable RJ45 al rúter o switch.*
Cliente (Informático)	*Ordenador que se conecta a otro (servidor), mediante la red, para trabajar con la información almacenada en una base de datos.*
Cliente-Servidor	*Modelo de diseño de software ideado para trabajar en red, especialmente con bases de datos, de tal manera que un ordenador (servidor) provea la información a los demandantes (Clientes).*
Control remoto	*Programa informático que se instala en dos dispositivos y permite el control de uno mediante el otro.*
Dispositivo	*Equipo informático, como pudiera ser un ordenador, portátil, Tablet, teléfono o impresora, por ejemplo.*
Dominio (red)	*Gestión de la seguridad, credenciales y recursos de la red mediante la auditoria de un servidor especializado.*
Escritorio remoto	*Control remoto propio, e integrado en algunas versiones, de Windows de forma nativa.*
Ethernet	*Denominación técnica para referirse a una red local.*
Firewall o Cortafuegos	*Herramienta informática, integrada o no en el sistema operativo, diseñado para bloquear el acceso no autorizado al ordenador o a la red, permitiendo el mismo a los sistemas autorizados. A modo de símil, funcionaria como una frontera política.*
Instancia (SQL Server)	*Agrupación centralizada de las bases de datos del usuario que utiliza el programa.*
IP	*El identificador único de un dispositivo en la red.*
IP privada	*El identificador de cada dispositivo en la red local.*
IP pública	*El identificador de nuestro rúter en internet.*
ISP	*Proveedor de Internet (Orange, Vodafone, Jazztel, etc.)*
Latencia	*El tiempo que tarda la información en ir y volver en la red, ya sea local o en internet.*
Lista blanca (Firewall)	*Conjunto de aplicaciones con privilegios especiales excluidas de las reglas del cortafuegos permitiendo así su uso sin limitaciones.*
Microsoft	*Empresa tecnológica internacional con sede en EE. UU. conocida por desarrollar el sistema operativo «Windows» o el paquete ofimático «Office».*
Monopuesto	*Configuración de nuestro programa para trabajar en un único ordenador.*
Nube	*Espacio de almacenamiento y procesamiento de datos y archivos ubicado en internet, al que puede acceder el usuario desde cualquier dispositivo.*
Puerto (Informático)	*Punto de conexión por el que la información fluye entre dispositivos o una web.*
Puesto de red	*Véase «Cliente».*
Red (Informático)	*Conjunto de ordenadores conectados entre sí mediante un medio (normalmente un rúter o Switch) cuya finalidad es compartir información y recursos.*
Red privada	*Red de confianza o segura, como pudiera ser la red de casa o de la oficina.*
Red pública	*Red abierta o protegida pero que no puede garantizarse un mínimo de seguridad. Un ejemplo sería el Wifi de un establecimiento de comida o la de un aeropuerto.*
Router	*Término anglosajón para rúter.*

Rúter	*Dispositivo informático que permite la conexión a internet a una red interna y gestiona la misma.*
Servicios (Windows)	*Programa interno informático que se ejecuta en segundo plano dedicado a una tarea específica.*
Servidor	*Ordenador que por sus características provee de información a otros dentro de la red. Puede ser un tipo de PC dedicado o no.*
Sistema Operativo (SO)	*Software básico y principal cuya finalidad es permitir interactuar con el sistema informático (Como, por ejemplo, Windows, MAC OS o Android, entre otros).*
SQL Server	*Gestor de bases de datos diseñada por Microsoft.*
Software	*Combinación de rutinas y procesos necesarios para que el PC funcione, como, por ejemplo, el sistema operativo o los programas informáticos (antivirus, Office, etc.).*
Switch	*También conocido como «Conmutador», es un dispositivo informático que permite enlazar o interconectar redes internas entre sí.*
TCP/IP	*Protocolo informático especializado en la comunicación de servicios en la red.*
Tipo de red (Windows)	*La identificación dada a la conexión de red existente en Windows, ésta puede ser de dos tipos, privada o pública.*
VPN	*Tecnología de red capaz de conectar un ordenador externo de la red local a la misma mediante internet (requiero de la instalación de un programa).*
Wifi (conexión red)	*Conexión a la red mediante un dispositivo inalámbrico (como un rúter o móvil).*
Windows	*Sistema operativo para PC creado y desarrollado por Microsoft.*

Copia de seguridad

Cualquier sistema informático está expuesto a multitud de factores de riesgo, internos y externos, directos e indirectos, que podrían poner en peligro la integridad lógica y física de los datos hasta el punto de poder sufrir una pérdida total e irremediable. Robos, incendios, inundaciones, golpes, roturas, problemas eléctricos, infecciones de virus, ataques cibernéticos, …son sólo algunos de los problemas que tristemente pueden darse. Por todo ello, la copia de seguridad debe ser un pilar fundamental en el que se base la seguridad de la empresa. Tal es la importancia de las copias de seguridad, que existe el día internacional de la copia de seguridad, el cual se celebra cada 31de mayo, para recordarnos los beneficios de disponer de una copia en caso de emergencia.

Por esta misma razón, todas nuestras aplicaciones disponen de una herramienta totalmente gratuita que, bajo interacción del usuario, realizará la copia de seguridad (accesible desde el menú «Utilidades», «Copias de Seguridad»). Dicho asistente, además servirá para restaurar las copias de seguridad, si fuera necesario.

Adicionalmente a lo dispuesto en el párrafo anterior, si lo prefiere y para mayor comodidad, **es posible automatizar** el proceso mediante la adquisición del módulo especialmente diseñado para programar la realización de las copias de seguridad. Podrá obtener más información contactando con nuestro departamento comercial o llamando al 96 338 79 21 en horario de oficina (de 9 h a 14 h y de 16 h a19 h).

Para más información, puede consultar el documento «Manual copia/restauración de datos» en nuestra web.

Descarga de responsabilidad

AVISO IMPORTANTE:

Microarea no se hace responsable de los posibles daños, alteraciones, ataques o pérdidas de información acaecidos en el servidor, algún ordenador o en la red debido a la manipulación del antivirus, firewall de Windows, rúter o cualquier otra causa relacionada.

De hecho, Microarea recomienda encarecidamente disponer siempre y en todo momento de las herramientas y útiles necesarias para salvaguardar la información, así como garantizar su integridad y protección.

Notas

Notas

Notas


microarea®
software