Redes informáticas

Las necesidades de redes informáticas de una oficina o complejo son muy específicas en función de los presupuestos, el tamaño, la capacidad y las necesidades operativas generales del organismo. Las agencias deberían estudiar la posibilidad de contratar personal especializado en TI y redes para ayudar a configurar las redes de las oficinas y suboficinas.

Instalación de la oficina o del recinto

En la mayoría de las ubicaciones sobre el terreno, habrá una mezcla de varios equipos de red de oficina muy próximos. Entre ellos, cabe destacar:

Conexión a un ISP externo - La conexión a un proveedor de servicios de Internet (ISP) externo puede realizarse a través de Internet por satélite, línea telefónica u otra forma de conexión dedicada a una red proporcionada por el ISP.

Módem - Los módems reciben las señales procedentes de los ISP y las traducen en señales utilizables por las redes domésticas o de oficina. Los módems también contienen información específica del usuario que se utiliza para identificar, rastrear y controlar el tráfico con fines de seguridad y facturación. Sin un módem, un equipo de red doméstico o de oficina sería incapaz de comunicarse con redes externas.

Router -Un router es un dispositivo que divide y gestiona el tráfico de Internet, permitiendo que varios dispositivos informáticos tengan sus propias direcciones IP y MAC y se comuniquen con Internet y entre sí al mismo tiempo a través de una red. Los routers tienen diversas configuraciones y funciones. Algunos pueden supervisar y controlar el tráfico en la red local y otros tienen capacidad wifi. El tipo de router utilizado dependerá de las necesidades operativas.

Cortafuegos -Un cortafuegos es cualquier dispositivo que supervisa y filtra específicamente el contenido de Internet procedente de redes externas. Los cortafuegos son útiles para evitar el software malicioso, la intrusión casual no autorizada en las redes o incluso para bloquear contenidos no permitidos por la política informática de cada organización. En las redes simplificadas, los cortafuegos suelen estar fusionados con módems o routers, pero las redes avanzadas pueden tener cortafuegos independientes con protocolos diferentes para los distintos usuarios del servicio.

Conmutador - Un conmutador de red es como una forma avanzada de enrutador; controla y distribuye Internet entre varios dispositivos conectados en red. Sin embargo, los conmutadores son capaces de supervisar y controlar en detalle hasta el nivel de cada dispositivo. Los conmutadores también se utilizan para filtrar, bloquear y proteger las redes internas, de forma similar a los cortafuegos que protegen de las amenazas externas.

Servidor - Los servidores se definen como ordenadores dedicados por completo a almacenar y compartir archivos dentro de una red. Los servidores pueden ser tan sencillos como ordenadores de sobremesa normales o tan complejos como grandes dispositivos informáticos especializados con requisitos de instalación especiales. En los últimos años, muchas agencias han empezado a utilizar servidores "externos", que alojan y gestionan archivos y datos desde ubicaciones fuera de las oficinas, a veces desde otro país. Los servidores externos son soluciones perfectamente aceptables, pero si los usuarios del servidor tienen una conexión no constante a Internet, puede ser preferible un servidor localizado.

1 ISP externo

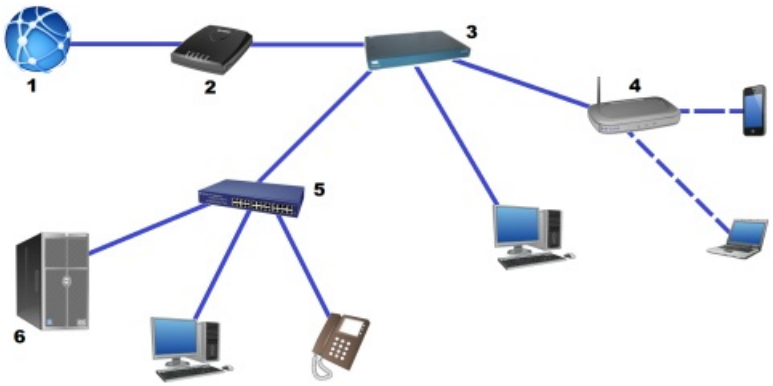
2 Módem

3 Router/cortafuegos

4 Router Wi-Fi

5 Conmutador de red

6 Servidor



Seguridad operativa

Los requisitos de seguridad operativa de cada una de las redes locales deben seguir unas reglas básicas.

Control de acceso - Sólo las personas autorizadas deben tener acceso a las redes y dispositivos informáticos. Todos los ordenadores deben estar protegidos por contraseña, y los routers wifi también deben requerir unas credenciales de acceso. Algunas redes permiten el acceso temporal de invitados, pero las necesidades de configuración especial varían en función del entorno operativo.

Software malicioso - Todos los dispositivos informáticos de las redes deben disponer de algún tipo de software antivirus y los sistemas operativos deben estar siempre actualizados. Las agencias deberían considerar la instalación de cortafuegos o conmutadores con ajustes gestionados para reducir también los intentos de intrusión o la transmisión de software malicioso.

Política de TI - Las agencias deben desarrollar y difundir políticas internas de TI para todos los empleados y usuarios de la red. Las políticas de TI deben incluir normas y reglamentos sobre lo que se considera un comportamiento aceptable y cuáles son las normas de uso de los distintos tipos de hardware, así como establecer directrices en caso de incumplimiento.