



## GLOSARIO DE TÉRMINOS

### CUALIFICACIÓN PROFESIONAL: OPERACIÓN DE REDES DEPARTAMENTALES

**Código: IFC299\_2**

**NIVEL: 2**



**Analizador de red o analizador de protocolos:** Es una herramienta que sirve para examinar en profundidad el tráfico de red, depurar protocolos y aplicaciones de red. Permite al ordenador capturar diversas tramas de red para analizarlas, ya sea en tiempo real o después de haberlas capturado. Por analizar se entiende que el programa puede reconocer que la trama capturada pertenece a un protocolo concreto (TCP, ICMP...) y muestra al usuario la información decodificada. De esta forma, el usuario puede ver todo aquello que en un momento concreto está circulando por la red que se está analizando.

**Agente** (de monitorización): Software que se instala en los sistemas a monitorizar y que recopila información regularmente del sistema en que se ha instalado y la manda al sistema de gestión centralizado que recopila los datos de todos los agentes y la procesa.

**Cliente/Servidor:** Concepto que, en informática de redes, sirve para clasificar los ordenadores: los servidores almacenan información y la entregan a los clientes, que la solicitan.

**Concentrador:** Punto de conexión central para un conjunto de dispositivos de una red configurada en estrella. Actúa a modo de agente de tráfico, dirigiendo la transmisión de los datos entre dichos dispositivos. El número de nodos conectados a un concentrador está limitado por los puertos disponibles de éste pero, si se necesita que la red soporte un número mayor de nodos, se pueden conectar varios concentradores.

**Conmutador:** Dispositivo que realiza traducciones entre aplicaciones o LANs con distintos protocolos (por ejemplo, traducciones de correo electrónico). Tiene múltiples entradas y salidas y, generalmente, posee características centralizadas tales como directorio, tablas de encaminamiento, seguridad y control de accesos. Los conmutadores también pueden distribuirse para formar una estructura que integre LANs o aplicaciones de empresa.

**Cortafuegos** (firewall): Sistema que se interpone entre el servidor de la red local e internet, de tal forma que proteja al primero de ataques malintencionados procedentes de la red y que no han sido convenientemente identificados. Asegura que las comunicaciones entre la red local e internet se realizan conforme a las políticas de seguridad de la empresa. Incorporan elementos de privacidad, autenticación, seguridad.

**Encaminador:** Dispositivo (llamado router en inglés) que ayuda a que los paquetes de datos enviados por la red encuentren su destino. En una estructura en red puede tenerse un puerto para la LAN y otro para el encaminador, o bien múltiples puertos para conectar múltiples encaminadores.



**Encriptación:** Encriptación: Conjunto de técnicas que permiten codificar la información que circula en internet de manera que las personas no autorizadas no puedan leerla ni manipularla.

**Ethernet:** Tecnología de conexión entre ordenadores desarrollada principalmente para redes pequeñas y medianas. Aunque existen cableados distintos, lo más habitual por su precio es usar cables compuestos por 8 hilos trenzados y acabados en una clavija similar a la de las líneas telefónicas, aunque ligeramente más grande. Su velocidad puede oscilar entre 10 Mb/s hasta el Gigabit por segundo, aunque los equipos más extendidos en el mercado doméstico actualmente solo transmiten a 100 Mb/s. El estándar se usa también sobre redes inalámbricas.

**IDS (Sistema de detección de Intrusos):** Sistema que detecta intrusiones no autorizadas en la red local. Se usa para detectar tráfico de red y uso de computadora maliciosos, que no pueden ser detectados por un cortafuegos convencional.

**IPS (Sistema de Prevención de Intrusos):** Son sistemas que se pueden considerar como extensiones de los IDS, pero que presentan una capacidad proactiva y una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos. La diferencia con el IDS es que este alerta al administrador ante la detección de un posible intruso (usuario que activó algún Sensor), mientras que un Sistema de Prevención de Intrusos establece políticas de seguridad para proteger el equipo o la red de un ataque; se podría decir que un IPS protege al equipo proactivamente y un IDS lo protege reactivamente.

**Interfaz (de usuario):** La interfaz de usuario es el medio con que el usuario puede comunicarse con una máquina, un equipo o una computadora, y comprende todos los puntos de contacto entre el usuario y el equipo, normalmente suelen ser fáciles de entender y fáciles de accionar.

**Internet:** Red mundial de ordenadores, tanto ordenadores personales como superordenadores, que emplean el protocolo TCP/IP para comunicarse. Ofrece una gran cantidad de servicios a todo el que esté conectado a ella.

**Intranet:** Red local que utiliza, total o parcialmente, las tecnologías de la Internet.

**IP (dirección IP):** Abreviatura de Internet Protocol. Una dirección IP sirve para identificar de forma inequívoca a un equipo en una red. No puede existir más de un equipo con la misma dirección IP dentro de una misma red. En la versión más común actualmente (IPv4) está formada por una secuencia de cuatro números de 0 a 255 (un byte cada uno) y separados por puntos. La versión IPv6 está



formada por 8 bytes escritos en forma hexadecimal y separados por un símbolo “.”.

**Mac** (dirección Mac): Siglas del inglés Media Access Control. Es una dirección que usualmente está compuesta por números y letras asignado a los equipos que forman parte de una red, que es único e identifica su lugar dentro de la red. El comité de IEEE asigna bloques de direcciones a los fabricantes de tarjetas de red. De esta forma se asegura que no existan dos tarjetas de red con el mismo Mac address.

**MIB** (Management Information Base): La Base de Información Gestionada es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una red de comunicaciones. Es parte de la gestión de red definida en el modelo OSI. Define las variables usadas por el protocolo SNMP para supervisar y controlar los componentes de una red. Está compuesta por una serie de objetos que representan los dispositivos (como enrutadores y conmutadores) en la red. Cada objeto manejado en un MIB tiene un identificador de objeto único e incluye el tipo de objeto (tal como contador, secuencia o gauge), el nivel de acceso (tal como lectura y escritura), restricciones de tamaño, y la información del rango del objeto.

**NAT** (Network Address Translation o Traducción de Dirección de Red): Es un mecanismo utilizado por encaminadores IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo. Su uso más común es permitir utilizar direcciones privadas (definidas en el RFC 1918) para acceder a Internet.

**Online**: Conectado directamente a una red telemática (ej. internet) y en disposición de funcionar en ella.

**OSI**: Interconexión de Sistemas Abiertos (Open Systems Interconnect). Es el protocolo en el que se apoya Internet. Establece la manera como se realiza la comunicación entre dos computadoras a través de siete capas: Física, Datos, Red, Transporte, Sesión, Presentación y Aplicación.

**PAT** (Port Address Translation): Es una característica del estándar NAT, que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna. Permite que una sola dirección IP sea utilizada por varias máquinas de la intranet. Con PAT, una IP externa puede responder hasta a ~64000 direcciones internas. La traducción de los puertos se apoya en el hecho de que el puerto de origen carece de importancia



para la mayoría de los protocolos. Igual que NAT, se sitúa en la frontera entre la red interna y externa, y realiza cambios en la dirección del origen y del receptor en los paquetes de datos que pasan a través de ella. Los puertos (no las IP), se usan para designar diferentes hosts en la intranet.

**Productos o servicios digitales:** Son aquellos bienes o servicios que pueden ser pedidos y entregados directamente a los ordenadores a través de internet, por ejemplo: música, vídeos, juegos, software informático, prensa on-line, servicios de consultoría.

**Protocolos:** Normativas estándar para las telecomunicaciones en general y la comunicación entre ordenadores en particular. El software de los ordenadores en red tiene que diseñarse para cumplir esta normativa. Ciertos protocolos se usan en las transferencias realizadas sobre LANs físicas (ApleTalk y PPP, entre otros) y otros como FTP y HTTP se "montan" sobre los primeros para completar la distribución de contenidos multimedia, correo electrónico, archivos de datos, etc.

**Protocolos seguros (SSL/TSL):** Secure Sockets Layer (SSL) y Transport Layer Security (TLS) son protocolos criptográficos que permiten realizar comunicaciones seguras a través de internet

**Rack:** El Rack es un armario que ayuda a tener organizado todo el sistema informático de una empresa. Posee unos soportes para conectar los equipos con una separación estándar de 19". Debe estar provisto de ventiladores y extractores de aire, además de conexiones adecuadas de corriente. Hay modelos abiertos que sólo tienen los soportes con la separación de 19" y otros más costosos cerrados y con puerta panorámica para supervisar el funcionamiento de los equipos activos y el estado de las conexiones. También existen otros modelos que son para sujetar en la pared, estos no son de gran tamaño.

**Red de Área Local (LAN):** Una red de área local, red local o LAN (del inglés local area network) es la interconexión de varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a varios edificios cercanos. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, o fábricas, por ejemplo. El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información, de forma que permite a sus usuarios el intercambio de datos y la compartición de recursos

**Red Privada Virtual:** Red en la que al menos alguno de sus componentes utiliza la red Internet pero que funciona como una red privada, empleando para ello técnicas de cifrado.



**RMON (Remote Monitor, monitor remoto)** Es un monitor de red remoto que permite recolectar información acerca del tráfico en la red.

**Sesión Remota:** Uso de los recursos de una computadora desde una terminal la cual no se encuentra cercana a dicha computadora.

**Sistemas de monitorización:** Permiten hacer un seguimiento de los valores recopilados por todos los elementos que forman la red. Estos sistemas de monitorización dispondrían de una interfaz para visualizar los datos capturados en la pantalla de nuestro ordenador, teléfono móvil o PDA. También se podrían obtener estadísticas, gráficas, realizar consultas a un historial de datos.

**Sistema Operativo:** Operating System (OS) en inglés. Programa especial el cual se carga en una computadora al encenderla, y cuya función es gestionar los demás programas, o aplicaciones, que se ejecutarán, como por ejemplo, un procesador de palabras o una hoja de cálculo, un juego o una conexión a Internet. Windows, Linux, Unix, MacOS son todos sistemas operativos.

**SNMP:** El Protocolo Simple de Administración de Red es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

**TCP/IP:** Siglas tomadas de Transfer Control Protocol/Internet Protocol, es el protocolo en el que se basa todo el tráfico en Internet. Cualquier ordenador en Internet debe tener una única dirección IP. Ésta consta de un conjunto de cuatro cifras de la forma xxx.xxx.xxx.xxx donde xxx puede ser un número comprendido entre 0 y 255. Los ordenadores de Internet utilizan esta dirección para llamar a otros, de manera similar a como lo hacen los teléfonos.

**UTP:** del inglés: Unshielded Twisted Pair, par trenzado no apantallado es un tipo de cable de par trenzado que no se encuentra apantallado y que se utiliza principalmente para comunicaciones. Se encuentra normalizado de acuerdo a la norma estadounidense TIA/EIA-568-B y a la internacional ISO/IEC 1180

**WAN:** Derivada de Wide Area Network, la expresión alude a una red de área ancha o a un conjunto de redes locales conectadas entre sí.

**Web (WWW):** Web o las siglas que corresponden a World Wide Web o telaraña mundial, conjunto de sitios Web que se encuentran en la Internet y a los que se accede a través de una dirección URL. Para la exploración de otras páginas de ese sitio o de páginas de sitios distintos se usan enlaces de hipertexto. Familiarmente se la llama la Web.



**Webhosting:** Conjunto de servicios que posibilitan la utilización de un servidor externo y funcionar, a todos los efectos, como si se hubiera realizado una gran inversión en equipos y conexiones para el desarrollo de la tecnología Internet en los aspectos más interesantes para la empresa.