ESPECIALIDAD FORMATIVA
GESTIÓN DE REDES DE VOZ Y DATOS

IFCM0310

UF1874: Mantenimiento de la infraestructura de la red de comunicaciones

* Bibliografía usada en este documento:

UF1874: Mantenimiento de la infraestructura de la red de comunicaciones, Autor: J. A. Jimenez Toro, EDITORIAL ELEARNING S.L. Edición: 5.0

Capturas de pantalla y textos electrónicos de varias web únicamente para ilustrar la actividad educativa

Luis Orlando Lázaro Medrano

Contenido

1. Infraestructura de la red de comunicaciones

1.1. Elementos de conmutación y transmisión de la red

En una red de comunicación tenemos un conjunto de elementos que comunican a través de una serie de enlaces o líneas de transmisión. En una red se produce un intercambio de información entre dos puntos, la información se envía desde un origen a un destino por un enlace. Toda red de comunicación está compuesta por una serie de elementos.

- Estaciones: Son dispositivos que envían o reciben información, como por ejemplo computadores.
- Nodos: Se encargan de la comunicación entre las estaciones.
- Enlaces: Líneas de transmisión por donde "viaja" la información.

La red de comunicación más importante en la actualidad es Internet, que es un conjunto de redes de diferentes tecnologías que se comunican entre sí mediante una serie de protocolos. Esto permite que una red que este en China se pueda comunicar con otra red en España sin importar la tecnología que utilicen. Prácticamente todos los servicios que proporcionaban otras redes de comunicaciones como teléfono, televisión, radio, etc. están disponibles en Internet.

Enlaces

Los enlaces las líneas de transmisión por donde se transporta la información, los enlaces pueden ser físicos (cables) o enlaces inalámbricos. Para poder enviar o recibir información por los enlaces se necesita un componente denominado tarjetas de red, dependiendo de la tecnología utilizada se necesitará una tarjeta específica.

Enlace físicos	La información se transporta a través de un cable, se denominan medios de comunicación guiados	– Par trenzado – Cable Coaxial – Fibra óptica
Enlaces inalámbricos	La información no está unida a un enlace físico, sino que el medio de propagación que utiliza es el aire.	– Radio – Microondas – infrarrojo

Enlaces físicos

Se realiza una comunicación guiada entre dos o más partes de red de comunicación, que se realiza a través de un elemento físico por donde se conduce la comunicación, por algún tipo de cable. La velocidad y la capacidad de transmisión dependen de la distancia y del tipo de red utilizada (multipunto o punto a punto). La comunicación proporciona ciertas ventajas, como la seguridad, la señal se comunica a través de un cable, para acceder a la señal es necesario tener acceso físico al enlace. Otra ventaja es la protección ante interferencias, el cable proporciona cierta protección, depende del tipo de cable, ante posible interferencia. Con las dos ventajas anteriores la velocidad de transmisión puede ser, teniendo en cuenta las limitaciones descritas en el párrafo anterior. Muy alta.

El record de velocidad de transmisión (febrero 2013) es 1,05 Petabits por segundo a través de fibra óptica fabricada especialmente para este experimento. Realizado por equipo de investigadores de Universidad de Santiago de Compostela, Nec Laboratories América, Corning y la Universidad de Princeton.
1 petabit = 1015 bits = 1.000.000.000.000.000 bits.

Par Trenzado

Consiste en dos cables de cobre envuelta en un aislante entrelazado para anular las interferencias de fuentes externas e interferencias electromagnéticas. Los pares trenzados se trenzan a diferentes distancias para atenuar las interferencias y la longitud del trenzado varía entre 5 cm y 15 cm. Los conductores que forman parte del par pueden tener un grosor entre 0,4 mm y 0,9 mm.
El par trenzado se utiliza para señales analógicas como señales digitales, es el medio utilizado en redes de telefonía. También se utilizan dentro de los edificios para las redes comunicación.
En telefonía, se utiliza para el bucle de abonado, que es la conexión del terminal del usuario con la central, este tipo de instalación es el utilizado para transportar tráfico de voz.

En redes de área local son muy utilizadas con velocidades de hasta un 1 Gbps, con los dispositivos apropiados. El par trenzado es menos costoso que cualquier otro medio de comunicación guiado y es el más sencillo de instalar, pero permite menores distancias, menor ancho de banda y menor de velocidades que otros medios guiados.
En la transmisión de señales analógicas se necesitan amplificadores cada 5 km o 6 km. Para señales digitales se requiere un repetidor cada 2 km o 3 km.
El par trenzado es muy vulnerable a las interferencias y el ruido, para evitar esto, se puede apantallar el cable o trenzado utilizando diferente longitud de trenzado. Tenemos dos tipos de par trenzado; Apantallado (STP), no Apantallado (UTP) y apantallado con papel de plata (FTP). El cable apantallado recubre el par trenzado con una malla metálica que reduce las interferencias, proporciona mayores velocidades aunque es más costoso y difícil de utilizar. El cable no apantallado es el utilizado en telefonía debido a que el rendimiento que proporciona es suficiente para el tráfico de voz, es más barato y manejable que el STP, este tipo de cable es muy utilizado en las instalaciones de los edificios. Por último, el cable apantallado con papel de plata, son unos cables de pares que poseen una pantalla conductora global en forma trenzada, respecto a la calidad sería un término medio entre el STP y UTP.
Dependiendo de la calidad del cable par trenzado, podemos distinguir varias categorías:

Categoría	Ancho de banda	Aplicaciones
Categoría 1	50 MHZ	Líneas telefónicas y módem de banda ancha.
Categoría 2	40 MHz	Cable para conexión de antiguos terminales.
Categoría 3	250 MHz	10BASE-T and 100BASE-T4 Ethernet.
Categoría 4	200 MHz	16 Mbit/s Token Ring.
Categoría 5	150 MHz	100BASE-TX y 1000BASE-T Ethernet.
Categoría 5e	175 MHz	100BASE-TX y 1000BASE-T Ethernet.
Categoría 6	300 MHz	1000BASE-T Ethernet.
Categoría 7a	1200 MHz	Para servicios de telefonía, Televisión por cable y Ethernet 1000BASE-T en el mismo cable.
Categoría 8	1200 MHz	Norma en desarrollo. Aún sin aplicaciones.
Categoría 9	25000 MHz	Norma en creación por la UE.

Cable coaxial

Está compuesto por dos conductores, un conductor cilíndrico externo que rodea a un cable conductor interior y este conductor se mantiene a lo largo del eje axial mediante una serie de anillos aislantes regularmente espaciados o mediante una materia sólida - dieléctrica. El conductor exterior se protege con una cubierta o funda. El cable coaxial tiene un diámetro aproximado entre 1 cm y 2,5 cm. Comparado con el par trenzado, el cable coaxial se puede usar para cubrir distancias mayores así como para conectar un número mayor de estaciones en líneas compartidas.

El cable coaxial se utiliza en múltiples aplicaciones como:

- Televisión.
- Telefonía a larga distancia.
- Enlace a computadoras a corta distancia.
- En redes de área local.

El cable coaxial se utiliza en televisión por cable hasta el domicilio del usuario, permite llevar cientos de canales, y muy utilizado en la telefonía para transmitir a largas distancia, utilizando FDM (multiplexación por división de frecuencia) permite transportar simultáneamente miles de canales de voz.

El cable coaxial se usa para transmitir tanto señales analógicas como digitales. Comparado con el par trenzado ofrece mayores velocidades y tiene más resistencia a interferencias, debido a su construcción, como limitaciones ofrece poca inmunidad al ruido.
Para el envío a largas distancias se necesitan amplificadores cada varios kilometro, la distancia de los amplificadores es menor cuanto mayor sea la frecuencia con el que se envía la señal.
Existen múltiples tipos de cable coaxial, cada uno con un diámetro e impedancia diferentes. Normalmente se utilizan dos tipos de cables:

- Cable coaxial delgado: tiene un diámetro de 6 mm que lo hace muy flexible y se puede utilizar en la mayoría de las redes. La longitud máxima de transmisión es de 185, sin pérdida de señal. Utiliza la norma 10 Base 2 en redes LAN.
- Cable coaxial grueso: tiene un diámetro de 12 mm, la longitud máxima de transmisión sin pérdida de señal es de 500 metros y proporciona un ancho de banda de 10 Mbps Por contra, es un cable menos flexible debido a su grosor. Utiliza la norma 10 Base 5 en redes LAN.

Dentro del cable coaxial delgado hay diferentes tipos en función del núcleo.

Cable	Descripción
RG-58 / U	Núcleo central que consiste en un solo hilo de cobre
RG-58 A/U	Trenzado
RG-58 C/U	Versión militar del RG-58 A/U
RG-59	Transmisión de banda ancha (televisión por cable)
RG-6	Diámetro más grueso, recomendado para frecuencias más altas que las del RG-59
RG-62	Red Arcnet

El cable coaxial utiliza diferentes tipos de conectores.

Tipo conector	Descripción
BNC	Usados en la familia RG-58 y RG-59, se hizo muy popular por ser utilizado en las primeras redes Ethernet. Consiste en un conector tipo macho instalado en cada extremo del cable. Este conector tiene un centro circular conectado al conductor del cable central y un tubo metálico conectado en el parte exterior del cable. Un anillo que rota en la parte exterior del conector asegura el cable mediante un mecanismo de bayoneta y permite la conexión a cualquier conector BNC tipo hembra.
N	Conector para cable coaxial robusto, resistente a la intemperie, de tamaño medio y con buenas prestaciones en radiofrecuencia hasta 11 GHz, siendo el primero con buenas propiedades en la banda de microondas.
SMA	Conector roscado utilizado en microondas. Utiliza un dieléctrico de politetrafluoretileno (PTFE) que centra la parte interior a lo largo del plano de acoplamiento. La variabilidad en este acoplamiento y la propia construcción de los conectores limita la repetibilidad de la impedancia tipica. Por este motivo y el hecho de que está garantizado para tan solo un número limitado de ciclos de conexión. Existen SMA inversos, con la tuerca en la hembra, utilizados como conector en antenas wifi.
TNC	Es una versión con rosca del conector BNC. Tiene una impedancia de 50 Ω y el margen de frecuencias preferible a las que opera va de entre 0 a 11 GHz. Las frecuencias de microondas tiene un mejor comportamiento que el BNC.

Fibra Óptica

Es un medio flexible y delgado empleado para la transmisión de datos a alta velocidad, un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado y se propaga por el interior de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, en función de la ley de Snell. La fuente de luz puede ser láser o LED.

Un cable de fibra óptica tiene una forma cilíndrica y está formada por tres secciones concéntricas:

- Núcleo: es la sección más interna, está constituido por una o varias fibras de cristal o plástico, con un diámetro entre 8 y 100 micras.
- Revestimiento: rodea a cada fibra, compuesto por otro cristal o plástico con propiedades ópticas distintas a las del núcleo. La separación entre el núcleo y el revestimiento actúa como un reflector, confinando así el haz de luz, ya que de otra manera escaparía del núcleo.
- Cubierta: la capa más exterior que envuelve a uno o varios revestimientos, está construido por plástico y otros materiales dispuestos en capas para proporcionar protección.

Las características diferenciales de la fibra óptica son.

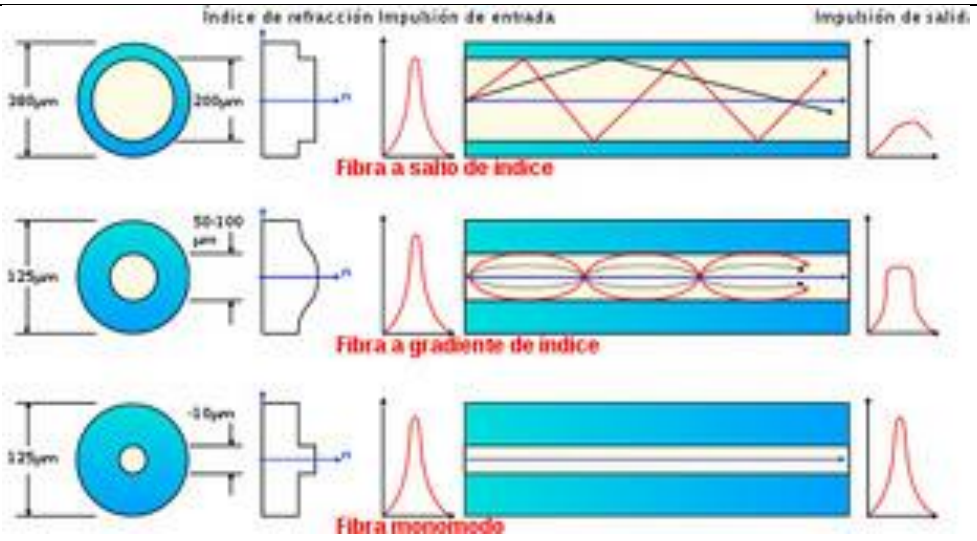
- Alta capacidad: ancho de banda y velocidad muy altas.
- Tamaño, peso bajo y gran flexibilidad: el núcleo de la fibra, por donde la luz es transmitida, está hueco - la luz es transmitida por el vacío-, y los materiales que se utilizan, plásticos y cristales, hacen que la fibra tenga un peso bajo. La reducción es debida a su ancho de banda requiere menos fibras para transmitir gran cantidad de datos.
- Atenuación pequeña: Atenuación muy pequeña independiente de la frecuencia, lo que permite salvar distancias importantes sin elementos activos intermedios.
- Aislamiento electromagnético: no se ve afectada por los efectos del campo electromagnético.
- Separación entre repetidores: la distancia entre repetidores es del orden de decenas de kilómetros.
- Gran seguridad.
- Resistencia a factores ambientales.

Las principales desventajas de la fibra óptica.

- La alta fragilidad de las fibras.
- Necesidad de usar transmisores y receptores más caros.
- La fibra óptica no transmite energía eléctrica, esto limita su aplicación donde el terminal de recepción debe ser energizado desde una línea eléctrica. La energía debe proveerse por conductores separados.
- La necesidad de efectuar, en muchos casos, procesos de conversión eléctrica-óptica.

La fibra óptica propaga internamente el haz de luz que transporta la señal codificada de acuerdo con el principio de reflexión total. Este fenómeno se da en cualquier medio transparente que tenga un índice de refracción mayor que el medio que lo contenga. Según el modo de propagación tendremos dos tipos de fibra óptica: multimodo y monomodo.

Multimodo



Las líneas estas no creo que estén bien expresadas, personalmente lo pondría así: Los rayos que inciden con diferentes ángulos, dependiendo del grado del ángulo, se reflejan dentro del núcleo de la fibra. Mientras que para otros ángulos de incidencia, son absorbidos por el material que forma el revestimiento. Este tipo de propagación se llama multimodal de índice discreto, aludiendo el hecho de que hay multitud de ángulos para los que se da la reflexión total. En la transmisión existen múltiples caminos que verifican la reflexión total, con diferente tiempo de propagación, esto provoca que los pulsos de luz se dispersen en el tiempo limitando la velocidad de transmisión.
Si varía el índice de refracción varia (no es constante) tenemos el multimodo de índice gradual. En este tipo de fibra los rayos de luz avanzan en forma de curva.

Monomodo

Si se reduce el radio del núcleo de la fibra, de tal modo que solo pueda transmitirse un solo modo de luz. El modo de propagación es paralelo a la fibra, esto proporciona mayores prestaciones porque no se produce distorsión.
Los sistemas que implementan fibras monomodo utilizan como fuente de luz un láser infrarrojo. El haz de luz del láser generado por el emisor ingresa al núcleo en un ángulo de 90 grados. Consecuentemente, los haces de luz que transportan datos sobre una fibra monomodo son transmitidos en línea recta directamente por el centro del núcleo.
Este tipo de fibras permiten alcanzar grandes distancias (hasta 400 km máximo, mediante un láser de alta intensidad) y transmitir elevadas tasas de información (decenas de Gb/s).
Como desventajas, tienen un mayor coste, mayor fragilidad (debido a las dimensiones de la fibra) y la potencia transmitida es menor.
Hay dos tipos de fuentes de luz que se utilizan en la fibra óptica. Ambos son dispositivos semiconductores que emiten un haz de luz cuando se le aplica una tensión.

- LED: Utilizan una corriente de 50 a 100 mA, su velocidad es lenta, solo se puede usar en fibras multimodo, pero su uso es fácil y su tiempo de vida es muy grande, además de ser económicos.
- Laser: Este tipo de emisor usa una corriente de 5 a 40 mA, son muy rápidos, se puede usar con los dos tipos de fibra, monomodo y multimodo, pero por el contrario su uso es difícil, su tiempo de vida es largo pero menor que el de los LEDs y también son mucho más costosos.

En fibra óptica tenemos varios tipos de conectores para la conexión de las líneas de fibra a un elemento, ya puede ser un transmisor o un receptor. Algunos de estos conectores son:

Tipo	Descripción
FC	Usado para la transmisión de datos y en las telecomunicaciones.
ST	Usado en redes de edificios y en sistemas de seguridad.
SMA	Usado en dispositivos electrónico con algunos acoplamientos óptico. Además de uso Militar.
LC	Conector más pequeño y sofisticado, usado equipos de comunicación de alta densidad de datos.
SC	Conector de bajas pérdidas, muy usado en sistemas de seguridad y en redes de edificio.

Los conectores suelen llevar una serie de acrónimos: PC, APC, UPC; indicando tipo de conexión, es decir Phyical Contact (PC) ó Contacto Físico. Angle (A) con ángulos de inclinación en la punta. Y Ultra (U) conexión de muy bajas pérdidas.

Enlaces Inalámbricos

La comunicación se realiza por un medio no guiado, a través del espacio, la transmisión inalámbrica se realiza por medio de ondas electromagnéticas. Para realiza una comunicación inalámbrica tanto el receptor como el emisor deben tener algún tipo de antena para realizar la transmisión.

Según el rango de frecuencias que es utilizado para transmitir. El medio de transmisión pueden ser las ondas de radio, las microondas terrestres o por satélite, y los infrarrojos.

Ondas de radio

Transmiten señales en baja frecuencia y son omnidireccionales, su banda de frecuencia está entre 3Khz y 300 GHz. Tienen múltiples aplicaciones, en función de la frecuencia utilizada, como emisiones de radio, redes inalámbricas, televisión.etc.

Cuando la onda de radio actúa sobre un conductor eléctrico (la antena), induce en él un movimiento de la carga eléctrica (corriente eléctrica) que puede ser transformado en señales de audio u otro tipo de señales portadoras de información. No es necesario el uso de antenas parabólicas.

El emisor tiene como función producir una onda portadora, cuyas características son modificadas en función de las señales (audio o vídeo) a transmitir. Propaga la onda portadora así modulada. El receptor capta la onda y la «demodula» para hacer llegar al espectador auditor tan solo la señal transmitida.

Las ondas de radio se propagan a la velocidad de la luz. Es prácticamente constante y su valor es 300.000.000 metros por segundo.

Microondas

Ondas electromagnéticas que trabajan en el rango de frecuencias entre 300 MHZ y 300 GHz. Las microondas pueden ser generadas de varias maneras, generalmente divididas en dos categorías: dispositivos de estado sólido y dispositivos basados en tubos de vacío. Tenemos dos tipos de microondas.

- Microondas terrestres: Utilizan una antena parabólica y se utiliza en comunicaciones punto a punto. Las antenas deben tener contacto visual para poder transmitir, por ese motivo se suelen montar en sitios altos. Para conseguir transmisiones a largas distancias se concatenan distintas antenas. Se usan principalmente en servicios de telecomunicaciones de larga distancia, como televisión o voz. Su banda de frecuencias está comprendida entre 1 y 40 GHz, cuanto mayor sea la frecuencia utilizada mayor es el ancho de banda y mayor la velocidad. La principal causa de pérdidas en la señal es debido a la atenuación, pérdida de potencia sufrida por la misma al transitar por cualquier medio de transmisión, que puede aumentar por la lluvia. Los repetidores o amplificadores se suelen situar entre 10 a 100 km de separación.
- Microondas por satélite. Utiliza un satélite de comunicaciones, en órbita geoestacionaria, para retransmitir la señal y se usa como enlace entre dos o más estaciones terrestres. El satélite recibe la señal en una banda de frecuencia (señal ascendente), la amplifica o repite y la retransmite en otra banda de frecuencia (señal descendente). Cada satélite opera en una serie de frecuencias

denominadas canales transpondedores. Las microondas por satélite se utilizan en redes de multidifusión, se utilizan en televisión, telefonía a larga distancia, redes privadas.

Infrarrojos

Se enlazan transmisores y receptores que modulan la luz infrarroja no coherente. Deben estar alineados directamente o con una reflexión en una superficie. No pueden atravesar las paredes. Los infrarrojos van desde 300 GHz hasta 384 THz. La transmisión se puede realizar en tres tipos de modos.

- Modo punto a punto: el emisor y el receptor deben estar cerca y alineados.
- Modo Casi-difuso: las estaciones se comunican entre sí, por medio de superficies reflectantes. No es necesaria la línea de visión entre dos estaciones, pero sí deben de estarlo con la superficie de reflexión.
- Modo difuso: El poder de salida de la señal óptica de una estación, debe ser suficiente para llenar completamente el total del cuarto, mediante múltiples reflexiones, en paredes y obstáculos del cuarto. Por lo tanto la línea de vista no es necesaria y la estación se puede orientar hacia cualquier lado.

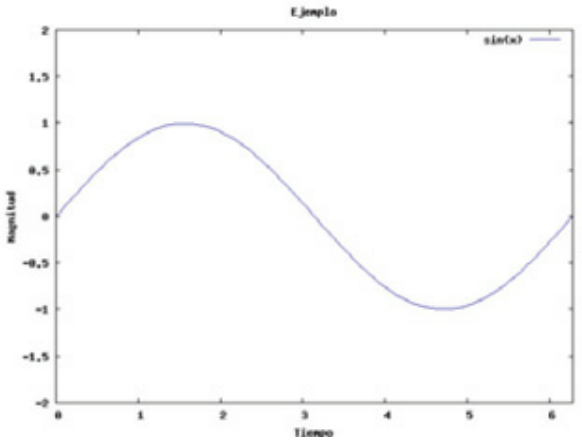
Datos: Digitales y Analógicos

Como en toda de red comunicación se transmiten datos entre dos puntos, estos datos se transmiten mediante señales que son generadas mediante electromagnetismo. Hay dos tipos de datos; digitales y analógicos, que son emitidas por sus respectivas señales; digital y analógica.

Dato analógico	Toma valores en un intervalo continuo que varían continuamente. Son utilizados en el audio y vídeo.
Dato digital	Toma valores en un rango discreto, donde se definen los valores que se tomarán del dato. Un ejemplo de datos digital lo encontramos en la computación que utilizan datos binarios que es un dato digital que solo puede escoger entre dos valores; 0 y 1.

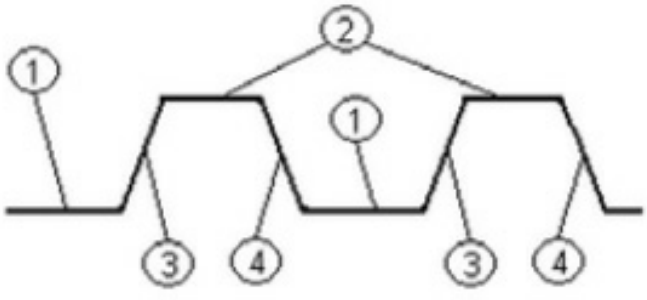
Tenemos dos tipos de señales para representar esos datos.

- Señales analógicas: es una onda electromagnética que varía continuamente y puede propagarse a través de una serie de medios.



Dato es cualquier entidad capaz de transportar información.

- Señales digitales: Es una secuencia de pulsos de tensión que se pueden transmitir a través de un medio conductor.



Los datos analógicos o digitales deben ser codificados mediante señales analógicas o digitales para realizar la transmisión. Tenemos cuatro posibles combinaciones.

- Datos digitales, señales digitales: se codifican los datos asignando un nivel de tensión al uno y otro nivel para cero. Es la mejor para codificar datos digitales.
- Datos digitales, señales analógicas: es utilizado en los modem que convierten los datos digitales en señales analógicos para la transmisión.
- Datos analógicos, señales digitales: datos analógicos como la voz se digitalizan para ser enviado por señales digitales.
- Datos analógicos, señales analógicas: los datos se modulan mediante una portadora para generar una señal analógica.

Cada una de estas combinaciones se utilizarán en función de varios factores y cada combinación utilizan diferentes técnicas para codificar los datos.

Datos digitales – señales digitales

Una señal digital es una secuencia de pulsos de tensión discretos y discontinuos. Los datos digitales (datos binarios) se transmiten codificando cada bit de datos en los elementos de señal, cada pulso corresponde a un elemento de señal.

Para realizar una transmisión de señales digitales se utilizan diferentes esquemas de codificación que realizan la correspondencia entre los bits de datos y los elementos de la señal.

No retorno a nivel cero (NRZ-L)	0 = nivel alto. 1 = nivel bajo.	Asigna un nivel de tensión diferente a cada uno de los valores binarios.
No retorno a nivel cero invertido (NRZI)	0= no hay transición al comienzo del intervalo. 1 = transición al comienzo del intervalo.	Mantiene constante el nivel de tensión durante un bit, la transición entre nivel se utiliza para asignar los valores a los datos binarios.
Bipolar-AMI	0 = no hay señal. 1 = nivel positivo o negativo, alternando.	Los 1 siempre fuerzan una transición.
Pseudoternaria	0 = nivel positivo o negativo, alternando. 1 = no hay señal.	Similar al Bipolar, pero cambiando las asignaciones.
Manchester	0 = transición de alto a bajo en mitad del intervalo. 1 = transición de bajo o alto en mitad del intervalo	Siempre hay una transición en mitad del intervalo que se utiliza para la sincronización a la vez que sirve para transmitir datos.
Manchester diferencial	0 = transición al principio del intervalo. 1 = no hay transición al principio del intervalo.	La transición al principio del intervalo solo se usa para sincronización.
B8ZS	Una cadena de ocho ceros se reemplaza por una cadena que tiene dos violaciones de código.	
HDB3	Una cadena de cuatro ceros se reemplaza por una cadena que tiene una violación de código.	

La señal digital tiene como ventaja que es más económica y menos susceptible a las interferencias de ruido que las señales analógicas. Como desventaja tiene que las señales digitales sufren más con la atenuación que las señales analógicas. La atenuación en las señales digitales se refiere a la reducción (atenuación) de la energía que afecta a las frecuencias altas, los pulsos se hacen más pequeños a la vez que se suavizan y pueden provocar con facilidad pérdida de información contenida en la señal.

Datos digitales – señales analógicas

Se deben convertir los datos digitales utilizando un modem que los convierte a datos analógicos y viceversa.

Para trasmitir señales analógicas se modula la señal, la modulación implica una modificación y afecta a uno de los tres parámetros que componen una señal analógica: amplitud, frecuencia y fase.

Se utilizan una serie de técnicas para modular la señal, cada una modifica un parámetro de la señal.

- Modulación por desplazamiento de frecuencia (ASK): Los dos valores binarios se representan con dos amplitudes diferentes. Es habitual que el cero se represente con una ausencia de amplitud y el uno con amplitud constante.
- Modulación por desplazamiento de frecuencia (FSK): Los dos valores binarios se representan con dos frecuencias diferentes próximas a la frecuencia de la portadora.
- Modulación por desplazamiento por fase (PSK): la señal portadora se desplaza para representar los datos digitales. Se utilizan dos fases para representar los dos dígitos binarios, también se denomina BPSK (PSK binario). Otra opción es utilizar cuatro fases, con un desplazamiento que es múltiplo de

90º, en este caso se transmite dos bits, esta modulación se denomina QPSK. También existe un PSK multinivel que permite transmitir más de dos bits, escogiendo múltiples fases.

Datos analógicos- señales digitales

El proceso de convertir datos analógicos a datos digitales se conoce como digitalización. El dispositivo que se encarga de realizar la conversión analógica a digital se denomina códec. Este dispositivo utiliza una serie de técnicas para realizar el proceso, las dos más utilizadas son:

- Modulación por impulsos codificados (PCM): utiliza el teorema de muestreo para realizar la conversión.
- Modulación delta (DM): que simplifica la complejidad de PCM.

Datos analógicos – señales analógicos

Existen dos razones para la transmisión de señales analógicas mediante modulación analógica:

- Para realizar una transmisión más efectiva que necesita una frecuencia mayor, esto es útil para las transmisiones inalámbricas.
- Permite utilizar multiplexación por división en frecuencias.

Las técnicas más conocidas para realizar modulación analógica son:

- Modulación por amplitud (AM): es una modulación muy simple y funciona mediante variación de la amplitud de la señal transmitida en relación con la información que se envía.
- Modulación por frecuencia (FM): es una modulación angular que transmite información a través de una onda portadora variando su frecuencia.
- Modulación por fase (PM): es una modulación angular, la fase de la onda portadora varía en forma directamente proporcional de acuerdo con la señal modulante.

Nodos

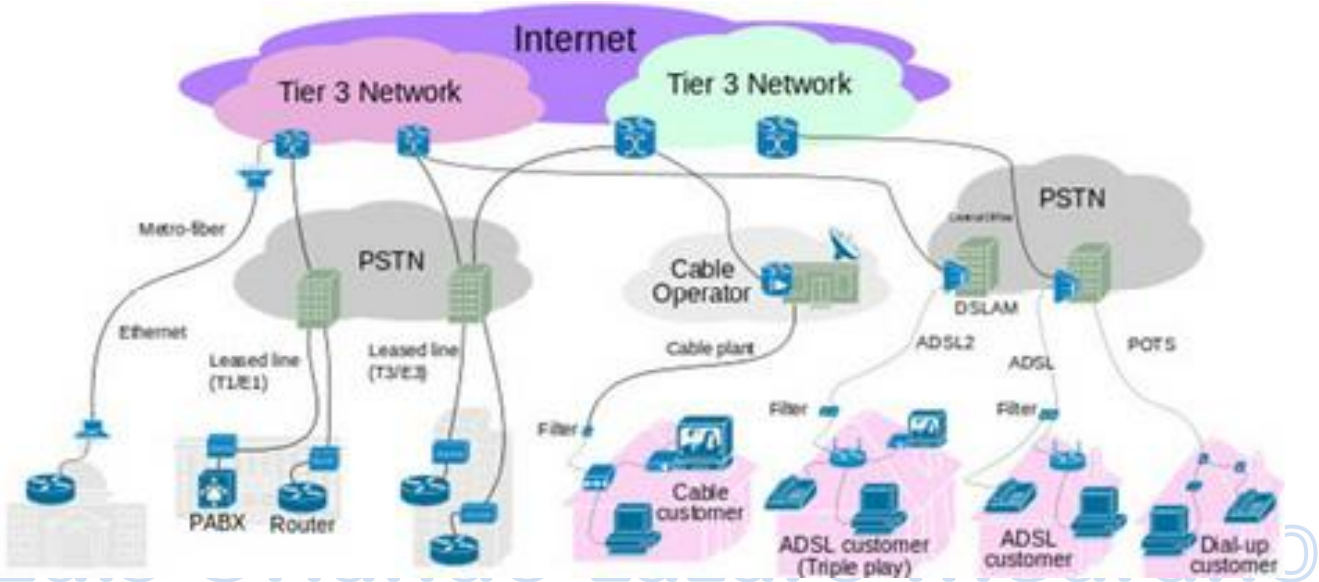
Los nodos son una parte esencial de toda red de comunicaciones son los encargados del transporte de la información entre dos estaciones. Los nodos pueden estar conectados a una estación o más estaciones, con otros nodos o con un conjunto de estaciones y nodos.

Tenemos diferentes tipos de dispositivos hardware que se colocan en un nodo, dependiendo de diferentes factores se deberá escoger un hardware u otro, algunos de los dispositivos hardware se describirán en este módulo serán: módem, router, punto de acceso y switch.

Una red comunicaciones necesita un conjunto de dispositivos hardware para su funcionamiento.

Anteriormente, se han definidos las estaciones y los nodos, en este apartado se describirán diferentes tipos de hardware.

Ejemplo de red de comunicación con diferentes tecnologías.



Dependiendo de la tecnología utilizada podemos distinguir:

- Redes punto a punto.
- Redes difusión.

Redes punto a punto

Un enlace punto a punto es aquel que la comunicación se realiza entre dos puntos, esta es la forma de comunicación más sencilla. Siempre hay un emisor que envía un mensaje y un receptor que recibe el mensaje, pero estos roles se pueden intercambiar. En las redes punto a punto se tiene la capacidad de enviar o recibir por parte de los nodos. Son redes muy fáciles de construir y baratas, si la red empieza a crecer se empeora su eficiencia y es mejor utiliza las redes multidifusión.
Se utiliza para transmitir a largas distancias, utilizando nodos intermedios. Se usan para transmitir señales de televisión, microondas terrestre y satélite o redes de comunicaciones.

Redes de difusión

También se denominan broadcasting, un nodo envía datos a múltiples receptores de forma simultánea, por lo que todos los usuarios reciben la misma información y a la vez. Dependiendo del tamaño de la red podemos distinguir.
Redes de área local (LAN): interconecta varios dispositivos y proporciona un medio para el intercambio de información. La cobertura es pequeña y la propiedad de la red es de la misma entidad, debido a esto la inversión que se realiza es mayor, requiere una compra mayor de componentes, que en una WAN. Dentro de las LAN tenemos varias configuraciones pero las más habituales son.

- LAN conmutada: la más utilizadas son la redes Ethernet, construida por un solo conmutador o con varios conmutadores interconectados en redes mas grande. En algunas redes se utilizan, donde se requiera el ancho de banda sea alta, un canal de fibra (Fiber Channel).
- LAN inalámbricas: se utilizan diversas tecnologías inalámbricas y distintas configuraciones.
- Redes de área amplia (WAN): cubren una extensa área geográfica, requieren atravesar rutas de acceso público y utilizan, redes proporcionados por una entidad proveedora de servicios de telecomunicación. Generalmente consisten en un conjunto de conmutadores, dispositivos lógicos que se utilizan para interconexión de segmentos de red, interconectados. La transmisión generada por cualquier dispositivo se encaminará a través de estos nodos internos hasta alcanzar el destino. A estos nodos, no le concierne el contenido de los datos, su función es proporcionar el servicio de interconexión para transmitir datos hasta el destino. Las redes WAN se han implementado con diferentes tecnologías.
    - Conmutación de circuitos: para la interconexión de dos estaciones se establece un camino dedicado a través de los nodos de la red. Este camino se realiza por medio de un conjunto de enlaces físicos entre los nodos, la estación fuente transmite información, un nodo recibe esa información y la encamina a un canal de salida en función del destino. Este tipo de tecnología es el utilizado por la red de telefonía.
    - Conmutación de paquetes: Los datos se envían en pequeños trozos denominados paquetes. Cada paquete se transmite de nodo a nodo en la red por algún camino de un origen al destino, el camino por donde se envían los paquetes no es fijo y cada paquete se puede enviar por caminos diferente en función de diferentes parámetros.
    - Frame relay (Retransmisión de tramas): Tecnología basada en la conmutación de paquetes, donde los paquetes tienen distintos tamaños e incluyen información de direccionamiento que se denominan tramas, los errores se controlan en el destino y los nodos intermedios solo retransmiten las tramas. La característica principal de esta tecnología es la alta velocidad que se consigue, esto es posible porque se elimina la mayor parte de información para el control de errores, ahorrando procesamiento.
    - ATM: Modo de Transferencia Asíncrono, usa paquetes de longitud fija denominadas celdas. ATM introduce poca información adicional para el control de errores, como en Frame Relay, confiando en el medio de transmisión y el control de errores se procesa en las estaciones finales. Al utilizar paquetes de longitud fija, el esfuerzo adicional de procesamiento se reduce incluso todavía más que en retransmisión de tramas. ATM permite definir múltiples canales virtuales con velocidades de transmisión que se define dinámicamente en el instante el que se crea el canal virtual. Al utilizar celdas de tamaño fijo, es más eficaz que puede ofrecer un canal a velocidad de transmisión constante aunque esté usando una técnica de conmutación de paquetes. ATM es una generalización de la conmutación de

circuitos en la que se ofrecen varios canales, en los que la velocidad de transmisión se fija dinámicamente para cada canal según necesidades.

La cobertura en la LAN es mucho menor, en redes LAN las velocidades son mayores que en la WAN. En redes LAN se suele utilizar redes de difusión, mientras que en redes WAN se utilizan difusión y punto a punto.

En función de cómo se realiza la transmisión tenemos Half-duplex y Full-duplex. En la transmisión Half-duplex sólo una de los dos nodos puede transmitir, en transmisión Full-duplex las dos estaciones pueden enviar y transmitir datos simultáneamente, es mucho más eficiente que el Half-duplex.

En los medios guiados hacen falta dos líneas para realizar transmisión Full-duplex.

Las redes LAN son muy utilizadas, la tecnología más utilizada para este tipo de redes es Ethernet. Este tipo redes están especificadas en el estándar IEEE 802.3 y utilizan protocolo CSMA/CD que es el encargado de controlar el acceso de la información al canal de comunicación.

La velocidad que se alcanza con redes Ethernet son de 10/100/1000 Mb/s, dependiendo del cable utilizado y de la tarjeta de red que se utilicen. Hay diferentes tipos de redes Ethernet que se diferencian en la velocidad que permiten, tipo de cable, la distancia máxima sin repetidores, la topología que se emplea.

Tecnología	Velocidad de transmisión	Tipo de cable	Distancia máxima	Topología
10Base2	10 Mbps	Coaxial	185 m	Bus (Conector T)
10BaseT	10 Mbps	Par Trenzado	100 m	Estrella (Hub o Switch)
10BaseF	10 Mbps	Fibra óptica	2000 m	Estrella (Hub o Switch)
100BaseT4	100Mbps	Par Trenzado (categoría 3UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (Switch).
100BaseTX	100Mbps	Par Trenzado (categoría 5UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (Switch).
100BaseFX	100Mbps	Fibra óptica	2000 m	No se permite el uso de hubs
1000BaseT	1000Mbps	4 pares trenzado (categoría 5UTP)	100 m	Estrella .Full Duplex(Switch)
1000BaseSX	1000 Mbps	Fibra óptica (multimodo)	550m	Estrella. Full Duplex(Switch)
1000BaseLX	1000Mbps	Fibra óptica (monomodo)	5000 m	Estrella. Full Duplex(Switch)

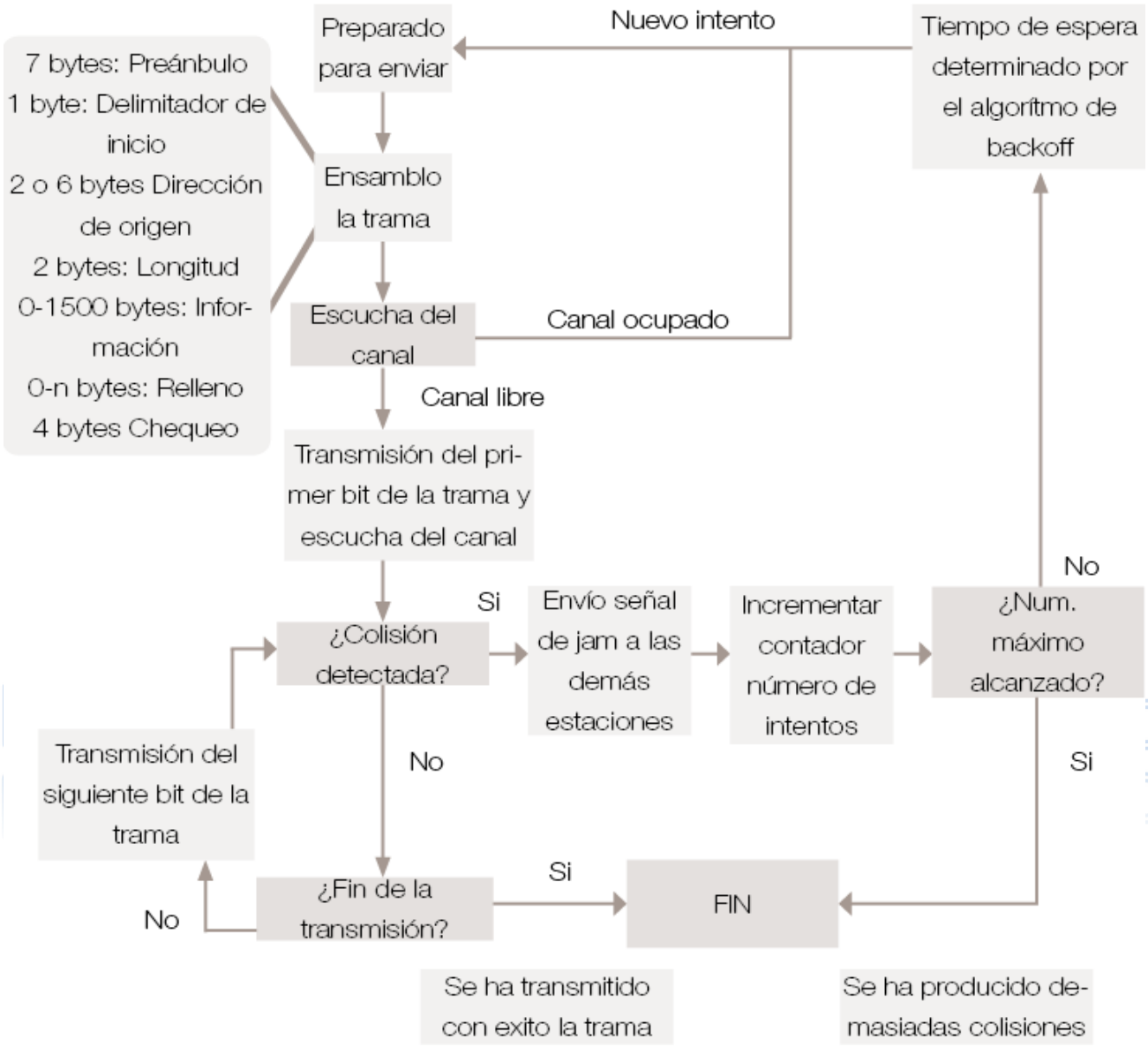
CSMA/CD

Este protocolo permite controlar el acceso al medio que realizan las computadoras, una red es un conjunto de computadoras conectadas generalmente mediante una serie de cables, estos cables son el medio de comunicación entre las diferentes computadoras. El CSMA/CD controla el acceso al medio de comunicación por parte de las computadoras, esto es un importante porque se evitan las “colisiones” que consiste en un paquete de datos que ha enviado una computadora se encuentra con otro paquete de datos que ha enviado otra computadora y los dos paquetes se encuentran en el mismo cable.

El funcionamiento del protocolo CSMA/CD tiene un componente de detección de colisiones (CD) para evitar las colisiones, el funcionamiento es el siguiente:

- Si el medio se encuentra libre, transmite; sino ir al paso 2.
- Si el medio se encuentra ocupado, continua escuchando hasta que le canal se libere, en cuyo caso transmite inmediatamente.
- Si se detecta una colisión durante la transmisión, se transmite una pequeña señal de interferencia para asegurarse de que todas las estaciones constantes la colisión. A continuación se deja de transmitir.
- Tras la emisión de la señal de interferencia, la estación espera una cantidad aleatoria de tiempo como espera, intentando transmitir de nuevo a continuación, volviendo el paso 1.

A partir de este momento entra en juego la parte de detección de colisión que se encarga de verificar que los paquetes han llegado a su destino sin colisionar con los que pudieran haber sido enviados por otras computadoras por error. En caso de colisión, se detecta y se suspende la transmisión, se espera un tiempo de espera aleatorio y comienzo el proceso desde el principio.



Formato de trama de Ethernet

La información que se desea enviar se divide en paquetes de datos, en una red Ethernet se denominan tramas que contienen la información que desea transmitir y otros datos adicionales que se utilizan en la transmisión. La trama que se transmite tiene este formato:

Preámbulo	SOF	Destino	Origen	Tipo	Datos	FCS
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 a 1500 bytes	4 bytes

- Preámbulo: Un campo de 7 bytes (56 bits) con una secuencia de bits usada para sincronizar y estabilizar el medio físico antes de iniciar la transmisión de datos.
- SOF (Start Of Frame) Inicio de Trama: Campo de 1 byte (8 bits) con un patrón de 1s y 0s alternados y que termina con dos 1s consecutivos.
- Dirección de destino: Campo de 6 bytes (48 bits) que especifica la dirección MAC de tipo EUI-48 hacia la que se envía la trama. Esta dirección de destino puede ser de una estación, de un grupo multicast o la dirección de broadcast de la red. Cada estación examina este campo para determinar si debe aceptar el paquete.
- Dirección de origen: Campo de 6 bytes (48 bits) que especifica la dirección MAC desde la que se envía la trama. La estación que deba aceptar el paquete conoce por este campo la dirección de la estación origen con la cual intercambiará datos.

- Tipo: Campo de 2 bytes (16 bits) que identifica el protocolo de red de alto nivel asociado con el paquete o, en su defecto, la longitud del campo de datos. La capa de enlace de datos interpreta este campo.
- Datos: Campo de 46 a 1500 Bytes de longitud. Cada Byte contiene una secuencia arbitraria de valores. El campo de datos es la información recibida del nivel de red (la carga útil).
- FCS (Frame Check Sequence - Secuencia de Verificación de Trama): Campo de 32 bits (4 bytes) que contiene un valor de verificación CRC (Control de redundancia cíclica). El emisor calcula este CRC usando todo el contenido de la trama y el receptor lo recalcula y lo compara con el recibido a fin de verificar la integridad de la trama.

Protocolos

Para el correcto funcionamiento de una red de comunicación se necesitan una serie de normas para establecer un correcto funcionamiento de la transmisión de la información. Estas normas se denominan protocolo de comunicación.
Protocolo de comunicación es un conjunto de reglas y normas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellos para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como posibles métodos de recuperación de errores.
Cada tipo de red de comunicación tiene sus propios protocolos que definen su funcionamiento.

Red de comunicación	Protocolos
Red de computadores.	TCP, IP, SSL, UDP, ATM, SNMP...
Red telefónica.	DECT,GSM,3G
Red Television.	PAL,SECAM,HDTV

Algunos protocolos se convierten en estándar están controlados por organizaciones, como IEEE u ISO. Cuando un protocolo es un estándar todas las especificaciones son públicas y pueden ser utilizadas por cualquier empresa siempre que cumplan todas las especificaciones del protocolo.
Dentro de los protocolos, hay dos que se considera de los más importantes porque son utilizados como base de Internet, estos son Protocolo de Control de Transmisiones (TCP) y Protocolo de Internet (IP). TCP/IP es una familia de protocolos considerados como un estándar de Internet.
El modelo **TCP/IP** se estructura en cinco capas independiente entre sí. Cada capa se encarga de una tarea específica.

- Capa física: define la interfaz física entre el dispositivo de transmisión de datos y el medio de transmisión. Esta capa se encarga de la especificación de las características del medio de transmisión, la naturaleza, la velocidad de datos y cuestiones afines.
- Capa de acceso a la red: es el responsable del intercambio de datos entre el sistema final y la red a la cual está conectado. El emisor debe proporcionar a la red una dirección destino para poder encaminar de manera correcta. Para sistemas finales conectados a la misma red, la capa de acceso de red está relacionada con el acceso y encaminamiento de datos.
- Capa Internet: Cuando dos dispositivos se encuentran conectados en dos redes diferentes, esta capa proporciona una serie de procedimientos para que se puedan transmitir datos entre las dos redes. El protocolo IP utiliza esta capa, que es implementado tanto estaciones como en nodos intermedios.
- Capa de transporte: En una red se intercambian datos, esta transmisión debe asegurarse de que llegue a su destino y en el mismo orden en el que fueron enviados, este cometido se encarga esta capa. El protocolo TCP se utiliza para proporcionar esta funcionalidad.
- Capa de Aplicación: contiene toda la lógica necesaria para posibilitar las distintas aplicaciones.

La mayor parte de las aplicaciones utilizan TCP como protocolo de transporte, proporciona una conexión fiable para transferir datos. Cada dato se encapsula en un segmento de TCP que contiene en la cabecera los puertos origen y destino. Estos puertos proporcionan una conexión lógica que será utilizado por las aplicaciones.

Existe otro protocolo de transporte que usa TCP/IP que es UDP (datagramas de usuario), este protocolo no proporciona control sobre el orden, ni la entrega al destino. UDP se utiliza en aplicaciones con una complejidad mínima, como SNMP.

TCP transmite información de control junto a los datos, si un emisor transmite datos y se lo pasa a TCP que divide los datos en bloques más pequeños y le añade información de control (cabecera TCP) a cada bloque. Al conjunto de la cabecera TCP y el bloque de datos se denomina segmento TCP.

La cabecera TCP incluye los siguientes campos.

- Puerto destino.
- Numero de secuencia.
- Suma de comprobación.

El puerto destino se utiliza para saber a quién se entrega el segmento, el número de secuencia se utiliza para saber el orden de envío de los segmentos. Por último, la suma de comprobación se utiliza para comprobar que el segmento recibido no ha sido modificado, es un código que se calcula en función del resto del segmento, el receptor recibe el segmento y realiza la misma operación y comprueba el resultado con el resultado recibido, si es igual el segmento es el original.

A continuación, el segmento TCP pasa a IP con instrucciones para que lo reciba el destino, será encaminado por varios nodos intermedios. Este encaminamiento requiere información de control que será añadida por el protocolo IP. El segmento TCP mas la cabecera IP que se añade, se denomina datagrama IP.

Cada datagrama IP se le pasa a la capa de acceso de red que añade su propia cabecera, creando un paquete o trama. El paquete se transmite a través de los dispositivos de encaminamiento para llegar a su destino. La cabecera que se añade contiene los siguientes campos:

- Dirección de la subred destino.
- Funciones solicitadas.

Cuando el paquete llega al destino, ocurre el proceso inverso, cada capa elimina la cabecera correspondiente y el resto se pasa a la capa inmediatamente superior, hasta que se consigan los datos.

IP versión 4

El protocolo IP es parte del conjunto de protocolos TCP/IP y es el protocolo de interconexión de redes más utilizados. Actualmente hay dos versiones del protocolo IP, versión 4(IPv4) y versión 6(IPv6), el estándar actual es IPv4 aunque a medio plazo será sustituido por IPv6.
Como se ha indicado anteriormente, el datagrama IP se utiliza en el proceso de transmisión, en la versión IPv4 los campos que incluyen un datagrama IP son los siguientes:

- Versión (4 bits): indica la versión del protocolo.
- Longitud de la cabecera Internet (IHL) (4 bits): longitud de la cabecera expresada en palabras de 32 bits.
- Tipo de servicio (16 bits): especifica los parámetros de fiabilidad, prioridad, retardo y rendimiento, no se utiliza habitualmente.
- Longitud total (16 bits): longitud total del datagrama.
- Identificador (16 bits): un número de secuencia que, junto a la dirección y destino y el protocolo usuario, se utiliza para identificar de forma única un datagrama.
- Indicadores (3bits): dos de los tres bits están actualmente definidos. Está compuesto por el bit “más datos” que se utiliza para la fragmentación y el reensamblado. El segundo bit es “no fragmentación” prohíbe la fragmentación cuando es 1.
- Desplazamiento del fragmento (13 bits): indica donde se sitúa el fragmento dentro del datagrama original.
- Tiempo de vida (8 bits): específica cuanto tiempo (segundos) se le permite a un datagrama permanecer en la red.
- Protocolo (8bits): identifica el protocolo de la capa de red inmediatamente superior que va a recibir el campo de datos en el destino.
- Suma de comprobación de la cabecera (16 bits): un código de detección de errores aplicados solamente a la cabecera.
- Dirección de origen (32 bits)
- Dirección de destino (32 bits)
- Opciones (variable): contiene las opciones solicitadas por el usuario que envía los datos.
- Relleno (variable): se usa para asegurar que la cabecera del datagrama tiene una longitud múltiplo de 32 bits.
- Datos (variable): el campo de datos debe tener una longitud múltiplo de 8 bits.

Los campos de dirección de origen y dirección destino están codificados para permitir una asignación variable de bits para especificar y el sistema final conectado a la red especifica.
Los campos dirección origen y destino en la cabecera IP contienen cada uno una dirección internet global de 32 bits que, generalmente, consta de un identificador de red y un identificador de computador. Este esquema de codificación proporciona flexibilidad al asignar las direcciones a los computadores y permite una mezcla de tamaños de red en un conjunto de redes.

IP versión 6

IPv6 incluye las siguientes mejoras sobre IPv4:

- Un espacio de direcciones ampliado: IPv6 utiliza direcciones de 128 bits en lugar de las direcciones de 32 bits de IPv4.
- Un mecanismo de opciones mejorado: La mayoría de estas cabeceras opcionales ni examinan ni procesan por ningún dispositivo de encaminamiento en la trayectoria del paquete. Esto simplifica y acelera el procesamiento que realiza un dispositivo de encaminamiento sobre los paquetes IPv6.
- Autoconfiguración de direcciones.
- Aumento de la flexibilidad en el direccionamiento.
- Funcionalidad para la asignación de recursos: IPv6 habilita el etiquetado de los paquetes como pertenecientes a un flujo de tráfico particular para el que el emisor solicita un tratamiento especial.

Los paquetes de IPv6 están compuestos por varias cabeceras, aunque la única cabecera obligatoria es la cabecera IPv6, que contiene los siguientes campos.

- Versión (4 bits): número de la versión del protocolo Internet; el valor es 6.

- Clase de tráfico (8 bits): disponible para su uso por el nodo origen y/o los dispositivos de encaminamiento para identificar y distinguir entre clases o prioridades de paquete IPv6.
- Etiqueta de flujo (20 bits): se puede utilizar por un computador para etiquetar aquellos paquetes para los que requiere un tratamiento especial en los dispositivos de encaminamiento dentro de la red.
- Longitud de la carga útil (16 bits): longitud del resto del paquete IPv6 excluida la cabecera.
- Cabecera siguiente (8 bits): identifica el tipo de cabecera que sigue inmediatamente a cabecera IPv6.
- Límite de saltos (8 bits): el número restante de saltos permitidos para este paquete.
- Dirección origen (128 bits).
- Dirección destino (128 bits).

Aunque la cabecera IPv6 es más grande que la parte obligatoria de la cabecera IPv4 (40 octetos frente a 20 octetos), contiene menos campos (8 frente a 12). Así, los dispositivos de encaminamiento tienen que hacer menos procesamiento por paquete, lo que agiliza el encaminamiento.

Mascara de red

Dentro de una red dividida en subredes, los dispositivos de encaminamiento locales deben encaminar sobre la base de un número de red extendido consistente en la porción de red de la dirección IP y el número de subred. Las posiciones a nivel de bit que contienen este número de red extendido se indican mediante la máscara de dirección. El uso de esta máscara de dirección permite a un computador determinar si un datagrama de salida va destinado a otro computador en la misma LAN (entonces se envía directamente) o a otra LAN (se envía a un dispositivo de encaminamiento).
La máscara de red o redes es una combinación de bits que sirve para delimitar el ámbito de una red de computadoras. Mediante la máscara de red una computadora (principalmente la puerta de enlace, router...) podrá saber si debe enviar los datos dentro o fuera de las redes.
Una máscara de subred por sí sola no nos dice nada. Tiene que ir siempre relacionada con una dirección IP, ya que por ejemplo la máscara 255.255.255.0 puede estar relacionada con una clase A, B, C.
La máscara por defecto de la clase A es 255.0.0.0.
La máscara por defecto de la clase B es 255.255.0.0.
La máscara por defecto de la clase C es 255.255.255.0.

1.2. Funciones y características de los elementos hardware

Estaciones

Son dispositivos hardware que utilizan los usuarios para enviar información o recibir información en una red comunicación. Pueden ser un computador, teléfono o un televisor, son dispositivos utilizados por los usuarios donde se realiza una comunicación.
Para que las estaciones puedan comunicarse y poder enviar o recibir información, pueden necesitar algún tipo de dispositivos de entrada- salida, como tarjetas de red o antenas.
En redes de computadores se utilizan tarjetas red en función de la señal y la tecnología utilizada, con las siguientes características.

Señal	Tarjeta de red	Características
Señal por cable	– Tarjetas Ethernet – Tarjeta Fibre channel	– Velocidad: 10/100/1000/10000 Mbit/s (Ethernet) 1,2,4,8 Gbit/s(Fibre Channel) – Conectores: Rj45, BNC (Ethernet)
Señal inalámbrica	– Tarjeta wifi	– Velocidad: 11/54/108-300 MB/s – Conectores: Para la antena, SMA,RP-SMA

Dentro de la red tenemos de dispositivos hardware encargados del transporte de datos en una red de comunicación, pueden ser hardware especializado o un computador con una serie de tarjetas de red y un software especifico para redes. Son un punto de interconexión de una red donde se conectarán varios de líneas de transmisión.
En este apartado se describirán diversos dispositivos hardware y sus principales características.

Switch

Es un elemento que se encarga de administrar varias líneas de transmisión, mediante una serie de puertos donde se conectan las líneas de transmisión. Su funcionamiento es simple, recibe una señal por un puerto y lo envía por otro puerto a su destino. El switch, para saber donde se encuentra el destino, almacena en una tabla donde todas las direcciones (MAC) de todos los nodos que se conectan a él, de esta forma sabe porque puerto debe enviar los datos. Son dispositivos que se suelen utilizar en redes LAN.

Las características principales tienen un switch.

- Soportan varias velocidades 10/100/1000.
- Alta conectividad: número de puertos disponibles, los más habitual va desde 5 a 32 puertos.
- Administración: algunos switch son gestionables a través de una interfaz web.
- Conectividad: Emplea puertos para conectores RJ45.

Los switch también se utilizan para conectar redes (segmento de red), su funcionamiento seria como un "puente" por donde se envía los datos entre las dos redes. Su funcionalidad es muy limitada, aunque algunas switch "caros" permiten otro tipo funcionalidad, lo más habitual es que se dediquen a enviar y recibir información entre estaciones.

Los switch solo proporcionan conectividad en un ámbito local (redes locales), no funcionan para dar servicio a Internet.

Router

También se denominan enrutador o encaminador, es un dispositivo que se encarga de enviar paquetes de datos de una red a otra. Este tipo de dispositivos tiene bastante más funcionalidades que un switch, el firmware y los componentes internos permiten realizar más tareas, aunque son más lentos y tiene menos puertos. Otra diferencia con los switch son que los router operan con direcciones IP para recibir y enviar datos.

Un router actual tiene un conjunto de puertos donde se conectan otros dispositivos, uno de esos puertos es utilizado para conectarse a Internet, en el caso de la red ADSL o cable ese puerto está conectado a un modem.

También suelen incluir conectividad inalámbrica mediante una serie de antenas, visibles o no, donde poder enviar o recibir una señal inalámbrica.

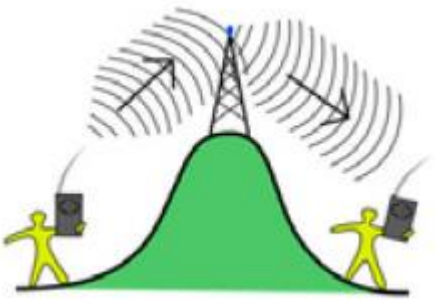
Con el auge de la telefonía y sus conexiones 3G, existen router para móviles. Son dispositivos proporcionan una señal Wifi para la conexión de diferentes dispositivos y el acceso a Internet se realiza mediante una conexión 3G u otra tecnología de datos. De esta forma, compartir una conexión de datos de telefonía móvil, estos dispositivos se denominan router MIFI.

Un tipo de router que podemos encontrar es el denominado router neutro, es un router que tiene un modem y no se pueden conectar a Internet de forma directa, se pueden conectar a otro router con modem para tener acceso a Internet a través de él. Sigue siendo un dispositivo que conecta dos o más redes.

REPETIDOR

Todas las tecnologías que se utilizan en las redes de comunicación tienen algunas limitaciones, una de ellas es la distancia máxima que puede transmitir una señal, para poder ampliar la distancia de transmisión se utilizan los repetidores. Estos dispositivos no almacenan la señal y pueden reconstruir la señal, si fuera necesaria, antes de retransmitirlas.

Los repetidores son dispositivos que reciben una señal, generalmente débil, y retransmite la señal con una potencia más alta. De esta forma, puede transmitir una señal a distancia más larga. Un uso muy común de los repetidores son las antenas que retransmiten señales de televisión y radio. En redes LAN podemos encontrarnos repetidores Wifi que amplifica la señal inalámbrica aumentando su cobertura.



PUNTO DE ACCESO

Es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica (Wifi). Estos dispositivos pueden tener puertos para conectarse a una red cableada. Estos dispositivos no proporcionan acceso a internet necesitan otro dispositivo, como un router, que proporcionen el acceso.

Los puntos de acceso son administrados por un interfaz web que permite configurar todos sus parámetros. Actualmente los puntos de acceso tienen muchas de las funcionalidades que un router.

Una características muy interesante de los puntos de acceso son la creación de redes ad-hoc que son redes inalámbricas descentralizadas donde cada nodo participa en el encaminamiento mediante el reenvío de datos hacia otros nodos, de modo que la determinación de estos nodos hacia la información se hace dinámicamente sobre la base de conectividad de la red.

MÓDEM

Son dispositivos que convierten señales digitales en analógicas y viceversa, se utilizan para acceder a Internet. El acceso a Internet por línea de teléfono proporciona una señal analógica y los computadores proporcionan señales digitales, el modem es el encargado de realiza la conversión de las señales. Las conexiones de los modem telefónicos son RJ11 para conexión telefónica, para la conexión al computador el más habitual es USB, aunque existen otras conexiones implementadas en modem más antiguos como: puerto COM, PCMCIA. La velocidad máxima que alcanzaban los modem telefónicos son 56 kbit/s.

Con la implantación de tecnologías como el ADSL -que usan router- el uso del módem ha caído enormemente. No obstante, se sigue utilizando con otras tecnologías como el cable modem para el acceso de Internet por cable, también en la telefonía móvil con los modem 3G.

GATEWAY

Una pasarela, puerta de enlace o Gateway es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino. En tecnologías como VOIP, transmisiones de voz a través de internet.

Un Gateway en VoIP es un dispositivo de red que convierte las llamadas de voz, en tiempo real, entre una red VoIP y la red telefónica pública conmutada o su centralita digital (PBX). Permite que las llamadas salientes generadas por la centralita tradicional se conviertan a IP y salgan por la conexión a Internet, o al revés, que una centralita convencional pueda recibir llamadas IP (de un proveedor SIP)

1.3. Funciones y características de los elementos software

El hardware que conforma una red, como los nodos o estaciones, necesitan software para poder gestionarlo y trabajar con ellos de forma más eficiente. El software nos permite "abstraer "del funcionamiento interno del hardware, no es necesario conocer los componentes internos de un determinado hardware para poder utilizarlos. Existen diferentes categorías de software, en este apartado se describirán las siguientes.

- **Sistema Operativo:** es software que nos permite gestionar los recursos de un hardware y proporciona servicios a otros programas.
- **Aplicaciones informáticas**: software que proporciona diversos servicios a un usuario, necesita de un sistema operativo para poder ejecutarse y poder acceder al hardware. Existen diversas categorías de aplicaciones en función del servicio proporcionado.
- **Firmware**: Software que gestiona un determinado hardware, se almacena en la memoria del hardware y se encuentra integrado en la electrónica del hardware.

Sistema Operativo

Es el software utilizado en los ordenadores y se encarga de gestión de sus componentes, ocultando al usuario los detalles. El sistema operativo cumple diversas funciones, algunas de estas funciones son:

- Administración del procesador.
- Gestión de la memoria.
- Gestión de entradas/salidas.
- Gestión de ejecución de aplicaciones.
- Administración de autorizaciones.
- Gestión de la información.

Para realizar estas tareas y otras, el sistema operativo se divide en una serie de componentes, cada uno de ellos se encargan de realizar las tareas en el hardware que corresponda.

Componentes del sistema operativo

Un sistema operativo está compuesto por una serie de partes o módulos, que permite realizar diferentes funcionalidades.

Núcleo	Software que constituye una parte fundamental del sistema operativo, el principal responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema.
Intérprete de comandos	Proporciona un sistema de comunicación entre el usuario y el sistema, Mediante una serie comandos que el intérprete se encarga de "traducir" a órdenes que se ejecuta en el hardware.
Sistema de archivos	Proporciona una estructura en el almacenamiento secundario para almacenar archivos.
Sistema de E/S	Permite interactuar con medio externos, teclado, impresoras, ratones, etc.
Administrador de memoria	Componente que se encarga de administrar la memoria principal del sistema, utiliza una serie de técnicas como la segmentación o paginación para un uso optimo de la memoria principal.

Las funcionalidades básicas de un sistema operativo:

- Gestión de procesos: un proceso es un programa en ejecución que necesita recursos para realizar su tarea. El sistema operativo se encarga del manejo de los procesos, realizando las siguientes tareas.
  - Creación y terminación de procesos.
  - Asignación/actualización/liberación de recursos.
  - Suspensión y reinicio.
  - Sincronización entre procesos.
  - Comunicación entre procesos.
  - Solución de trap y bloqueos.
- Manejo de memoria principal: La memoria es un almacén de datos de rápido acceso es compartido por la CPU y dispositivos E/S. El sistema operativo se encarga:
  - Realizar un "inventario" de la memoria, para conocer la cantidad de memoria libre y ocupada, conocer que procesos ocupan la memoria.
  - Selección y asignación de de los procesos a cargar en memoria.
  - Reservar o liberar de memoria.
  - Protección de memoria.

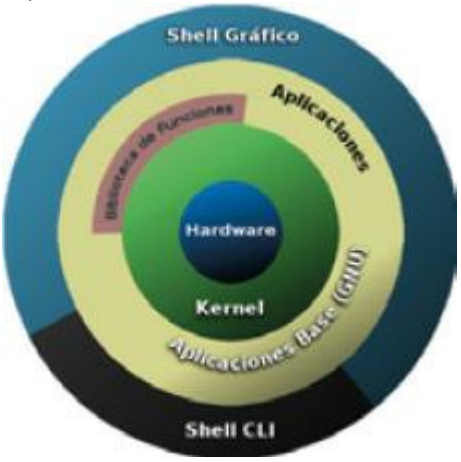
- Gestión de almacenamiento secundario: Tipo de almacenamiento no volátil, como discos duros. El sistema operativo se encarga de:
  - Planificar los discos.
  - Gestionar el espacio libre.
  - Asignar el almacenamiento.
  - Verificar que los datos se guarden en orden.
- Gestión de archivos: Los archivos son colecciones de información relacionada. El sistema operativo se encarga.
  - Creación y eliminación de archivos y directorios.
  - Operaciones de manipulación de archivos y directorios.
  - Asignar /manejar permisos de acceso a ficheros.
  - Realizar copias de seguridad de los archivos.
- Gestión de dispositivos de Entrada/Salida: Proporciona un sistema de memoria cache, para el acceso a los dispositivos por múltiples procesos.
  - Manejo de la memoria de E/S.
  - Gestionar las interrupciones.
  - Proporcionar una interfaz entre el usuario y dispositivo, sistema y dispositivo.
- Manejo de redes: El sistema operativo proporciona una interfaz de red para el acceso a dispositivos remotos.
- Interprete de comandos: Proporciona la interfaz entre el usuario y el sistema operativo, mediante línea de comandos en un terminal de texto o en un sistema gráfico basados en ventanas.

Dependiendo del uso, podemos clasificar el sistema operativo:

- Usuario: para tareas típicas de un usuario final, como ofimática, correo electrónico, Internet, juegos, etc.
- Servidor: especifico para instalar en servidores, incluye herramientas para gestionar diferentes servicios como redes, correo electrónico, desarrollo de aplicaciones o diferentes servicios de red.

GNU/LINUX

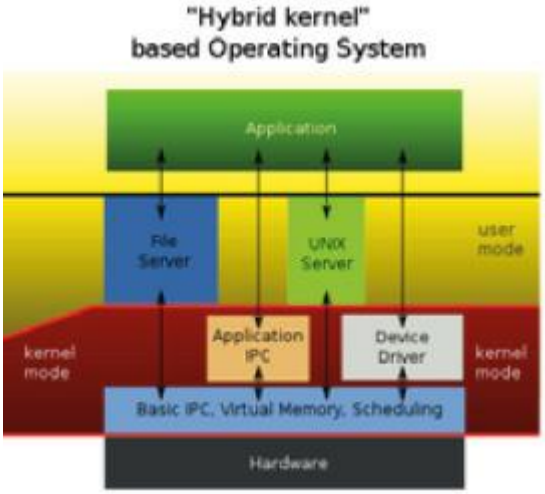
Es un sistema operativo libre y de código abierto, creado por una gran comunidad de personas y organizaciones con el apoyo de múltiples empresas. Este sistema está compuesto por un núcleo (Linux) y una serie de herramientas creadas por proyecto GNU, posteriormente a este sistema se le añaden un conjunto de aplicaciones creando lo que se le denomina Distribución de Linux.



Distribución de Linux: es una distribución de software basada en el núcleo Linux que incluye determinados paquetes de software para satisfacer las necesidades de un grupo específico de usuarios, dando así origen a ediciones domésticas, empresariales y para servidores. Por lo general están compuestas, total o mayoritariamente, de software libre, aunque a menudo incorporan aplicaciones o controladores propietarios.

Kernel

Es el núcleo del sistema operativo creado y mantenido por Linus Torvalds. Es un núcleo tipo monolítico híbrido donde los servicios que proporciona se encuentran dentro del kernel, pero mediante módulos externos se puede ampliar los servicios. Estos módulos compilados, modificados, cargados y descargados del kernel en tiempo de ejecución.
Este tipo de kernel son de un tamaño pequeño, no incluye todos los servicios, y modular, esto hace que tengan buen rendimiento.



Dentro del kernel hay dos modos de ejecución: modo kernel y modo usuario.

- Modo kernel: en este modo se ejecutan los procesos que tiene acceso al hardware, en su funcionamiento el proceso no tiene restricciones. Este modo debe ser controlado de forma muy cuidadosa por parte del sistema operativo.
- Modo usuario: modo de funcionamiento con restricciones, no tiene acceso directo al hardware, la mayoría de aplicaciones se ejecutan en este modo.

Un proceso puede ejecutarse en modo kernel, para realiza esta tarea se puede realizar de las siguiente formas.

- Llamada al sistema o 'system call'.
- Excepción: Señal que proviene de la CPU, que son condiciones que requieren especial atención, como un error.
- Interrupciones: Señal hacia la CPU que proviene de algún equipo hardware indicando que requiere su atención para que interrumpa su ejecución.

SISTEMAS DE ARCHIVOS

GNU/Linux soporta múltiples sistemas de archivos para gestionar el almacenamiento secundario. El lista de lo más conocidos.

- Ext3: es el sucesor ext2, entre sus características principales como que no requiere desfragmentación, incorpora tolerancia a fallos, poco consumo de CPU, registro por diario (Journaling).
- Ext4: sucesor de etx3, añade como características como aumento en el tamaño de los volúmenes, nuevo esquema de bloques (extents), más rápido, etc.
- BtrFS: es del copy on write (COW) que permite snapshots de solo lectura o modificables, creación de volúmenes lógicos.
- XFS: es un sistema con journaling de alto rendimiento, es considerado como un sistema muy estable, tiene alta capacidad de almacenamiento.
- ZFS: tiene un modelo COW, gran capacidad de almacenamiento, rápido, necesita mucha memoria para un funcionamiento optimo. Ideal para grandes sistemas de almacenamiento.

Administrador de Memoria

Linux comparte muchas de las características de los esquemas de gestión de memoria de otras implementaciones UNIX, pero tiene sus características propias y únicas, aunque hay que destacar que el esquema de gestión de memoria de Linux es bastante complejo.
Utiliza un direccionamiento de memoria virtual, que es una técnica de gestión de memoria, basado en el uso de una estructura de tabla de páginas con tres niveles. Linux utiliza paginación por demanda que es una técnica de gestión de memoria virtual, donde los programas se dividen en pequeñas partes o páginas y la memoria se divide en trozos del tamaño denominados marcos de página.
El kernel se le asigna un parte de memoria de forma permanente y este puede asignar o liberar memoria de forma dinámica, esto se usa para cargar módulos que tienen un tamaño arbitrario.
La memoria virtual es una técnica de gestión de la memoria que permite que el sistema operativo disponga, tanto para el software de usuario como para sí mismo, de mayor cantidad de memoria que esté disponible físicamente.

Sistema de Entrada/Salida

En Linux los dispositivos de entrada/salida aparecen como ficheros especiales que se encuentran normalmente en el directorio /dev. Cada fichero se le asigna un manejador de dispositivo que acepta peticiones del software de Entrada/Salida independiente del dispositivo, realiza las siguientes tareas.

- Traduce las peticiones a formato del controlador.
- Planifica el acceso de peticiones al dispositivo.
- Envía las órdenes al controlador.
- Espera a que se cumplan.
- Comprueba el estado de la operación cuando llega la interrupción.
- Gestiona los errores, si existen, y los resuelve, si es posible.

Los ficheros especiales se dividen en dos tipos: dispositivos de carácter y dispositivos por bloques, cada unos de estos tipos engloban un conjunto de dispositivos de E/S.

- Dispositivos de bloques: discos duros.
- Dispositivos de caracteres: impresora y teclado.

La entrada/salida se implementa como una colección de manejadores, uno por dispositivo, que abstrae del sistema operativo los detalles del dispositivo hardware.

Intérprete de Comandos

Proporciona un método para introducir comando en Linux que se ejecuta a través de un terminal. Linux está orientado a trabajar en terminal, hay varios intérpretes de comando e incluso varios terminales, algunos ejemplos de intérprete de comandos.

- Bourne Shell: el primer intérprete utilizado en UNIX.
- Korn Shell: creado por el proyecto GNU, la ventaja principal es su uso como lenguaje de programación. Es compatible con Bash.
- Bash: se utiliza por defecto por muchas distribuciones de Linux, tiene un modo interactivo.
- Zsh: intérprete diseñado para un uso interactivo.
- Tcsh: interprete compatible con Bourne Shell, es el intérprete por defecto en FreeBSD.

Como se ha indicado los intérpretes de comandos proporciona un lenguaje de programación que se utilizan para crear pequeños programas shell scripts, muy utilizados para tareas de administración y archivos de configuración. Se utilizan estructuras de control, condicionales o variables.
Para utilizar los intérpretes de comandos se debe utilizar un terminal que proporciona una línea de comandos, los terminales son herramientas muy potentes, se puede trabajar con Linux sin utilizar un entorno gráfico, solo con el terminal.
Los terminales simulan el funcionamiento de un terminal físico, Linux proporciona una serie de terminales, algunos con algunas características avanzadas. Algunos de estos terminales.

- Xterm: terminal que incluye X.org.
- Konsole: terminal que incluye KDE.
- Gnome-terminal: terminal que incluye Gnome.
- Tmux.

Aplicaciones Informáticas

Un sistema operativo se complementa con un conjunto de aplicaciones informáticas que aumenta la funcionalidad de un computador. Hay muchas categorías de aplicaciones una función de la tarea que nos permite y del campo donde se utiliza. Enfocándonos en el campo de las redes nos podemos encontrar las siguientes categorías:

- Herramientas de acceso remoto.
- Herramientas de comunicación.
- Monitorización.
- Administración de redes.
- Herramientas de seguridad.
- Gestión de incidencias y servicio técnico.
- Sistemas de instalación remota.

Dentro de cada categoría tenemos múltiples aplicaciones, una breve descripción de cada categoría y de aplicaciones que pertenecen.

Herramientas de acceso remoto	Aplicaciones que desde una equipo local poder acceder a equipos a distancia, utiliza cuando no podemos acceder físicamente a una equipo. Ejemplos VNC, SSH o TeamViewer.
Herramientas de comunicación	Aplicaciones donde los usuarios realizan una comunicación a través de una red, también se utiliza para realizar trabajo colaborativo. Ejemplo, chat, sistemas de videoconferencia, o pizarra digital.
Monitorización	Aplicaciones controlar el funcionamiento de una red y todos los servicios que se ofrecen, alertando en caso de problemas. Ejemplos, Nagios, Zabbix o OpenNMS.
Administración de redes	Aplicaciones que nos permite realizar diferentes tareas para la gestión de una red. Los sistemas operativos incluyen herramientas de este tipo, también herramienta como webmin o Zenytal.
Herramientas seguridad	Aplicaciones controlan el acceso a la red y que no se ejecute software no deseado. Ejemplos cortafuegos, antivirus o sistemas de detección de intrusos.
Gestión incidencias y servicio técnico	Aplicaciones que registran todas las incidencias producidas en un sistema, para poder solucionarlas lo antes posible. Ejemplo concursive o Dynamic CRM o Mantis.
Sistema de instalación remotas	Aplicaciones para realizar múltiples instalaciones en una red. Ejemplo Opsi, RIS o SpiceWork.

Servidores

En una red se suelen ofrecer una serie de servicios a los usuarios, estos servicios son proporcionados por un conjunto de software y hardware.

Este tipo de software que ofrecen servicios se denominan Servidores y suelen estar implementado en un hardware específico.

Es una parte importante de cualquier red, sobre todo en redes corporativas, que necesita una serie de cuidados. Los servidores tienen las siguientes características:

- Funcionan de forma ininterrumpida: ofrecen un servicio que siempre debe estar disponible para los usuarios.
- Hardware potente: para poder ofrecer un servicio a muchos usuarios con un rendimiento optimo.
- Necesitan algún tipo de refrigeración: por funcionamiento y hardware los servidores generan mucho calor y debe disiparse para no provocar errores.
- Utiliza una arquitectura cliente-servidor.

Se pueden tener servidores “caseros” que no necesitan algunas de las características mencionadas, pero tiene un rendimiento pobre y pueden ofrecer servicio s en un ámbito domestico.

Un usuario realiza una petición a un servicio ofrecido por un servidor, que procesa la petición y envía la respuesta al usuario. Esta arquitectura se denomina cliente-servidor.

Hay múltiples servidores en función del servicio que ofrece. Una lista de algunos de ellos:

Servidor	Servicio
Web	Almacena página web y muestra los contenidos.
Base de datos	Proporciona acceso a sistemas de base de datos.
Correo	Proporciona servicios de correo electrónico.
FTP	Implementa servicios de FTP.
Aplicaciones	Almacena, ejecuta aplicaciones que acceden los usuarios.
Proxy	Controla el acceso a internet a una red.
Archivos	Almacena archivos que pueden acceder los usuarios.
PBX	Implementa un centralita digital de VOIP.
Impresión	Servicios para gestionar el acceso de los usuarios a una impresora.

Los servidores pueden ser dedicados, los recursos del hardware están destinados al servicio de un solo software servidor. También tenemos los servidores no dedicados, los recursos hardware se comparten entre varios software servidor.

Los servidores tienen varios formatos físicos.

- Formato rack. Permite instalar varios servidores en unos armarios denominados rack. Estos armarios disponen de unos soportes metálicos, donde introducir los servidores que deben tener unas dimensiones especificas. Los armarios rack tienen normalizados las anchuras para que sea compatible con equipamiento de cualquier fabricante y están diseñados para facilitar la ventilación, puede incluir ventiladores. Lo servidores en formato rack tienen formato en unidad de rack (U), un servidores puede ser de 1U, 2U o 4U. Hay disponible en formato rack otro tipo de hardware como cortafuegos o antivirus o IDS.

- Formato torre: Es el formato tradicional de ordenadores personales, es barato y fácil de conseguir, pero como desventajas el tamaño (no son apilable).
- Formato Blade: este tipo de formato aprovecha al máximo el espacio, también utilizan armarios rack para sus instalaciones. Cada servidor Blade está compuesto por únicamente microprocesador, memoria y buses en un formato “tarjeta”. Varios servidores Blade se instalan en un chasis y el chasis contiene los demás elementos, como fuentes de alimentación o ventiladores, que son compartidos con todos los servidores Blade. Como ventajas son más baratos, consumen menos energía y ocupan menos espacio.

Firmware

Es un **software** que se encuentra en múltiples dispositivos hardware como router, switch, impresoras, televisores, teléfonos, etc. Es **específico para el hardware donde está instalado y controla el funcionamiento de ese dispositivo**. Los firmware suelen estar desarrollado en lenguaje ensamblador que

permitir interactuar directamente con los componentes electrónicos del dispositivo, teniendo mayor control sobre él.

El nombre de firmware es debido a que está fuertemente integrado en el hardware, de ahí viene la parte de firm que significa firme, y está almacenado en la memoria del dispositivo (ROM, flash, EEPROM, etc.). El firmware se puede actualizar, siempre que el fabricante proporcione la actualización, esto permite aumentar la funcionalidad de un dispositivo y corregir errores.

Han surgidos firmware no oficiales, sin soporte del fabricante, para diversos dispositivos que permiten que amplían las funcionalidades del dispositivo. Dos de los más famosos son OpenWrt y DD-WRT son firmware para router y punto de accesos, soportan una amplia variedad de dispositivos, e implementan características avanzadas que viene incluidas en el firmware original. Los dos firmwares proporcionan una interfaz web para configurarlos, sustituyendo la interfaz original del dispositivo, donde podemos configurar sus múltiples opciones.

El proceso de sustituir o actualizar el firmware de un dispositivo se denomina flashear o flasheo, la dificultad del proceso depende mucho del dispositivo e implica un considerable riesgo. Si el flasheo no se realiza de forma correcta, el dispositivo puede sufrir una avería irreparable, si su firmware no funciona correctamente, puede no arrancar. Tomando ciertas precauciones el riesgo baja considerablemente, aunque es un proceso que debe realizar un usuario con ciertos conocimientos técnicos.

La ventajas del flashear un dispositivos son muy grandes, como se ha expuesto anteriormente, aumenta la funcionalidad del producto, incluso añadiendo nuevas características, arreglar ciertos errores y mejora su funcionamiento en general.

2. Mantenimiento y actualización de elementos de conmutación y transmisión de la red

2.1. Herramientas de acceso y control remoto, características

Cuando debemos administrar un equipo de una red y no podemos acceder de forma física o no tenemos dispositivos de entrada/salida disponible para ese dispositivo, no tenemos disponibles un teclado y un monitor para interactuar con él. Necesitamos algún tipo de herramientas para poder acceder a ese dispositivo para poder administrarlo. Para realizar un acceso remoto es necesario:

- Un equipo local donde el usuario realiza un acceso remoto.
- Un equipo remoto.
- Un protocolo para realiza el acceso remoto.

Este tipo de herramientas se denominan herramientas de acceso y control remoto, nos permiten administrar un equipo a través de una red. Este tipo de herramientas tiene las siguientes características:

- Ejecución de comandos remotos.
- Acceso al entorno gráfico del equipo remoto.
- Cifrado de la comunicación.

Para poder utilizar tenemos que cumplir una serie de requisitos.

- Disponer de acceso a la red donde se encuentre el dispositivo.
- Disponer de los permisos necesarios.
- Disponer del mismo sistema operativo, en algunos casos.

El primer requisito es evidente, debemos disponer de una red para acceder al dispositivo. Si no está accesible por medio de una red, por ejemplo por fallo hardware en el dispositivo, este tipo de herramientas no sirven y solo tenemos la opción del acceso físico.
El segundo requisito, indica que debemos tener los permisos, ya sean credenciales de usuarios del dispositivo, el típico nombre de usuario y contraseña; si el equipo remoto tiene instalado algún cortafuego que controla el acceso, configurarlo para que permita el acceso. En algunas redes el acceso al exterior está con el tercer requisito, algunas herramientas solo están disponibles para un determinado sistema operativo. Como ejemplo, el sistema operativo Windows incluye una herramienta de escritorio remoto que solo se utiliza para acceder a equipos remotos con Windows y el equipo local debe tener el mismo sistema operativo.

Herramientas De Acceso Remoto

Dependiendo del tipo de acceso al equipo remoto, tenemos varias categorías de herramientas de acceso remoto.

Escritorio remoto	Acceso al entorno gráfico del equipo remoto, es la mejor forma de trabajar de forma remoto con equipos de escritorios. Por contra, requiere más recurso y la velocidad de la red influye mucho en su funcionamiento. Ejemplo de esta categoría, Escritorio remoto de Windows, Teamviewer o TightVNC.
Terminal	Acceso mediante la línea de comandos de un terminal, es muy utilizado en entornos Linux. Se utiliza habitualmente para ejecutar comandos en el equipo remoto, consume muy pocos recursos y es muy rápido. Por el contrario, no es muy cómodo de utilizar y requiere ciertos conocimientos técnicos, se utiliza mucho para administrar servidores. Un ejemplo de esta categoría es openSSH o Telnet.
Interfaz web	Acceso mediante una página una web, solo requiere un navegador en el equipo local para acceder al equipo remoto. Es utilizado para administrar dispositivos como router, también hay aplicaciones de administración que utilizan interfaz web que permiten acceso remoto.

Protocolos

Para utilizar herramientas de acceso remoto necesitamos una red para comunicarnos con el equipo remoto. Para la comunicación se utilizan varios protocolos que proporcionan una serie de normas de funcionamientos.

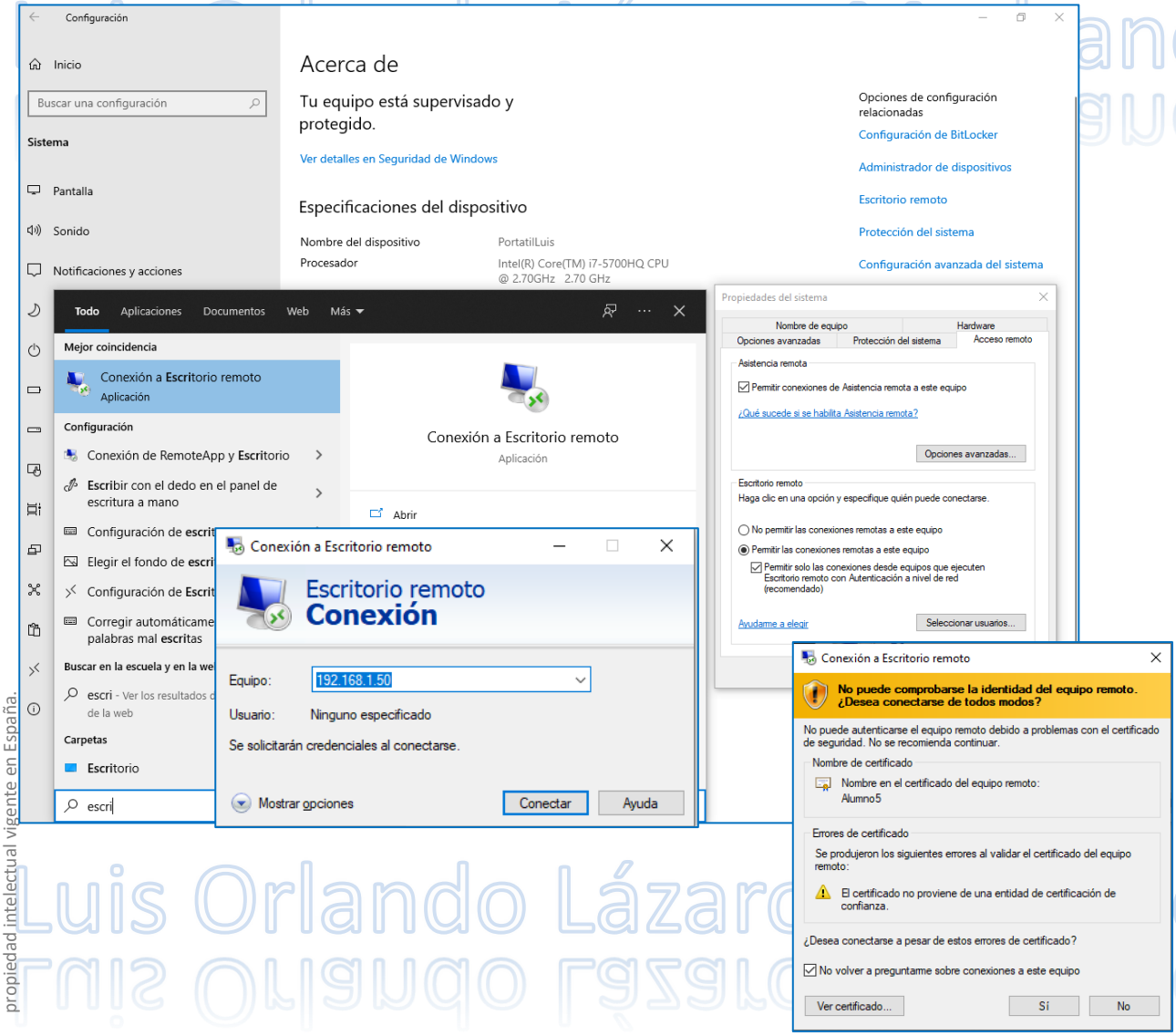
Cada protocolo tiene una serie de características y una serie de programas que lo soportan, una lista de los protocolos que se verán en este apartado son:

RDP

Remote Desktop Protocol es un protocolo desarrollado por Microsoft y utilizado para la comunicación entre un servidor Terminal Server y un cliente de Terminal Server, también el escritorio remoto de Windows utiliza este servicio. Está basado en la familia de protocolos T.120, es un estándar para la comunicación de datos multimedia, multipunto y en tiempo real, utiliza una arquitectura cliente-servidor.

Su funcionamiento consiste en convertir los datos en formato RDP, estos datos son generados por el servidor y enviados por la red al equipo cliente, denominado terminal, donde se reconstruirán para mostrarla por pantalla. En cuanto a la introducción de órdenes en el terminal por parte del usuario, las teclas que pulse el usuario en el terminal así como los movimientos y pulsaciones de ratón son redirigidos al servidor. El protocolo también permite que toda la información que intercambien cliente y servidor sea comprimida para un mejor rendimiento en las redes menos veloces. Es muy útil en redes con clientes ligeros (thin client).

Este servicio utiliza por defecto el puerto TCP 3389 en el servidor para recibir las peticiones. Una vez iniciada la sesión desde un punto remoto el ordenador servidor mostrará la pantalla de bienvenida de Windows, no se verá lo que el usuario está realizando de forma remota.



RDP está diseñado para admitir distintas topologías lógicas (ISDN, POTS, IPX, NetBios, TCP/IP, etc.), lo que le hace muy versátil, se puede utilizar múltiples redes. RDP es encapsulado y cifrado dentro de TCP/IP, pero está desarrollado para ser independiente en la pila de transporte de TCP/IP, dejando abierta la posibilidad de agregarle otros controladores de transporte y poder hacerlo más seguro.
El protocolo RDP incluye las siguientes características.

- Uso de encriptación RC4 de 128 bits, también utiliza TLS.
- Permite reducir el tráfico de red mediante varios mecanismos como la compresión de datos que aumenta el rendimiento en redes lentas.
- Impresión remota.
- El redireccionamiento del audio permite al usuario ejecutar un programa de audio en una ventana remota y escuchar el sonido en el ordenador local.
- Compartir el portapapeles. Se puede copiar, pegar y corta entre el equipo local y el remoto.
- Programas remotos. Se pueden ejecutar aplicaciones en el terminal server con ficheros en el terminal.
- Soporte para varios monitores.
- El redireccionamiento del audio permite al usuario ejecutar un programa de audio en una ventana remota y escuchar el sonido en el ordenador local.
- Se puede arrastrar desde el escritorio “Cliente” al escritorio “Servidor”, Drag and Drop.
- Varios administradores pueden trabajar en el mismo server.
- No necesita servidor para trabajar.

El cliente remoto debe ser en Windows, si necesita Terminal Server se necesita un Windows Server. Hay un cliente oficial de Windows y un conjunto de clientes no oficiales en otros sistemas operativos, como Rdesktop, que nos permitirá acceder al equipo con Windows desde otro sistema operativo.
Se describirá como usar el escritorio remoto y Terminal Server en Windows, viendo la instalación y como se usa.

Escritorio remoto en Windows

Software incluido en diferentes versiones de Windows que nos permite acceder desde un equipo local al entorno gráfico de un equipo remoto, se tendrá acceso a todos los recursos de equipo remoto. Este software hace uso del protocolo RDP para la conexión remoto.
Primero deberemos configurar el equipo remoto para permitir el acceso remoto.
Abrimos el menú Inicio, en la opción Equipo pulsamos con el botón derecho. En la ventana siguiente, escoger Configuración de acceso remoto. Pulsar en Seleccionar usuario, para agregar usuario que tengan permisos para acceder de forma remota a la máquina.
La Autenticación a nivel red aumenta la seguridad para acceder al equipo remoto, La Autenticación a nivel red aumenta la seguridad para acceder al equipo remoto, mediante nombre usuario y contraseña. Está disponible la versión 6.0 o mayor del Escritorio remoto.
Para acceder al escritorio remoto, en el equipo local desde donde se realiza el acceso remoto, pulsamos en Inicio, opción Todos los programas, Accesorios y Conexión a Escritorio remoto.
En la ventana de Conexión de Escritorio remoto, si pulsamos en Opciones se despliega un conjunto de pestañas disponibles. Para conectarnos introducir la dirección IP o el nombre del equipo de la máquina remota.

Terminal Server

Es un componente de la familia Windows Server que permite a un usuario acceder a las aplicaciones y datos almacenados en otro ordenador mediante el acceso por red. Podemos instalar aplicaciones de forma centralizada en un servidor de Terminal Server y acceder desde un cliente a las aplicaciones, solo se transmite por la red la información del ratón, teclado y pantalla.
Está compuesto de tres componentes:

- Servidor de Terminal Server, instalado en un Windows Server.
- Cliente de Terminal Server, soporta varios sistemas operativos.
- Protocolo de escritorio remoto.

El servidor de terminal server está incluido en la familia de Windows Server, aunque es posible que tenga que instalar en el sistema.
Podemos distinguir dos tipos de instalación:

- Modo Administración remota: proporciona acceso remoto a los servidores por parte de los administradores. Soporta, además de la sesión de consola, dos sesiones más, sin tener que pagar ninguna licencia extra.
- Modo Servidor de Aplicaciones: permite el acceso simultáneo por parte de varios clientes remotos. En este caso sí será necesario adquirir licencias de terminal.

En Windows 2008 Server, para instalar los roles de Terminal Server en la consola de administrador del servidor y escoger Terminal Services para agregar ese rol al sistema.
Se nos mostrará un asistente donde mediante una serie de pasos configuremos todos los aspectos de Terminal Services. Dependiendo de los roles escogidos los pasos a seguir cambiáran. Los pasos que se muestran en una serie de ventanas.

- Pequeña introducción sobre Terminal Services.
- Escoger diferentes tipos de rol dentro de Terminal Services.

Terminal Services	Instalación del servidor.
TS Licensing	Servidor de licencias de terminal server. Para acceder a los servicios de terminal server más de 120 días necesitamos adquirir licencias CAL. Tenemos dos formas de licencias; por dispositivos o por usuarios.
TS Web Access	Permite a los usuarios obtener acceso a programas y a escritorio remoto desde un sitio Web.
TS Session Broker	Permite realizar balanceo de carga de sesión entre los servidores de Terminal Server y la reconexión a una sesión existentes.
TS Gateway	Permite a los usuarios remotos autorizados conectarse a recursos de una red corporativa interna desde cualquier dispositivo conectado a internet.

Algunas funcionalidades escogidas requieren de ciertos requisitos que deben ser instalados, se mostrará una ventana indicando estos requisitos y la posibilidad de instalarlos.

- Recomendación, primero instalar Terminal Server y después las aplicaciones, si ya hay aplicaciones instaladas pueden dejar de funcionar.
- Escoger el nivel de seguridad, nos da la posibilidad de escoger el nivel de autenticación, podemos utilizar NLA, que aumenta la seguridad de la conexión, para la conexión con el servidor o no.
- Escoger el modo de licenciamiento: por dispositivo o por usuario. La tercera opción permite utilizar Terminal Server sin necesidad de licencia durante 120 días.
- Seleccionar un grupo de usuarios que podrán conectarse a este servidor de Terminal Server.
- Introducción a Network Policy Server (NPS) podremos asegurar la conexión o configurarlo con unas directivas.
- Seleccionar los servicios para NPS.
- Confirmar la instalación, se muestra en una pantalla todas las opciones escogidas.
- Instalación.
- Informe para ver el resultado de la instalación. Para algunas componentes requiere reiniciar el sistema.
- Si todo ha sido correcto, se muestra un informe.

Para conectar con un cliente al Terminal Server, utilizar el cliente remoto de Windows como el Escritorio Remoto.

VNC

Virtual Network Computing es un protocolo para acceso remoto que emplea el protocolo RFB, que es un protocolo para acceso remoto de entornos gráficos de usuario. Utiliza una arquitectura cliente-servidor y no impone ninguna restricción respecto al sistema operativo que se utiliza en el servidor ni en el cliente, hay versiones para casi todos los sistemas operativos, se puede utilizar un servidor en un sistema operativo y en el cliente otro sistema operativo.
El funcionamiento consiste en el cliente, también se le denomina visor, envía eventos de teclado o ratón al servidor que envía las actualizaciones de pantalla como respuesta al cliente.

VNC se compone de tres componentes.

- SERVIDOR
- RFB
- CLIENTE

La comunicación se realiza a través del protocolo RFB que utiliza el framebuffer, que es una memoria que se utiliza para gráficos, utiliza el puerto 5900, si tenemos más conexiones 5901.5902, etc., en el servidor y si se utiliza un navegador para acceder, disponible en algunas implementaciones, se utiliza el puerto 5800.
La comunicación no es muy segura, la contraseña se envía cifrada pero este cifrado se puede romper fácilmente por fuerza bruta (probando múltiples claves de forma automática) pero el resto de la comunicación se envía en formato de texto plano, un atacante puede escuchar el tráfico y obtener esos datos. Se utiliza VNC con otros protocolos más seguros como SSH, para que la comunicación sea más segura.
VNC es un protocolo estándar que tiene una aplicación con el mismo, que tiene el código fuente disponible.
Hay múltiples variantes, algunas compatibles con el VNC original y otras que no son compatibles, también hay variantes optimizadas para un sistema operativo, todas estas variantes han añadido nuevas funcionalidades, una lista de ellas se muestra a continuación:

- Transferencia de archivos.
- Cifrado de datos con RC4.
- Compresión de los datos, útil en redes lentas.
- Utiliza un driver de pantalla para actualizar la pantalla del cliente.
- Túnel automático sobre SSH, mejora la seguridad.
- Uso de Jngle para mejorar la transferencia de datos.

Existe una gran cantidad de clientes de VNC, empezando por el original VNC, RealVNC, TightVNC, UltraVNC, Apple Remote Desktop, etc.

ICA

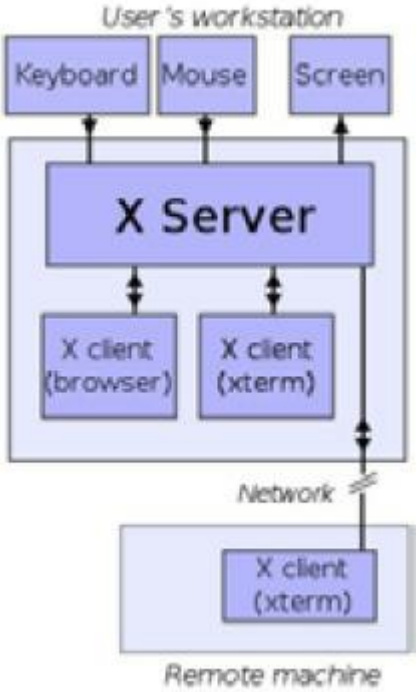
Independent Computing Architecture pertenece a la compañía Citrix, el protocolo crea una especificación para pasar datos entre el servidor y los clientes, pero no está ligado a ninguna plataforma en particular. El protocolo ICA se ha diseñado especialmente para transmitir datos de pantalla gráfica de Windows y entradas de teclado y ratón a través de una conexión de red. Como media sólo consume 20 Kbaudios de ancho de banda y logra así un rendimiento impresionante incluso en las conexiones de bajo ancho de banda.
Este protocolo se utiliza en varios productos de la compañía Citrix para que aplicaciones ordinarias de Windows puedan correr en un servidor de Windows conveniente, y que cualquier cliente soportado pueda ganar acceso a esas aplicaciones.
Para conseguir una latencia de red baja y un alto desempeño utiliza las siguientes características:

- Comando inteligente y compresión específica del objeto.
- Caché inteligente de los objetos Windows, incluidos mapas de bit, pinceles, glyphs y punteros.
- Codificación de longitud de ejecución.

El protocolo ICA se utiliza en la comunicación con estación espacial internacional (ISS), debido a la limitación en el ancho de banda de comunicación con la estación.

X11

Protocolo que también se denomina X Windows System o X, este protocolo permite la interacción gráfica en red entre un usuario y una o más computadoras haciendo transparente la red para éste, utilizando una arquitectura cliente-servidor. Con este protocolo podemos acceder a una máquina remota en Linux pero hay clientes que soportan este protocolo en diversos sistemas operativos. Aunque el código fuente está disponible y se puede portar al cualquier sistema operativo.
El sistema X-Windows distribuye el procesamiento de aplicaciones especificando enlaces cliente-servidor. El servidor provee servicios para acceder a la pantalla, teclado y ratón, mientras que los clientes son las aplicaciones que utilizan estos recursos para interacción con el usuario. De este modo mientras el servidor se ejecuta de manera local, las aplicaciones pueden ejecutarse remotamente desde otras máquinas, proporcionando así el concepto de transparencia de red.



El servidor X toma datos de entrada desde el teclado y el ratón y la muestra en una pantalla. Un navegador web y un emulador de terminal se ejecutan en la workstation del usuario, y un emulador de terminal se ejecuta en un servidor remoto pero es controlado desde el ordenador del usuario. Notar que las aplicaciones remotas se ejecutan de la misma manera que lo harían en forma local.

TELNET

TELecommunication NETwork, protocolo facilita la realización de conexiones remotas, mediante las cuales el usuario en un terminal o computador se conecta a otro de forma remoto y trabajar como si estuviera delante de él. Este protocolo está diseñado para acceder con un terminal, simula a los antiguos ordenadores que funcionaban como un terminal de texto. El puerto que utiliza por defecto es 23.

Telnet se implementa en dos módulos: el usuario Telnet interactúa con el módulo de Entrada/Salida para comunicarse con un terminal local. Este convierte las particularidades de los terminales reales a una definición normalizada de terminal de red y viceversa. El servidor Telnet interactúa con la aplicación, actuando como un sustituto del gestor del terminal, para que de esta forma el terminal remoto le parezca local a la aplicación. El tráfico que se genera se realiza sobre una conexión TCP.

Telnet no proporciona un sistema de autentificación y la comunicación no está cifrada, este protocolo prácticamente no se utiliza. Aunque este protocolo se ha utilizado como base para otros protocolos.

SSH

Secure Shell, protocolo de acceso remoto que tiene una aplicación que lo implementa con el mismo que proporciona un método para acceder de forma segura a un equipo remoto. SSH se utiliza en terminal de texto, aunque se pueden ejecutar aplicaciones gráficas, mediante una línea de comandos podemos ejecutar comandos de forma remota. SSH utiliza el puerto por defecto 22, esto es configurable, para trabajar.

SSH utiliza una arquitectura cliente-servidor y es muy utilizado en Linux para administrar equipos remotos, debido a que la comunicación está cifrada, todo lo que se envía o recibe se encripta. Por este motivo también se utiliza con otros protocolos para hacerlos más seguros.

El protocolo SSH proporciona los siguientes tipos de protección:

- Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.
- El cliente transmite su información de autenticación al servidor usando una encriptación robusta de 128 bits.
- Todos los datos enviados y recibidos durante la sesión se transfieren por medio de encriptación de 128 bits, lo cual los hacen extremamente difícil de descifrar y leer.

- El cliente tiene la posibilidad de reenviar aplicaciones X11 [1] desde el servidor. Esta técnica, llamada reenvío por X11, proporciona un medio seguro para usar aplicaciones gráficas sobre una red.

Para acceder a un equipo remoto tenemos varios sistemas de seguridad como una contraseña o claves RSA que ofrece más seguridad y evita escribir contraseñas.

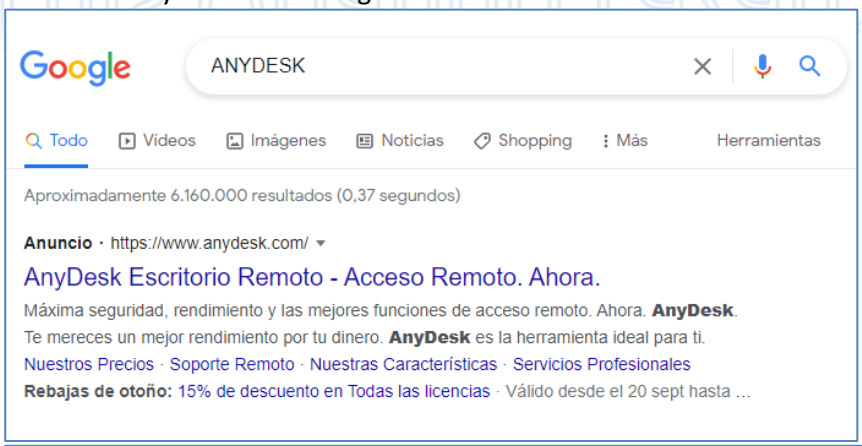
Tunneling sobre SSH

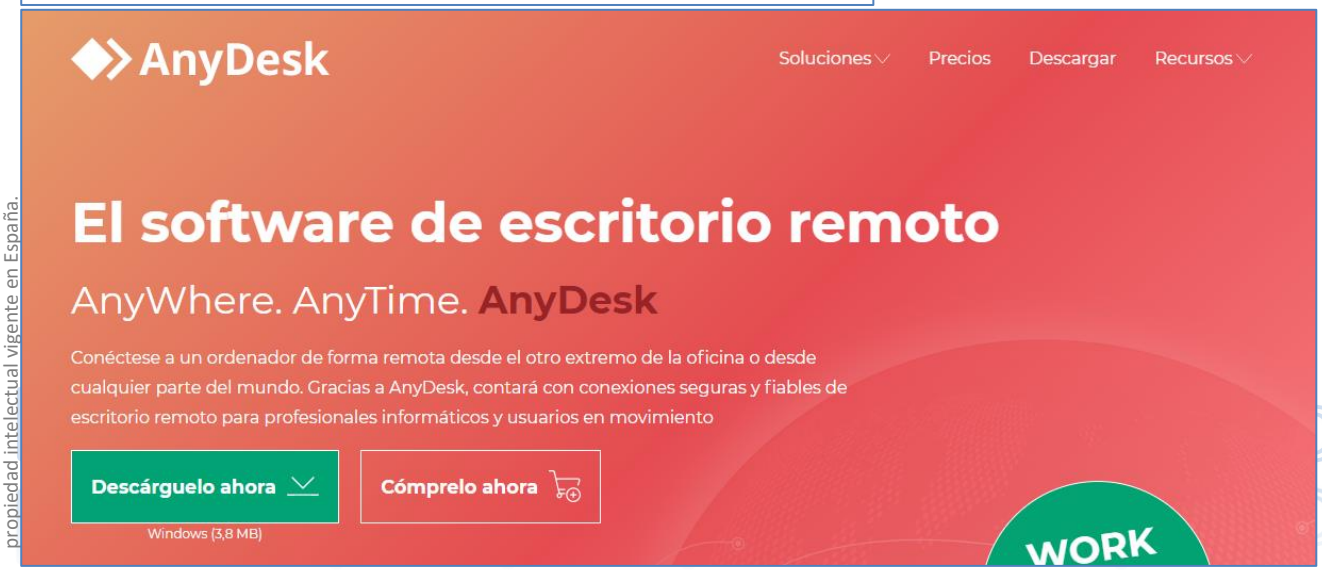
Un uso de SSH es utilizarlo para asegurar otro protocolo, esto denomina hacer un túnel con SSH o Tunneling. Los túneles pueden ser locales o remotos. En los túneles locales, es nuestra máquina la que redirecciona un puerto hacia un puerto remoto de una segunda máquina, a la que se tiene acceso. Los túneles remotos es a la inversa, es decir, la máquina remota redirecciona un puerto hacia nuestra máquina. La técnica de tunelizar puede ser usada también para evitar o circunvalar un cortafuegos. Para ello, se encapsula el protocolo bloqueado en el cortafuegos dentro de otro permitido, habitualmente HTTP.

Anydesk

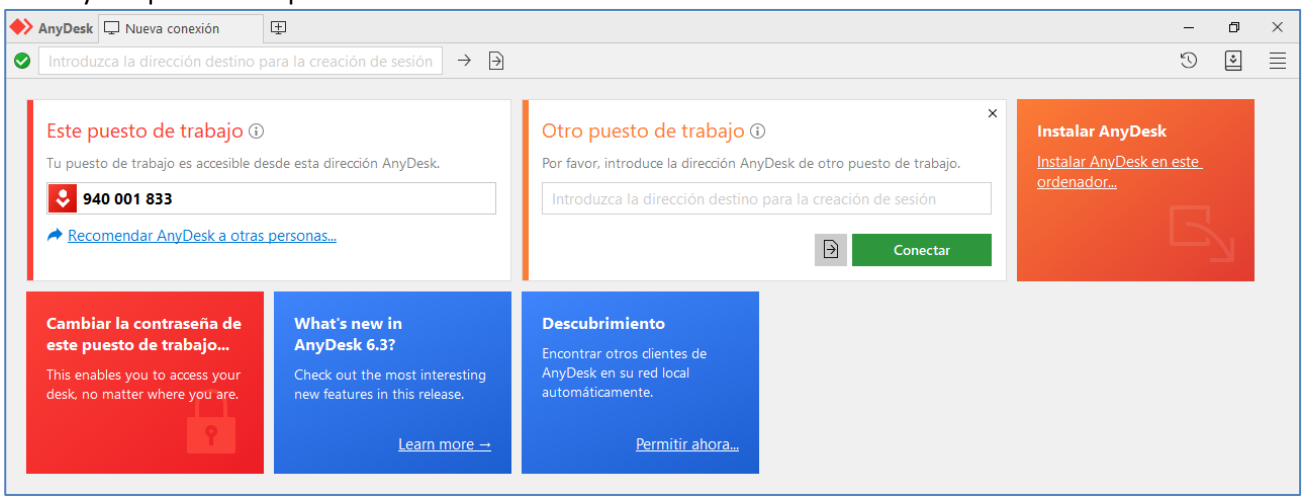
AnyDesk es un programa de software de escritorio remoto desarrollado por AnyDesk Software GmbH en Stuttgart, Alemania. Provee acceso remoto bidireccional entre computadoras personales y está disponible para todos los sistemas operativos comunes. El software ha estado en desarrollo activo desde 2012

Buscamos Anydesk en el navegador:

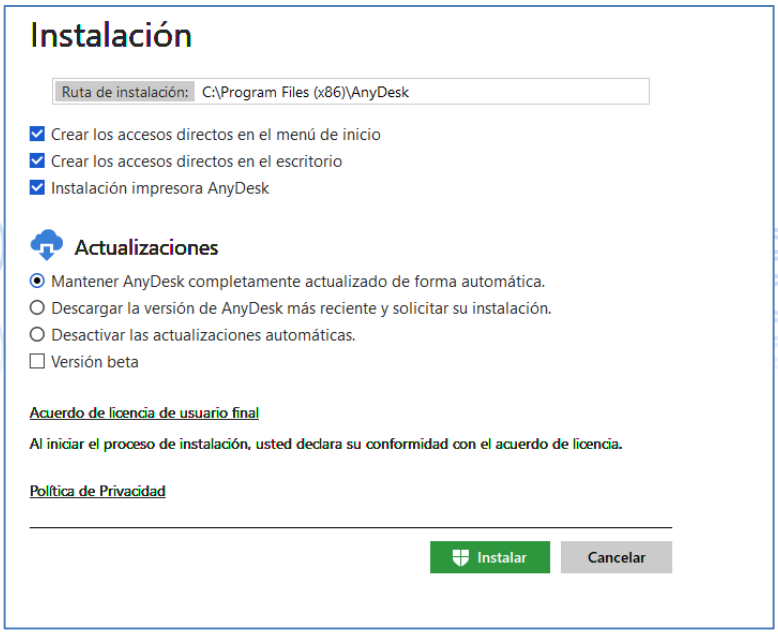




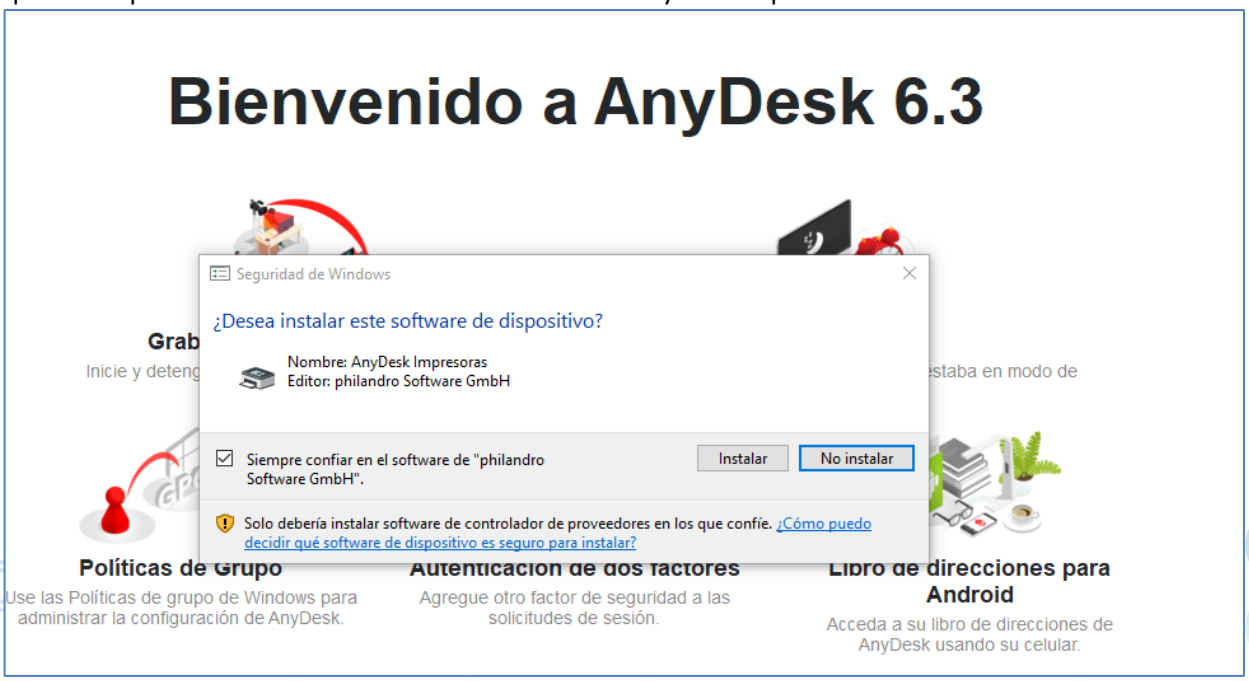
Ahora ya se puede usar pero no está instalado:



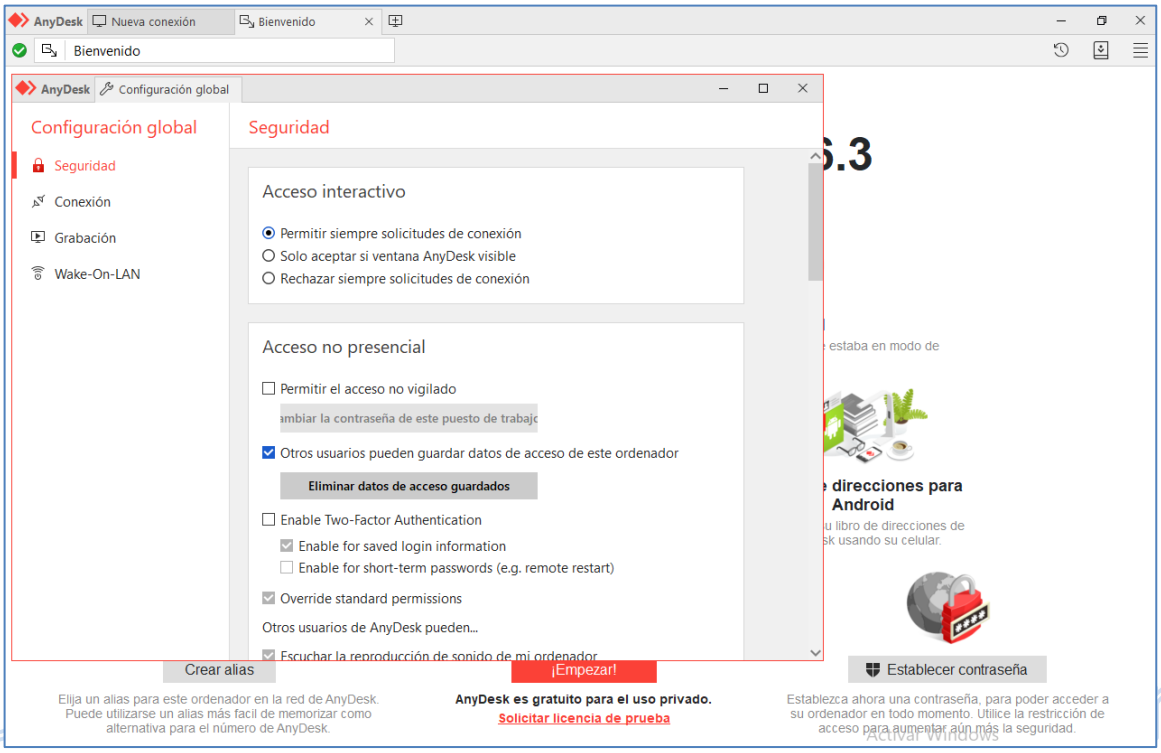
Lo Instalamos:



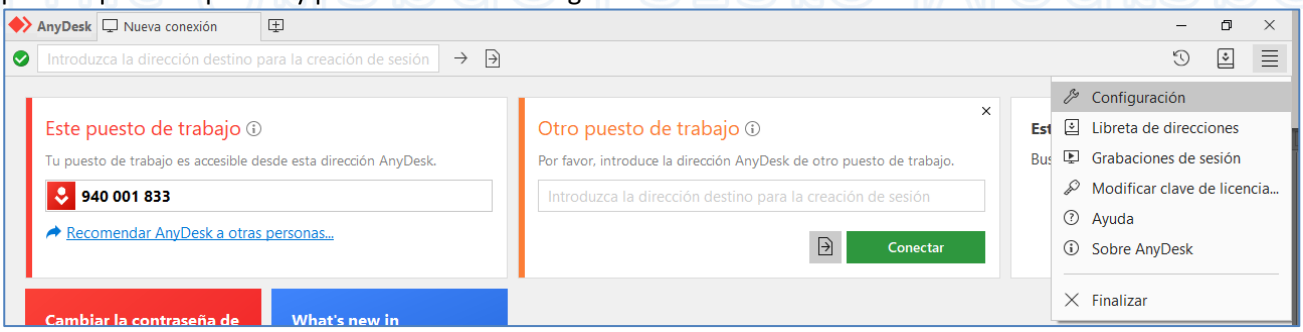
Si quieres imprimir remotamente… Le darías a Instalar AnyDesk Impresoras:



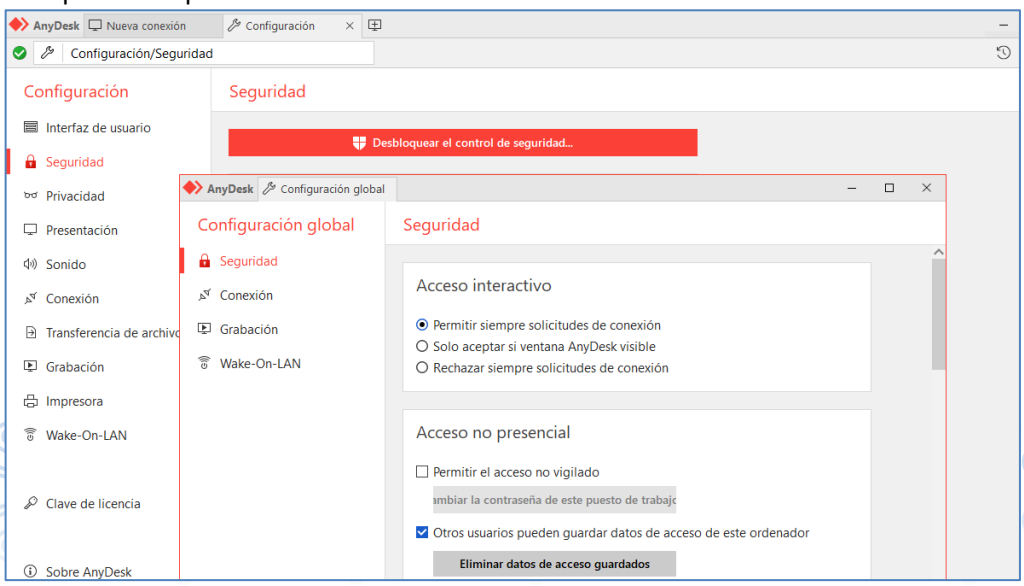
Por defecto para conectar a un equipo remoto tienes que darle autorización, pero tenemos una opción de conexión con contraseña sin necesitar autorización, para poder hacerlo pulsamos sobre **Establecer Contraseña**



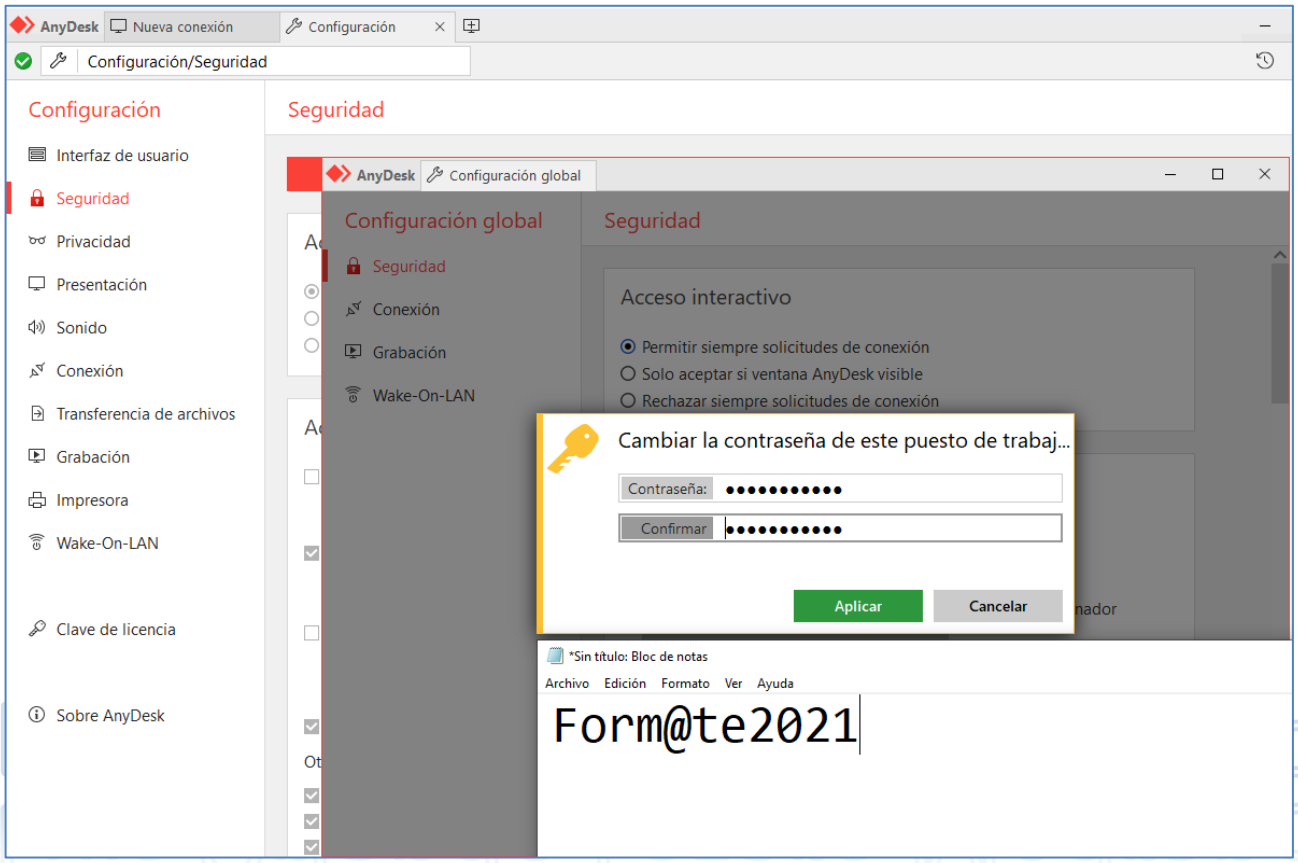
Si habéis cerrado la ventana anterior podemos volver a acceder desde el menú de administración de la parte superior izquierda y pulsamos sobre configuración:



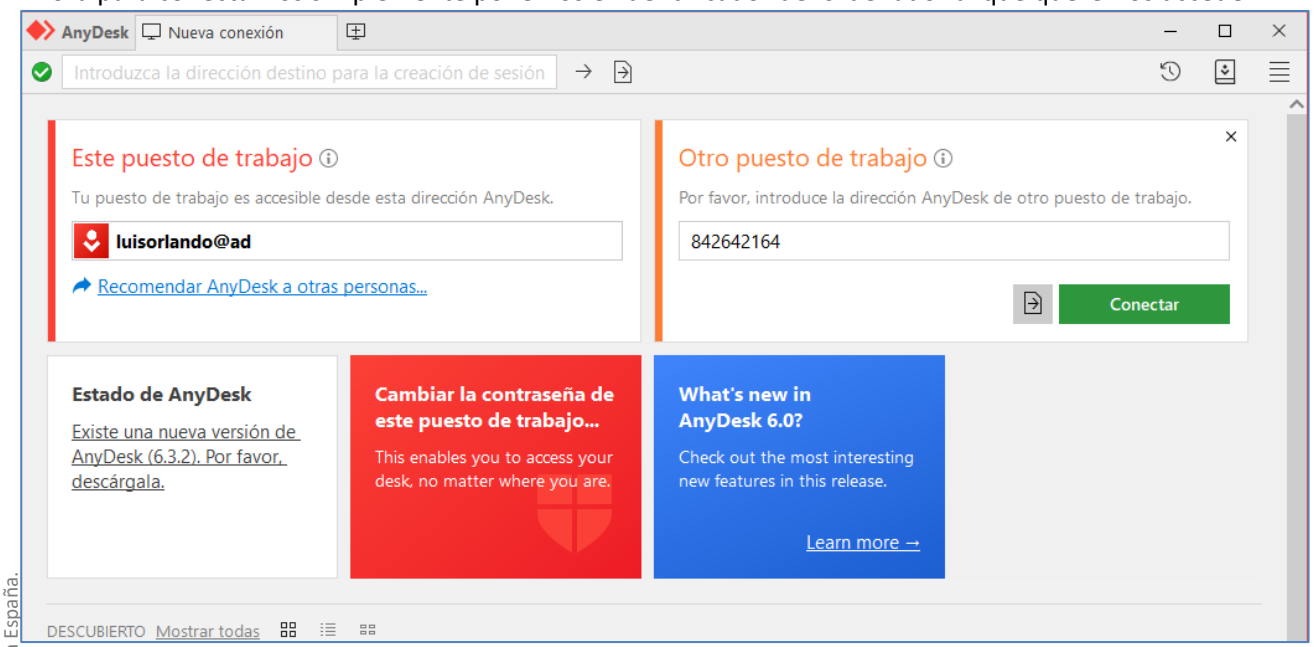
Y en la pestaña **Seguridad** pulsamos sobre el botón **Desbloquear el control de seguridad…** y accedemos a la misma pestaña que en la opción anterior:



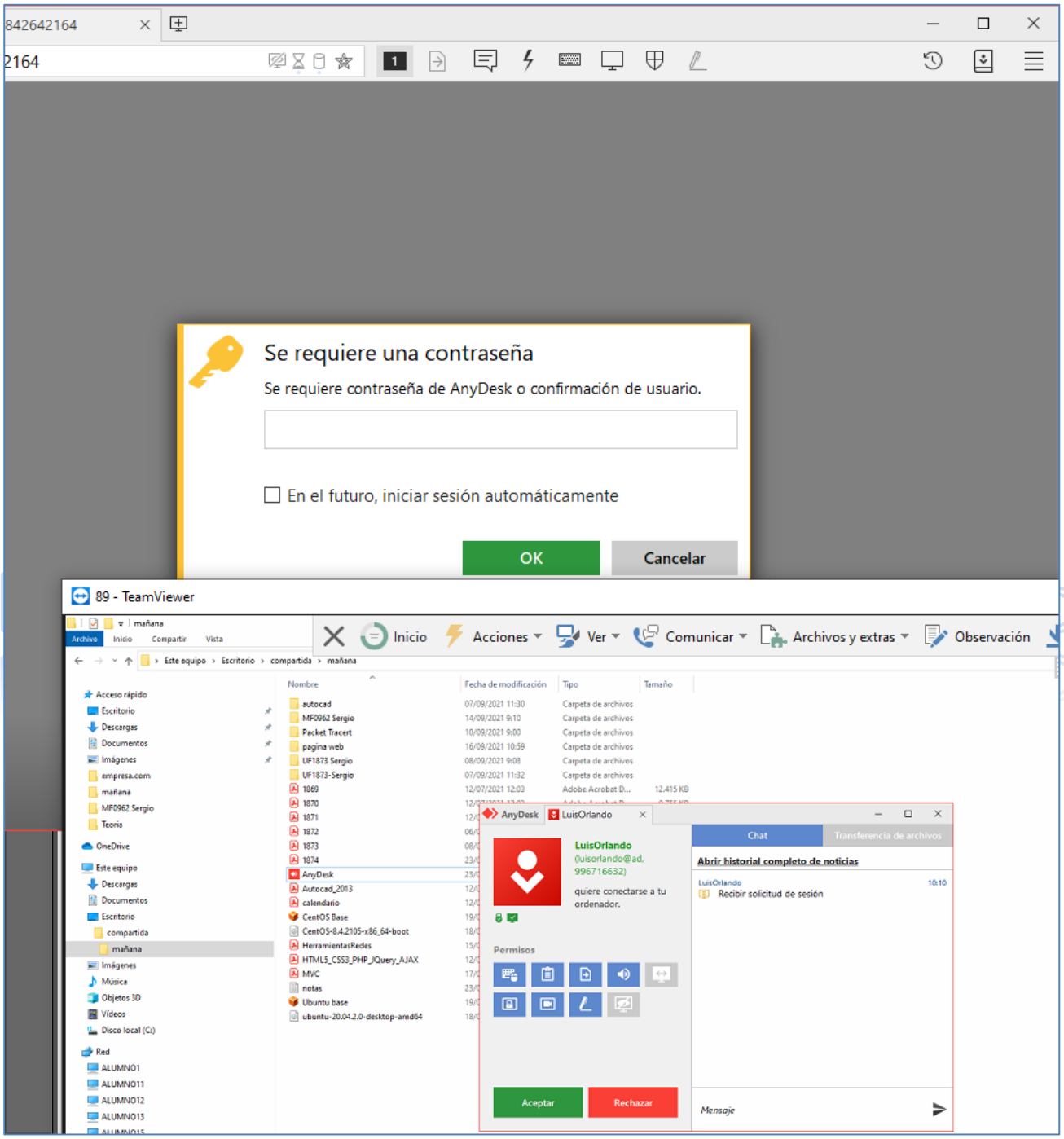
Pulsamos sobre **Permitir el acceso no vigilado** y le ponemos la contraseña segura, por ejemplo Form@te2021:



Ahora para conectarnos simplemente ponemos el identificador del ordenador al que queremos acceder:



En el equipo remoto aparecerá una petición e confirmación, pero si hemos puesto contraseña podríamos conectarnos sin solicitar autorizaciones.



Y si marcamos la casilla **En el futuro, iniciar sesión automáticamente** no necesitarías volver a escribir la contraseña en próximas conexiones.

De cualquier forma para cerrar una conexión remota, simplemente pulsamos sobre Rechazar…

2.2. Mantenimiento correctivo y preventivo

Después de la puesta en funcionamiento de una red de comunicación, por diversos factores se producen errores que se deben reparar, tanto problemas en hardware como software. Estas reparaciones deben influir lo más menos posible en el funcionamiento y en caso de tener que para el funcionamiento de la red que sea en el menor tiempo posible.

El mantenimiento se debe realiza de forma periódica y tener planificado un calendario de mantenimiento, cada componente de la red necesita una periodicidad diferente, hay que tener diferentes factores para

decidir esa periodicidad como: el uso del componente, el lugar donde se encuentre, la importancia del componente, etc.
Todo el mantenimiento debe estar reflejado en algún documento para su posterior estudio para detectar fallos reincidentes y realizar un estudio para detectar defectos en la red y corregirlos para que no se vuelvan a producir. Podemos considerar dos tipos de mantenimiento:

- Mantenimiento correctivo: se efectúa después de producirse el error, consiste en reparar el error y estudiar las causas para que no se vuelva producir.
- Mantenimiento preventivo: se efectúa antes de producirse un error y evitar que se produzca.

Mantenimiento Correctivo
Este tipo de mantenimiento se realiza después de un fallo o problema surge en un sistema, con el objetivo de restablecer la operatividad del sistema. En algunos casos, puede ser imposible de predecir o prevenir un fracaso, lo que hace el mantenimiento correctivo la única opción.
El proceso de resolución de un fallo requiere un proceso dinámico y fluido requiere actuar rápido, el tiempo de respuesta debe ser lo más bajo posible para que error afecto el menor tiempo posible a la red. La primera regla que se debe tener en cuenta antes de resolver el problema, es no estropear datos, haga copia de seguridad de los datos antes de empezar, porque en el proceso de resolver el problema puede perder datos que son importantes. Los pasos básicos para resolver un problema son.

- Establecer los **síntomas**: saber que le ocurre a la red, esto se puede saber de varias formas. Preguntando al usuario que describan lo ocurrido, extrayendo información para su posterior análisis o con una alerta del sistema.
- **Aislar la causa del problema**: saber el alcance del error, para saber la gravedad del error producido y si ha afectado a otras partes de la red.

Mantenimiento correctivo, es aquel que corrige los defectos observados en los equipamientos o instalaciones, es la forma más básica de mantenimiento y consiste en localizar averías o defectos y corregirlos o repararlos. Pasos:

- Establecer qué ha cambiado: acotar el error al elemento donde se ha producido (hardware, software, error de usuario, etc.) identificando qué ha cambiado en el sistema. Esto se puede conseguir con información del usuario, examinando datos de la red, software y hardware.
- Identificar la causa más probable: con la información obtenida en los anteriores pasos y la experiencia, se debe escoger la causa del error más probable.
- Determinar las competencias: informar a los usuarios que le haya afectado el error, también es necesario informar a los superiores para tomen una decisión.
- Implementar una solución: ya se tiene una idea del error, escoger la solución más adecuada de todas las posibles.
- Probar la solución: solo intente una solución, si prueba varias soluciones a la vez no sabrá cual de ellas ha resuelto el error.
- Comprobar los efectos de la solución: la solución no debe disminuir el rendimiento de la red, ni realiza modificaciones sin autorización. Si el error se ha resuelto y el funcionamiento es correcto, se ha conseguido un rendimiento igual o mayor al rendimiento antes del error, la solución era la adecuada.
- Documentar la solución: se crea una base de conocimientos para referencia futuras y solucionar errores futuro de forma mas rápida.

El primer paso para resolver el error es obtener información sobre el sistema, la información se puede obtener de los usuarios. Hay diferentes formas de obtener de los usuarios, como realizar entrevista para obtener información que será muy importante para saber lo que ha pasado.
Los responsables de red, sobretodo en redes grandes, necesitan la ayuda de los usuarios para detectar los errores. Hay herramientas software que ayudan en la comunicación entre los técnicos y los usuarios. Este tipo de herramientas se denominan Gestión de incidencias.
Los gestores de incidencias son utilizados en múltiples ámbitos, su funcionamiento es sencillo, mediante una interfaz web un usuario rellena un formulario indicando los síntomas que ha detectado, este formulario se envía a algún técnico. Este formulario con información del usuario se denominan incidencia o tickets, el

técnico debe solucionar el problema expuesto en la incidencia, este proceso se denominan cerrar la incidencia.

Cuando se rellena una incidencia se proporciona una serie de datos para facilitar el trabajo a los técnicos.

- Nombre del usuario.
- Lugar por si el técnico debe desplazarse.
- Descripción de los síntomas que ha detectado el usuario.
- En algunos errores, el sistema muestra información, incluirla en la incidencia.

Los técnicos examinarán los datos de la incidencia y si consideran oportuno, añadirán más información y asignarán recursos que sean necesarios, como personal.

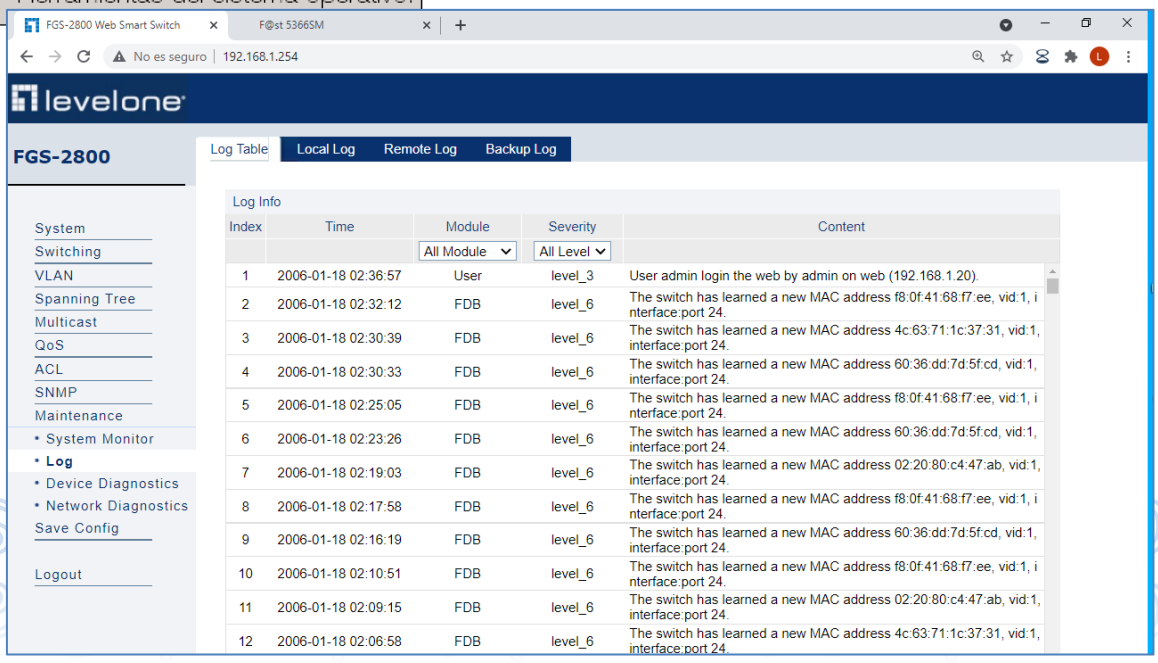
Las incidencias tienen una serie de estados definidos, aunque las herramientas de gestión de incidencias pueden tener estados propios. Podemos considerar una serie de estados comunes, como los siguientes:

Abierta	La incidencia ha sido enviado por un usuario.
Asignada	La incidencia ha sido asignada a un técnico para ser examinada.
En proceso	Un técnico está trabajando en la incidencia.
Cerrada	El problema se ha resuelto, se debe detallar solución que ha sido aplicada.

Aparte de la información que puedan aportar los usuarios, el técnico necesitará otra información más técnica o información que proporciona el sistema.

Esta información se puede obtener mediante un conjunto de herramientas (software y hardware) que nos facilitan el proceso de obtener los datos para un examen con detalle.

Tipo	Herramientas
Hardware	– Comprobadores de cables, TDR. – Analizadores de protocolo. – Software de diagnostico y log.
Software	– Visor de log. – Análisis forense. – Herramientas de monitorización. – Herramientas del sistema operativo.



Diagnostico Hardware

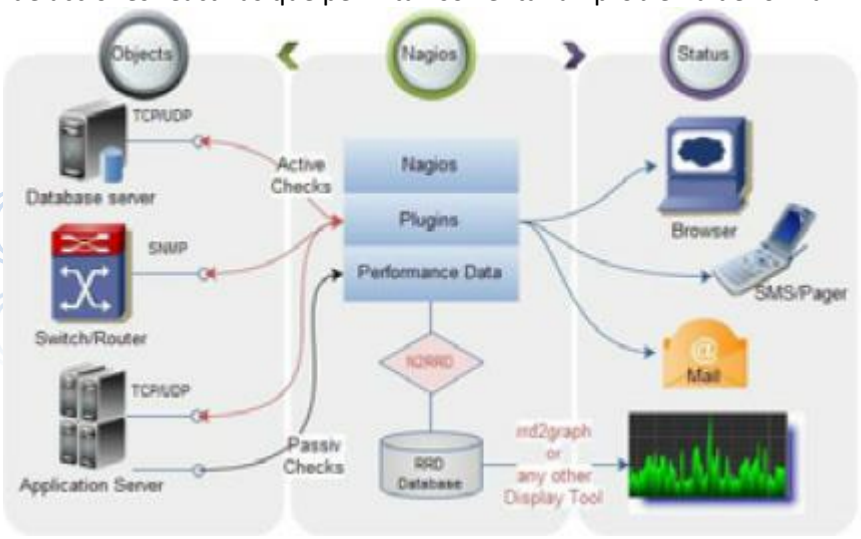
Para este tipo de diagnóstico tenemos disponibles una serie de herramientas para comprobar diferentes partes de una red.
Uno de los componentes que pueden ser causa de errores son los cables, los errores que se producen son desconexión total, cuando un cable falla no produce fallos intermitentes o pérdida de velocidad de transmisión, un cable funciona o no. Hay varios tipos de herramientas para diagnóstico de cables que ya hemos visto en otros módulos.
Cuando tenemos problemas en una red por el rendimiento, baja velocidad o determinados servicios no funcionan correctamente. Para detectar erros podemos examinar el tráfico de la red.
El hardware y software de una red funcionan por medio de un protocolos que especifican su funcionamiento, se examinamos el trafico de esos protocolos podremos detectar errores en el funcionamiento.
Un analizador de protocolo monitorización los distintos protocolos que están en funcionamiento en la red, pueden ser hardware o software, nos permite ver los datos en la red para ver los problemas como ralentizaciones, exceso de tráfico o algún tráfico inesperado.
Hay determinado software que nos permite realizar un diagnostico del dispositivo, en computadoras tenemos software que hace diagnostico de la memoria RAM, CPU, disco duro, etc., generando un informe con el resultado.
Dispositivos como router, servidores, puntos de acceso, etc., guardan información de todos los eventos que se producen durante su funcionamiento, este fichero se denomina log. Este fichero está en formato de texto y muestran la información muy legible, si el log es muy extenso o para visionar varios log, existen visores de log que nos facilitan el visionado.
En una red se pueden producir errores en software que hay instalado en una red (sistemas operativos y aplicaciones) o en el software del dispositivos hardware de la red. Hay disponibles software para diagnostico, el primero son log, visto anteriormente, pueden proporcionar información muy valiosa para detectar la causa del error.
Cuando surge un error irreparable, por ejemplo rotura de un disco duro, debemos conocer las causas de ese error, recuperando los datos del dispositivo para examinarlos. Para realizar esta tarea tenemos el análisis forense que son una serie de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.
Ejemplo de este tipo de herramientas es Sleuth Kit.
Una lista de diferentes técnicas que se pueden utilizar.

- Recuperación de datos borrados.
- Recuperación de los datos de una imagen.
- Clonado de dispositivos.
- Recuperar registros.
- Volcado de memoria.
- Análisis de imágenes.
- Recuperación de contraseñas.
- Recuperación de datos cifrado.

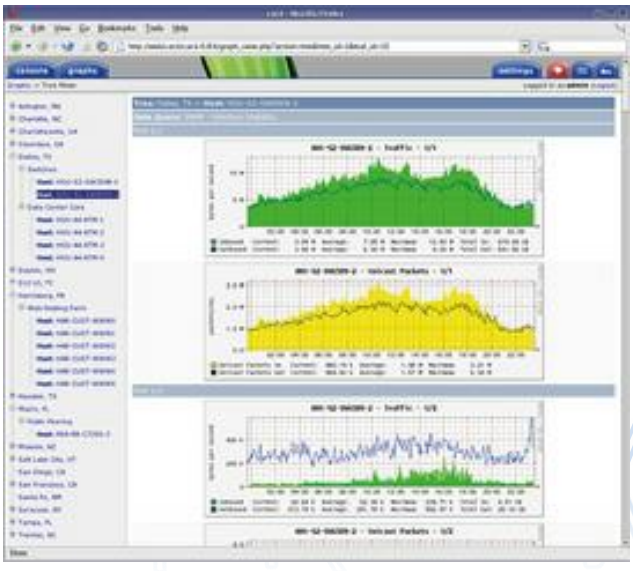
El primer paso para el análisis forense es realizar un duplicado exacto de la información de todas las fuentes de datos. El siguiente paso, analizar cualquier rastro que pueda identificarse y por último realizar un informe técnico, donde describirán la causa o causas del error, y un informe ejecutivo con las acciones a ejecutar para evitar ese error.
Toda red necesita de vigilancia y que alerte cuando ha surgido algún fallo. Una herramienta de monitorización realiza esta tarea, es un software que se encarga de comprobar el estado de la red, en caso de que ocurra un fallo en el dispositivo, poder enviar un mensaje a los responsables correspondientes.
Una herramienta de monitorización puede vigilar el estado tanto de software como de hardware, proporciona información sobre el funcionamiento de dispositivos de una red, incluso puede proporcionar gráficas de diferentes parámetros.

Una de las herramientas mas utilizadas es **Nagios**, de monitorización de redes de código abierto que vigila equipos (hardware) y servicios (software) que genera alertas en función de ciertos parámetros y avisando a los responsables en caso necesario. Nagios proporciona una interfaz web para administrar y visualizar los datos de la monitorización.
Nagios es muy versátil y tiene un plugin de sistema para añadir nuevas características, aunque es un poco complejo de configurar. Un resumen de sus características.

- Monitorización de múltiples servicios.
- Monitorización de hardware.
- Monitorización remota.
- Diferentes tipos de notificaciones, correo electrónico, sms, etc.
- Posibilidad de definir manejadores de eventos.
- Monitorización de factores ambientales a través de sondas físicas.
- Múltiples tipos de gráficos.
- Programación de intervalos de tiempo sin notificaciones.
- Soporte de arquitecturas de servidor redundantes y distribuidas.
- Definición de acciones reactivas que permitan solventar un problema de forma inmediata.



Como alternativas a las herramientas de monitorización, tenemos las herramientas generación gráficas de red. Son herramientas que presentan múltiples gráficas del estado del sistema, este tipo de herramientas son sencillas de instalar y configurar, solo visualizan gráficas, pero proporcionan de forma visual mucha información que puede ser útil para detectar fallos en la red.
Ejemplo de este tipo de herramientas son Cacti o Munin que nos permite generar múltiples gráficas de diferentes parámetros.



Los sistemas operativos incluyen un conjunto de herramienta para realizar diversas tareas de monitorización. Son pequeños programa de **línea de comandos** que realizan determinadas tareas, pero al ser incluidas en el sistemas operativo no necesitan instalación ni configuración. Pueden ser muy útiles en determinados momentos, su conocimiento es muy aconsejable. Una lista de algunas de ellas se muestra a continuación. Entre paréntesis aparece su nombre en Windows.

Nombre	Tarea
Tracert(traceroute)	Se utiliza para trazar todos los enrutadores que hay entre dos puntos.
Ifconfig(ipconfig)	Muestra información de la interfaz red del computador.
Ping	Sirve para comprobar la conexión a un equipo.
Dig(nslookup)	Para realizar comprobaciones de DNS.
MTR	Traceroute de forma dinámica, muestra la información en tiempo real.
Route	Visualiza y edita la tabla de enrutamiento.
Netstat	Muestra información de todos los procesos IP que se están ejecutando.

Hay una herramienta muy útil en redes, para descubrir su alguien ha entrado en el sistema es un escáner de puertos que muestra información de los puertos del sistema, indicando cuales están abierto o cerrados.
En un sistema se deben tener los mínimos puertos abiertos posibles, solo aquellos puertos que utilicemos, el resto de puertos deben estar cerrados. Un puerto abierto en una forma para que un atacante pueda entra en el sistema sin permisos y obtener el control del equipo, si el atacante tiene un control de un equipo de la red puede seguir atacando los diferentes dispositivos, produciendo múltiples errores y más daños a la red.
Cuando se produce un error en la red, puede ser que se ha haya producido por un ataque del exterior, debemos cerrar el acceso al atacante. Con un escáner de puertos podemos comprobar si hay puertos abiertos no deseados y cerrarlos para impedir posibles intrusiones.
Un ejemplo de escáner de puerto es NMAP un escáner muy potente de código abierto.

Mantenimiento Preventivo

Es el mantenimiento que se realiza para evitar posibles errores, este tipo de mantenimiento se deben realizar periódicamente una serie de revisiones para detectar posibles errores y actuar antes de que se produzca el error. El mantenimiento correctivo conlleva una serie de ventajas.

- Mayor duración de los equipos: en las revisiones periódicas se realiza un mantenimiento para evitar futuros errores.
- Disminución en el tiempo cortes del servicio: si hay menos fallos en la red, porque se han prevenido, el tiempo que la red deja de funcionar será bastante menor.
- Menor gasto en reparaciones: los errores que se producen son menos graves, su reparación será más barata.
- Aumenta de la seguridad.

El objetivo de este mantenimiento es que todos los componentes de la red estén funcionando de manera óptima, tanto el hardware como el software.

Actualizaciones y parches de seguridad

En toda red el software es uno de los componentes más importantes y donde más errores se pueden producir. No existe software sin errores porque no se puede desarrollar un software sin errores, para resolver este problema están las actualizaciones.
Las actualizaciones sirven para mejorar un software, arreglando errores de versiones antiguas o mejorando su funcionamiento. Estas actualizaciones pueden ser pequeñas correcciones errores o versiones nuevas que incluyen correcciones de errores, nuevas funcionalidades, mejoras de rendimiento, etc.
Los sistemas operativos incluyen un sistema de actualizaciones, que son programas que se conectan a un determinado servidor que comprueban si los programas instalados tienen actualizaciones disponibles, si aceptamos estas actualizaciones, se descargarán e instalarán en el sistema de forma transparente al usuario.

En Windows y Linux tenemos los siguientes programas de actualización.

Programa	Funcionamiento
Windows update	Se conecta a un servidor de actualizaciones propio, dependiendo de la configuración establecida, descarga e instala las actualizaciones del sistema operativo y aplicaciones de Microsoft. El resto de aplicaciones no son soportadas.
Apt-get, yum, etc.(depende de la distribución de Linux)	Se conectan a un repositorio, un servidor almacena múltiples aplicaciones, y comprueba si hay actualizaciones para todo el sistema (incluyendo aplicaciones), las descarga e instala. Cualquier persona puede crear un repositorio, hay unos repositorios oficiales y otros no oficiales que pueden contener aplicaciones no encontradas en el oficial, incluso repositorio para un determinado software. Hay diferentes tipos de repositorio en función de la estabilidad: estable para software bastante probado y es más seguro. O desarrollo, que contiene software que tiene menos estabilidad porque todavía no ha sido conveniente probado.

Como ejemplos veremos cómo funciona yum, gestor de paquetes en formato rpm, se utiliza para instalar nuevos programas (paquetes en Linux), como realizar actualizaciones del sistema o desinstalar programas. Este gestor es originaria de una distribución denominada Yellow Dog, en la actualidad se utiliza en otras distribuciones como Fedora o Centos.

El funcionamiento es simple, primero hay que configurar los repositorios que son direcciones web que se almacenan en un archivo denominado yum.conf, también se pueden almacenar cada repositorio en su propio fichero con extensión .repo.

Ejemplo de dirección de un repositorio.

http://download1.rpmfusion.org/free/fedora/releases/$releasever/Everything/$basearch/os/

Se pueden añadir múltiples repositorios en el archivo yum.conf, en todos comprobará si hay actualizaciones, aunque no es muy recomendable mezclar muchos repositorios.

Dentro del fichero de configuración tenemos disponibles un conjunto de opciones que se aplican a los repositorios, como activar o desactivarlos, una lista de servidores donde se encuentra copia del repositorio.

Los repositorios se pueden incluir manualmente en el archivo de configuración o mediante un paquete instalable con yum.

Hay diferentes tipos de repositorios en función del tipo de paquetes que almacena. Hay tres categorías principales (Oficial, Desarrollo y Testing) y en cada uno de ellas se le pueden aplicar una serie de opciones (Free, Non-Free y source).

Tipo	Descripción
Oficial	Almacena paquetes estables, muy probados y con menos errores, por este motivo no contiene las últimas versiones de los paquetes. Es utilizado en equipos donde prima la estabilidad por encima de todo, como diferentes tipos de servidores.
Desarrollo	Almacena paquetes con la última versión de los paquetes y tiene menos estabilidad al no estar suficientemente probadas, aunque son funcionales.
Testing u otros nombres	Contiene paquetes con las versiones que están en desarrollo, son altamente inestables y solos se recomienda su uso para pruebas.
Free	Contiene paquetes con licencias libres.
Non-Free	Contiene software propietario o no contiene una licencia libre.
Source	Solo incluye el código fuente de los paquetes, no incluye los binarios (ejecutables).

Con los repositorios configurados correctamente, ya podemos utilizarlo para actualizar el sistema. Veremos cómo se utiliza yum en el terminal, aunque hay diferentes interfaces gráficas. Para actualizar el sistema.

yum update

Se conectará a los repositorios activos y si hay nuevas actualizaciones de los paquetes instalados en el sistema. Las mostrará en pantalla y nos preguntará si queremos actualizar. También podemos actualizar un solo paquete.

yum update nombre_paquete

Muestra por pantalla si hay una actualización del paquete y las dependencias, que son paquetes necesarios para el correcto funcionamiento del paquete actualizado.

Herramientas como yum o apt-get son más versátiles, pero más complejas de utilizar. Herramientas tipo Windows Update son más simples, pocas opciones de configuración y son más fáciles de utilizar, pero solo actualizan las herramientas del sistemas y no las aplicaciones instaladas (excepto las de Microsoft), que deben tener sus propios métodos para actualizarse.

Cuando una actualización solo corrige errores que no modifican la funcionalidad del programa, se denominan **parches de seguridad**. Estos parches arreglan errores de seguridad que pueden ser utilizados para que un atacante externo acceda al sistema a través de una aplicación instalada.
Una actualización puede resolver errores de diferentes tipos.

Tipo	Descripción
Errores de funcionamiento	Corrigen un mal funcionamiento del sistema, implica cortes en el funcionamiento, reinicios inesperados.
Errores de seguridad(vulnerabilidades)	Corrigen errores de acceso no autorizados, este tipo de error no afecta al funcionamiento.
Errores de rendimiento	Corrigen errores que afectan al funcionamiento óptimo, ralentizaciones, consumo excesivo de recursos, conexiones intermitentes.
Errores de ataque día-cero	Son errores que no han sido detectados y no se han arreglado. Por medio de diferentes técnicas protección podemos evitar que se produzcan.

Para estar informados sobre los parches de seguridad, como saber el contenido de estos parches, los errores que resuelven. Como de las diferentes actualizaciones de un determinado software. Tenemos disponibles los boletines de seguridad, son páginas web que muestran información de las diferentes actualizaciones. Es recomendable, estar suscritos (por RSS) a los boletines de seguridad del software instalado en nuestra red.
Un listado de diferentes boletines de seguridad se muestra a continuación.

Dirección web del boletín	Descripción
http://technet.microsoft.com/es-es/security/bulletin	Boletín de seguridad de Microsoft.
http://unaaldia.hispasec.com/	Hispasec proporciona boletines de seguridad de diferentes software.
http://secunia.com/community	Boletín de seguridad para múltiples software.
http://www.adobe.com/support/security/	Boletín de seguridad de productos de Adobe.
http://www.oracle.com/technetwork/topics/security/alerts-086861.html#SecurityAlerts	Boletín de seguridad de Oracle.
https://www.ccn-cert.cni.es/	Boletín de seguridad de diferentes software.
http://www.exploit-db.com/	Base de datos de diferentes tipos de exploits.
http://www.cvedetails.com/	Página web que muestra información sobre vulnerabilidades, se puede filtrar la información por diferentes parámetros.
http://cert.europa.eu/cert/newsletter/en/latest_Security%20Bulletins_.html	Boletín de seguridad del CERT.
http://httpd.apache.org/security_report.html	Boletín de seguridad del servidor web Apache.

Debemos tener el sistema actualizado, pero también debemos controlar la red de posibles errores, alguna herramienta vista en el mantenimiento correctivo, como herramientas de monitorización que se pueden configurar para que generen una alerta cuando se produzca una bajada de rendimiento, poder estudiar las causas y reparar, antes que esa bajada vaya a mayores.
Cualquier equipo que tenga acceso a internet, implica ciertos riegos de seguridad y debe estar protegido convenientemente con soluciones hardware o software. Principalmente deberíamos tener en cuenta dos tipos peligros.

- Virus informáticos: pequeños programas que se ejecutan de forma no autorizada en el equipo.
- Intrusiones: un ataque del exterior de la red que se realiza para tener acceso no autorizado del equipo.

Virus informáticos

Antiguamente los virus informáticos podían incluso dañar una computadora, hoy en día los virus tienen otros objetivos y no suelen producir daño porque tratan de ocultarse al usuario. Hay diferentes **categorías** de virus.

Categoría	Descripción
Troyano	Programas que se ocultan dentro de otro programa inofensivo, que se utilizan para tener acceso al sistema.
Gusano	Programas cuyo fin es duplicarse a sí mismo y propagarse lo más rápido posible, el peligro es el colapso que puede producir en la red.
Spyware	Programa que recopila información de un ordenador, sin permiso del usuario, y la envía a alguna empresa externa, generalmente esa información se usa para publicidad, este tipo de software sí puede afectar al rendimiento del equipo.
Rootkit	Programa que se utiliza para ocultar el rastro de un programa malicioso.

Para evitar la infección la solución más utilizada en el uso de software Antivirus, este tipo de software detecta el rastro que deja un virus que se denomina firmas. Los antivirus poseen una base de datos con una amplia variedad de firmas, que continuamente se van actualizando, que son utilizadas para compararlas con los archivos del sistema y comprobar si hay virus.

Este proceso es muy costoso porque para poder firmas de virus, este debe existir anteriormente, mediante el envió de ficheros infectados con ese virus por parte de los usuarios. Para facilitar esta tarea, todos los antivirus incluyen técnicas heurísticas que son técnicas de análisis que se emplean para detectar cualquier virus aun sin haberlo analizado antes y sin estar en la base de datos del antivirus.

Los métodos heurísticos usados actualmente se basan en el "desmontaje" del código de los virus y en el análisis de sus puntos críticos, buscando la secuencia o secuencias de instrucciones que diferencian a los virus de los programas "normales".

Cuando un antivirus detecta un virus genera una alerta y puede ejecutar una acción como eliminar el virus u otra acción.

Dentro de la categoría de antivirus podemos detectar dos tipos en función el tipo de la protección y al usuario que va enfocado.

- Antivirus **personales**: se instalan en la máquina del usuario, siempre están ejecutándose en segundo plano para detectar virus en cualquier momento. En algunos casos se engloban dentro de otros productos como cortafuegos, antispam, control parental, etc. Son productos fácil de instalar y utilizar, como desventajas tenemos que en redes pueden ser bastante costosos porque una instalación por equipo, en algunos casos pueden consumir bastantes recursos. Como ejemplo de antivirus personales tenemos Avast, Nod32, Panda, McAfee Kaspersky.
- Antivirus **corporativo**: está enfocado en un entorno de red para empresas, organismo o universidades, donde hay redes con un gran número de equipos. Este tipo de antivirus consta de dos partes; una parte servidor donde se instala el antivirus y una parte cliente que se instala en los equipos de los usuarios, que es un pequeño programa que se utiliza para comunicarse con el servidor del antivirus. Las actualizaciones de las firmas de los virus se realizan solo en el servidor, en los clientes solo hay un pequeño programa para detectar los virus. Este tipo de antivirus tiene la ventaja que en grandes redes son más baratos que instalaciones individuales de antivirus personales, la configuración y gestión centralizada. Por el contrario, son más complejos de instalar y administrar. Prácticamente todas las empresas de antivirus tiene una versión corporativa.

Intrusiones

En toda red se produce múltiples intentos que acceso no autorizados desde el exterior, si un atacante consigue acceso a la red los resultado pueden ser devastadores. Hay que evitar este tipo de acceso y detectarlos lo antes posible para evitar daños mayores.

Un tipo de software que se encarga detectar intrusos que se denomina IDS (Sistema de detección de intruso). Este tipo de software se encarga de interpretar el tráfico de red o actividades hostiles. Un IDS incluye una base de datos con las firmas de ataques conocidos, que son actualizadas, y pueden comparar patrones de actividad, tráfico o comportamiento que ve en los datos que monitoriza contra las firmas para reconocer cuándo se da una coincidencia entre una firma y un comportamiento actual o reciente. En ese caso, el IDS puede lanzar alarmas o realizar varias automáticamente.

Un IDS se puede considerar como un antivirus para intrusos, los dos tienen una base de datos firmada, hacen comparaciones con las firmas y generan alertas.

La detección de intrusión significa detectar un uso no autorizado o ataque a un sistema de red. Un IDS se diseña para detectar ciertos ataques o usos no autorizados de sistemas, redes u otros recursos, y desviarlos o impedirlos si es posible.
Los IDS pueden ser hardware, que son dispositivo con un IDS preinstalados y preconfigurados, o software que son ejecutados en el mismo equipo del usuario o en un equipo separado (servidor).
Hay varios tipos de IDS dependiendo de la funcionalidad:

- Sistemas de detección de intrusos de red (NIDS): Monitorizan los enlaces de red y conexiones centrales buscando firmas de atacantes.
- Sistemas detección de intrusión distribuidos (DIDS). Funciona como un grupo de sensores remotos y reportan a una estación central.
- Sistemas detección de intrusión de host (HIDS). Intenta detectar modificaciones en el equipo afectado.

El funcionamiento de un IDS dependerá de los datos que examina, un NIDS en red examina datos en red, pero en general la información que puede recoger se puede incluir en tres categorías.

- Información específica de una aplicación.
- Información específica del host.
- Información específica de red.

El IDS puede utilizar diferentes técnicas para recoger datos como un sniffer, analizar el registro del sistema o analizar llamadas al sistema.
Después de recoger los datos, usa varias técnicas para encontrar intrusiones o intentos de intrusión. Un IDS se puede ajustar a diversas políticas de seguridad para reconocer datos válidos y alertar en cualquier otro caso, también se puede configurar para políticas de datos inválidos, que son más simples, ya que no necesitan un modelo complejo de entradas permitidas, y alertan sólo sobre datos o tráfico que sabe que puede causar un problema. La mayoría de los motores de detección que utilizan los IDS suelen usar esta política.
Se pueden mezclar las políticas de datos válidas y no válidas en mismo IDS, usando la detección de firmas no válidas y la detección de anomalías de protocolos válidas para encontrar ataques.
Cuando un IDS detecta un intento de intrusión puede responder de dos formas.

Respuesta pasiva	El IDS genera alertas o registra las entradas, pero no interfiere en el tráfico de red.
Respuesta activa	El IDS puede enviar paquetes reset para interrumpir las conexiones TCP, cortar el tráfico si el IDS está en línea, añadir el host atacante a la lista de host bloqueados o intervenir activamente con el flujo de actividad dudosa.

Los IDS suelen trabajar con otro tipos de software como un cortafuegos, porque los IDS no tienen capacidad por sí mismos para bloquear una conexión. Cuando se detecta un intento de intrusión el IDS puede enviar una señal para que un cortafuego bloquee esa conexión.
Hemos visto que es un IDS, los tipos y cómo funciona, pero no se ha descrito por qué es necesario un IDS.
Un resumen de funcionalidades.

- Prevenir comportamientos problemáticos incrementando el riesgo percibido por los atacantes de ser descubiertos y castigados.
- Como control de calidad del diseño de seguridad y de la administración.
- Documentar las amenazas existentes para una organización.
- Detectar y manejar los pasos previos a ataques.
- Aumentar la información sobre las intrusiones que tengan lugar de cara a posibles medidas futuras.
- Permiten detectar los siguientes tipos de ataques:
    - Exploración de red o de un sistema (scanning).
    - Ataques de denegación de servicio.
    - Penetración en sistemas.

Una variante o evolución de los IDS son los IPS, Sistemas de Prevención de intrusos, un sistema que implementa una protección/prevención, y no solo genera alertas e informa. Un IPS protege de forma proactiva a un equipo, intenta proteger el equipo antes del intento de intrusión, para realizar esto implementa una políticas de seguridad para proteger el equipo de un posible ataque. Un IPS escanea todo el

tráfico independientemente del puerto y el protocolo para identificar y combatir tanto las amenazas existentes como las nuevas.

Los IPS se categorizan por la forma que detectan el tráfico malicioso:

- Detección basada en firma: genera una alarma cuando detecta un patrón conocido (firma), una base de datos almacena patrones reconocidos como ataques, deben actualizarse constantemente para que no pierdan eficacia.
- Detección basada en políticas: genera una serie de políticas de seguridad, si algún tráfico incumple la política se genera una alarma.
- Detección basada en anomalías: Este tipo de detección tiende a generar muchos falsos positivos, ya que es sumamente difícil determinar y medir una condición 'normal'. En este tipo de detección tenemos dos opciones:
    - Detección estadística de anormalidades: El IPS analiza el tráfico de red por un determinado periodo de tiempo y crea una línea base de comparación. Cuando el tráfico varía demasiado con respecto a la línea base de comportamiento, se genera una alarma.
    - Detección no estadística de anormalidades: En este tipo de detección, es el administrador quien define el patrón «normal» de tráfico. Sin embargo, debido a que con este enfoque no se realiza un análisis dinámico y real del uso de la red, es susceptible a generar muchos falsos positivos.

Un ejemplo de este tipo de software es Snort (GPL), un NIDS/IPS en red que contiene un sistema de firmas de ataque actualizable a través de diferentes boletines de seguridad, incluso se pueden añadir firmas por Internet. Está disponible para Windows y Linux.

Snort es un programa de línea de comandos, aunque hay múltiples interfaces web que facilitan su uso.

Cortafuegos

Otro aspecto que debemos controlar es los accesos no autorizados a la red, para realizar esta tarea tenemos los cortafuegos, que es un dispositivo software, hardware o una combinación de ambos, que permite controlar el acceso a un red, permite realizar **dos acciones** sobre un tráfico de una red que son **permitir** o **denegar** en función de ciertas reglas de configuración.

Un cortafuego es básicamente cualquier componente que restringe el flujo del tráfico de red. Hay diferentes tipos de cortafuegos en función de cómo realiza esa tarea. Una forma de realizarla es mediante filtrado de paquete, en el cual se decide si se acepta o deniega un flujo datos en función de una IP de origen o destino específico y un número de puerto. Este tipo de cortafuego tiene como desventaja que es relativamente fácil engañarlo.

Podemos tener un cortafuego correctamente para un servidor Web, que controla solo permite tráfico web por el puerto 80, pero es posible que el servidor Web no esté correctamente configurado permitiendo que un atacante externo acceda al sistema, el problema no es el tráfico sino la aplicación.

Para evitar lo anterior, tenemos los cortafuegos que funcionan a nivel de aplicación, no solo filtra por paquetes de red en base a unas reglas definidas, también entiende los datos que transporta cada paquete, puede volquear un flujo de datos en función de la información que contiene. Un inconveniente de este tipo de cortafuegos es lo complejo para programarlos, debe entender una cantidad alta de protocolo. Normalmente se da soporte a los protocolos más utilizados como HTTP, FTP o SMTP.

Los cortafuegos presentan una serie de limitaciones.

- Solo filtran el tráfico que pasa a través del cortafuego.
- No sirve para detectar virus.
- No protege del tráfico interno de red.
- No protege de los fallos de seguridad de los servicios y protocolos.

Un cortafuegos solo permite realizar dos acciones, aceptar o denegar. En función de esto, podemos tener dos políticas de seguridad:

- Restrictiva: Por defecto de bloquea todo el tráfico y después aceptar solo aquel tráfico que necesitemos.
- Permisiva: Por defecto se acepta todo el tráfico y después se bloquea el tráfico no deseado.

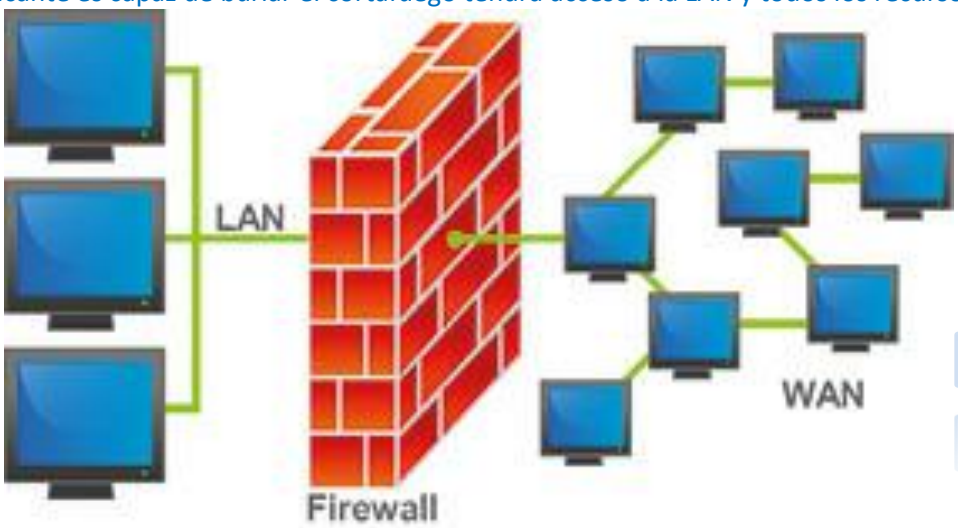
La política más segura es la restrictiva, la más aconsejable como política de seguridad, aunque puede ser más difícil de configurar. La política permisiva es muy fácil de configurar, pero es muy insegura, porque si

por defecto se acepta todo, después hay que tener mucho cuidado bloqueando todo el tráfico no deseado. Si por algún motivo no bloqueamos algún tipo de tráfico no deseado, tendrá acceso a la red porque la política por defecto.

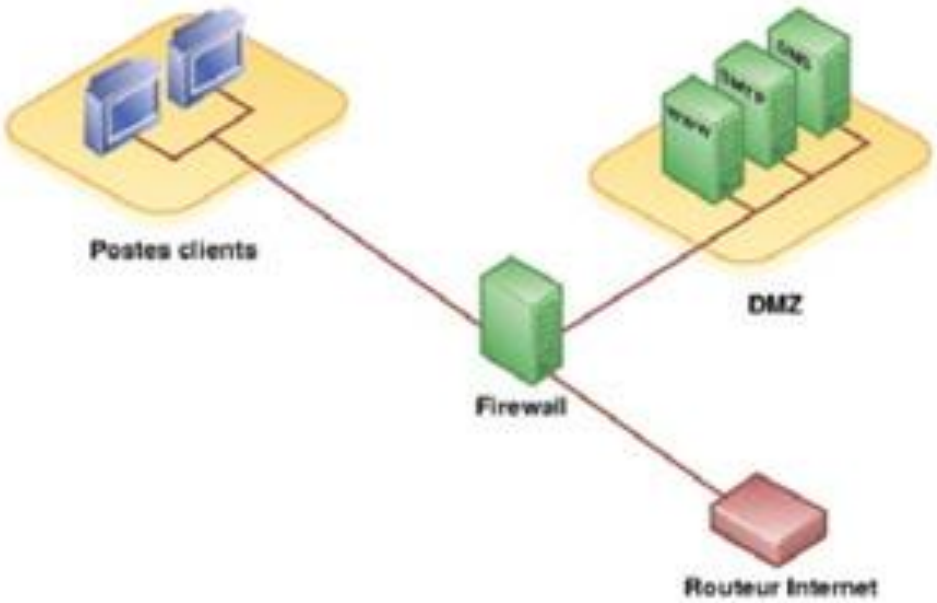
DMZ (Zona desmilitarizada) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

Otro punto muy importante de los cortafuegos que influirá en un funcionamiento optimo es un lugar donde los situamos, en función de donde se encuentre el cortafuego tenemos diversas categorías.

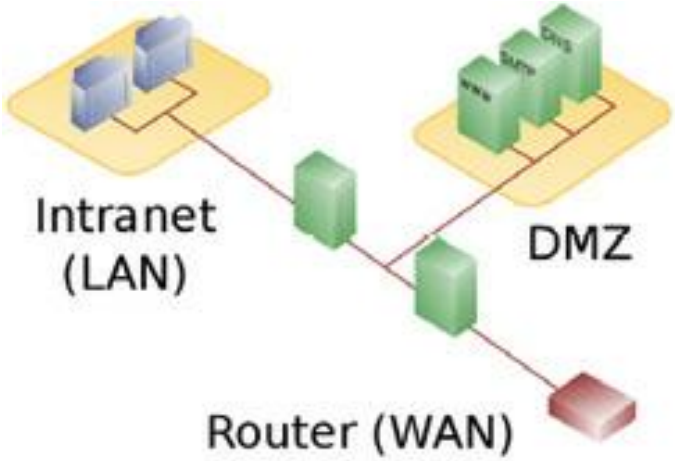
- **Cortafuegos lateral:** Se coloca entre dos redes, generalmente entre una red LAN e internet, el cortafuego se considera un dispositivo dentro de la LAN, dividendo todo en interno (LAN) y externo (Internet). Este tipo de configuración es muy simple, muy utilizada en redes pequeñas y redes domésticas, como desventajas dentro de la LAN no hay distinciones entre los equipos de los usuarios y los servidores. Un usuario puede acceder al servidor y el cortafuego no puede evitarlo. Si un atacante es capaz de burlar el cortafuego tendrá acceso a la LAN y todos los recursos de ella.



- **DMZ de una sola pata:** Se crea una separación en la red interna, una zona para los equipos de usuarios y otra zona donde se sitúan los servidores. El cortafuegos se sitúa entre las tres zonas: interna (equipos de usuarios), DMZ (servidores) y externa (red externa o Internet). Esta configuración añade una capa de aislamiento a los servidores. Los usuarios para acceder a internet a través del cortafuego, para acceder a los servicios que proporcionen los servidores deben atravesar el cortafuego. Este tipo de configuración proporciona el aislamiento que proporciona un DMZ a un coste bajo, como desventaja la configuración del cortafuego es más compleja que el primer caso y si el cortafuego cae toda la red estará expuesta.



- **DMZ Dual**: Se considera la configuración típica de DMZ y la más segura de las arquitecturas de cortafuegos. Hay dos cortafuegos, uno externo que se coloca entre la red externa y los servidores (DMZ) y otro interno entre los equipos de usuario y los servidores. Si un atacante tiene acceso a la zona DMZ no podrá acceder a la zona de los usuarios porque está protegido por otros cortafuegos. Podemos implementar diferentes tipos de cortafuegos y diferentes políticas de seguridad a cada cortafuego. Esta configuración es la más segura, si falla unos cortafuegos la red no queda expuesta, aunque es la costosa y más compleja de configurar.

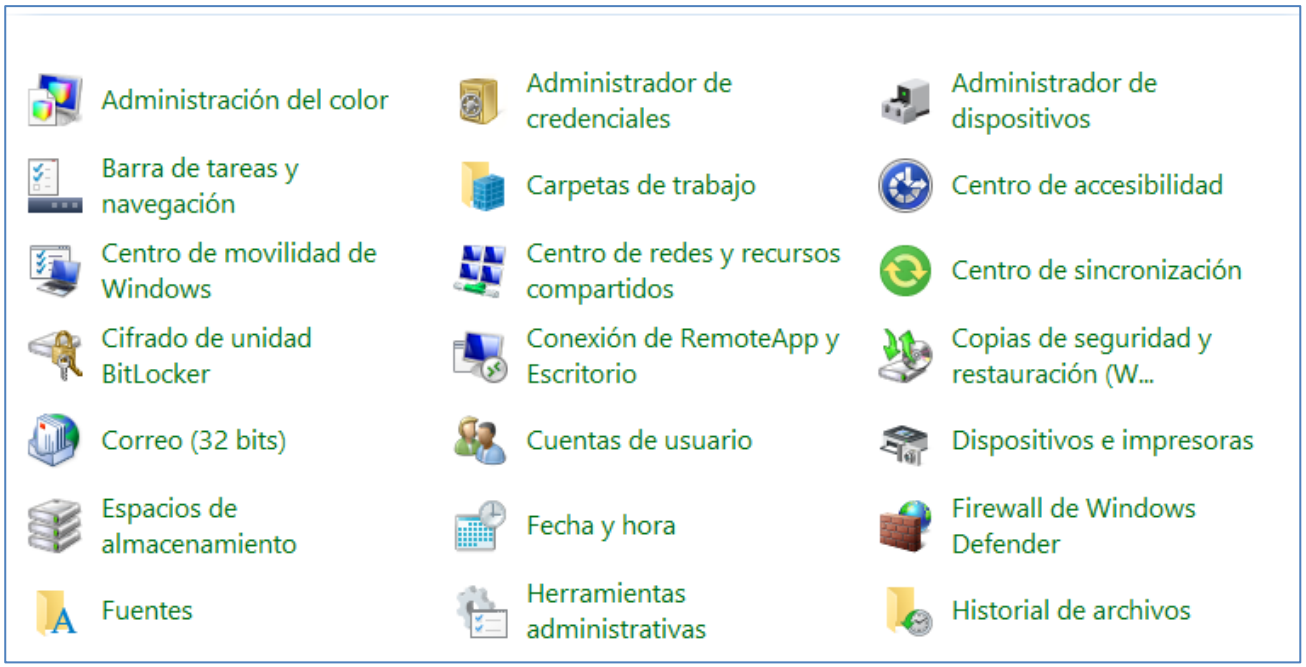


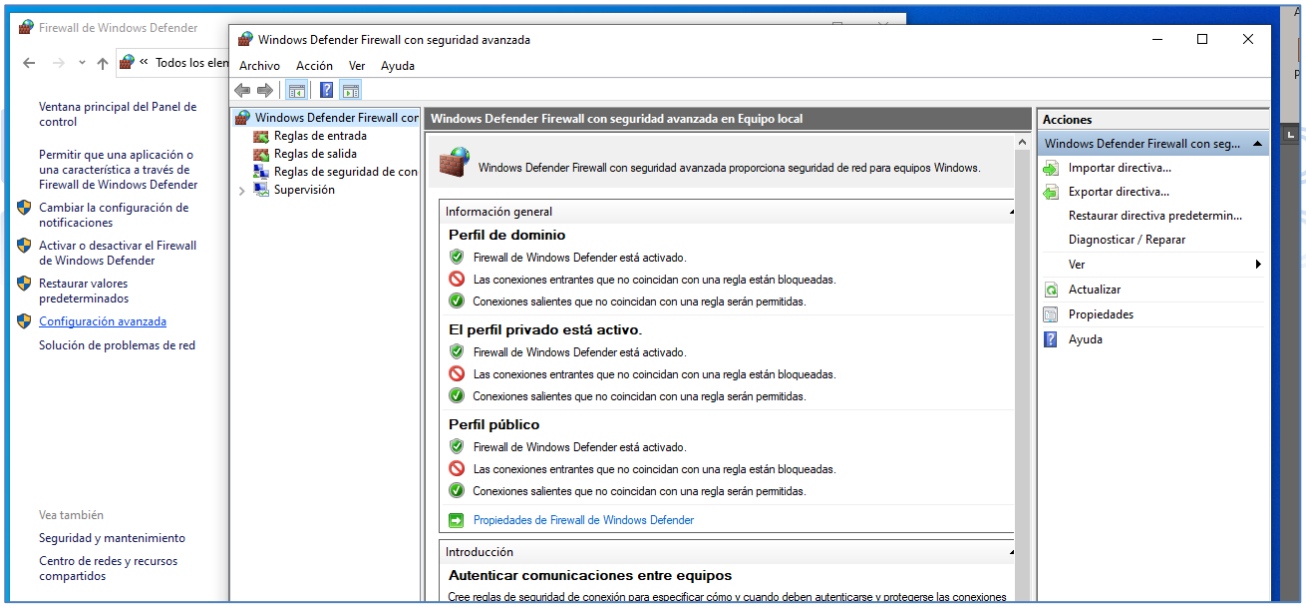
Los cortafuegos, al igual que los antivirus, se presentan en dos categorías en función del usuario a quien va dirigido.

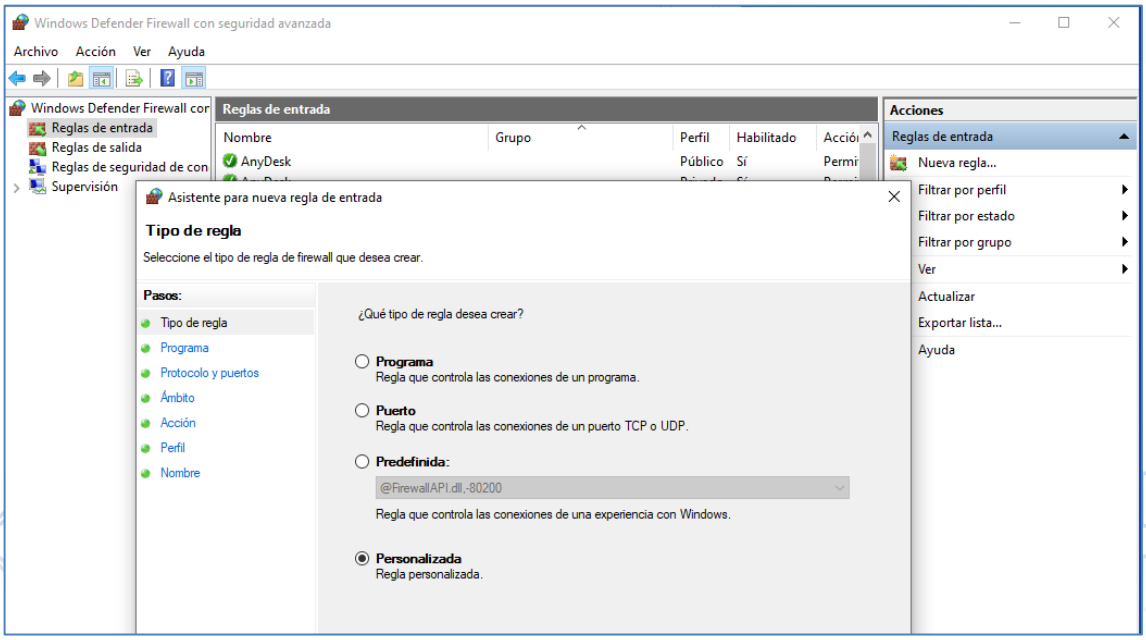
- Cortafuegos personal: se instala en el equipo del usuario, suele estar incluido en un paquete con más aplicaciones como antivirus, antispam, control parental; solo protege al equipo donde está instalado. Es una solución enfocada a uso doméstico, muchos antivirus ofrecen productos que incluyen un cortafuegos. También los sistemas operativos incluyen un cortafuego dentro de sus herramientas.
- Cortafuegos corporativos: se encargan de proteger una red, se instalan entre las redes para controlar el acceso de una red. También pueden venir acompañado de otro tipo de software como un IDS y suelen incluyen interfaz de administración web para su configuración. Podemos distinguir dos categorías.
    - Software: distribución de Linux enfocada a ser utilizada como cortafuegos, utilizando Netfilter/iptables. Podemos construir un cortafuego corporativo en Linux, con una distribución específica y un hardware no muy potente. Esta opción tiene un coste pequeño y no tiene nada que envidiar en potencia a otras soluciones. Como desventaja, es una solución que hay que montarla y requiere ciertos conocimientos técnicos. Como ejemplos de distribuciones para cortafuegos tenemos, IPCop, SmoothWall o Endian Firewall.
    - Hardware: implementan un cortafuegos en un hardware específico, con una interfaz web para la administración y suelen incluir varios puertos red para la conexión. Son más caros pero proporcionan un seguridad mayor debido a la su integración. Empresas que proporcionan cortafuegos hardware son Cisco, Fortinet o SonicWALL.

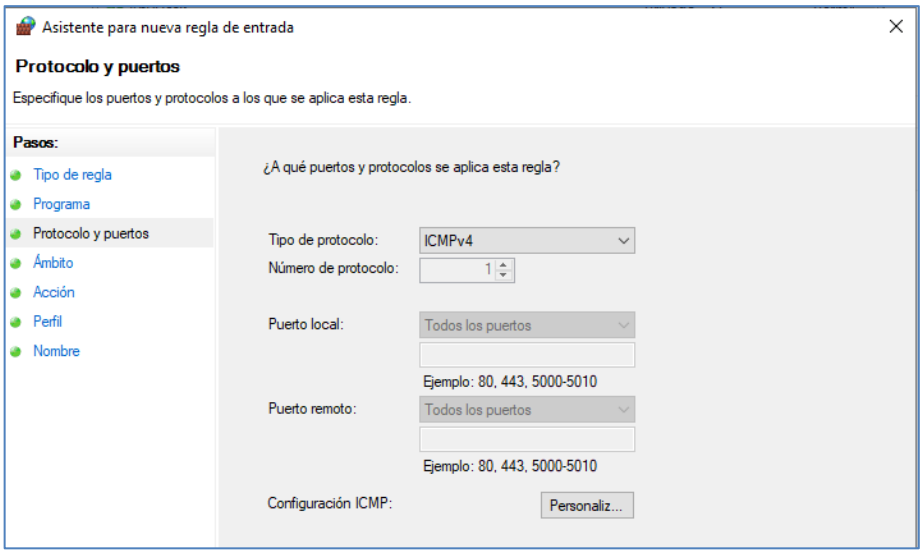
Ejemplo, configuración firewall para evitar responder a los **ping**:

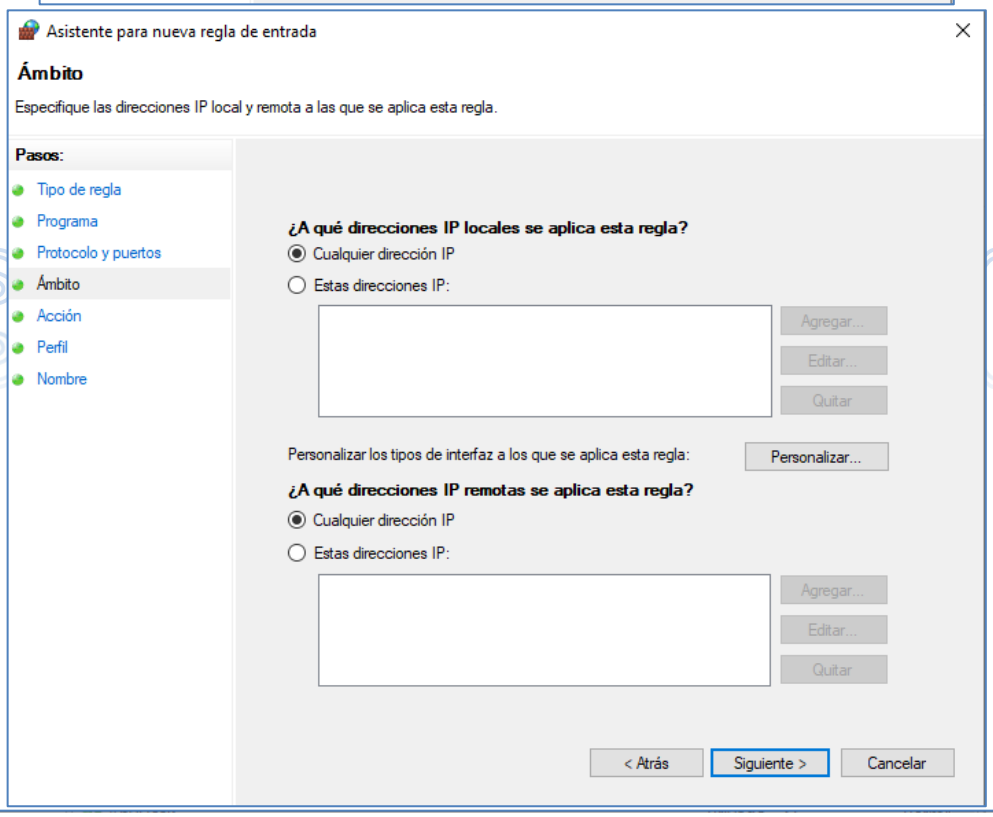
1. Panel de Control/Firewall de Windows.
2. Configuración avanzada en el menú vertical que está disponible en la parte izquierda.
3. Pulsa con el botón derecho el campo llamado Reglas de entrada y selecciona Nueva regla.
4. Personalizada -> siguiente -> Todos los programas -> siguiente.
5. Tipo de protocolo: ICMPv4. (Internet Control Message Protocol)
6. Cualquier dirección IP -> siguiente.
7. Bloquear la conexión -> siguiente.
8. Selecciona las tres casillas de selección que aparecen y pulsa siguiente.
9. Ponle un nombre descriptivo que te ayude a identificar la regla creada, por ejemplo, **Ping**.
10. Reiniciamos y ya estaría activa la regla.

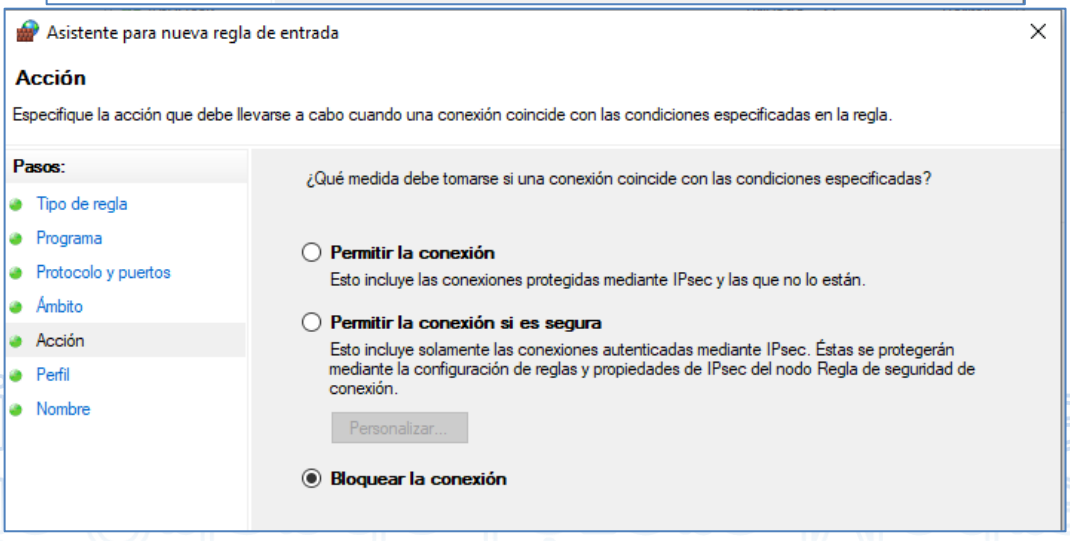


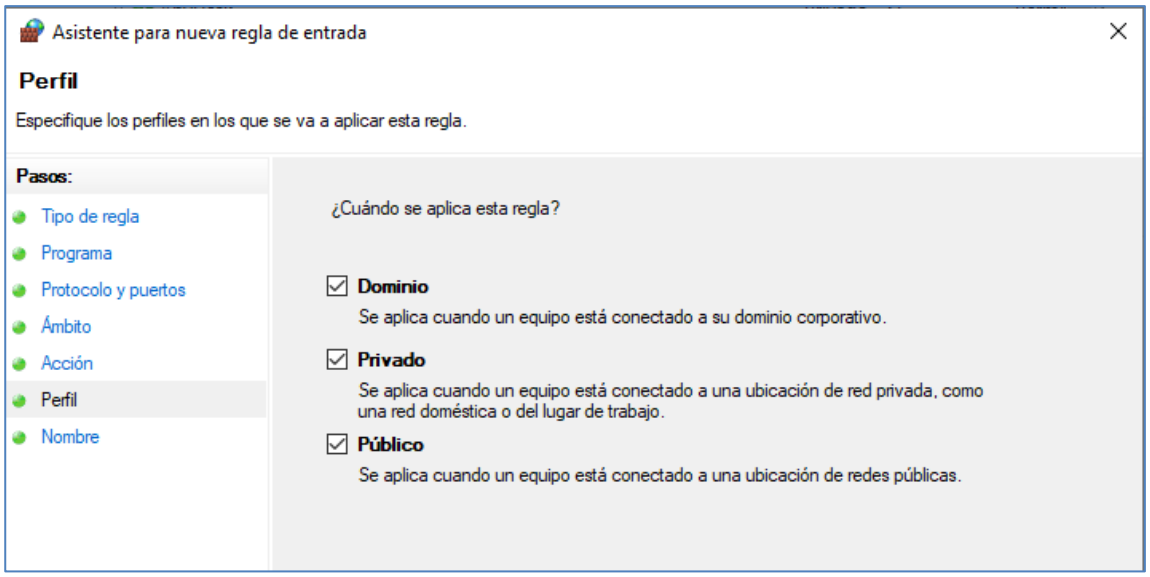


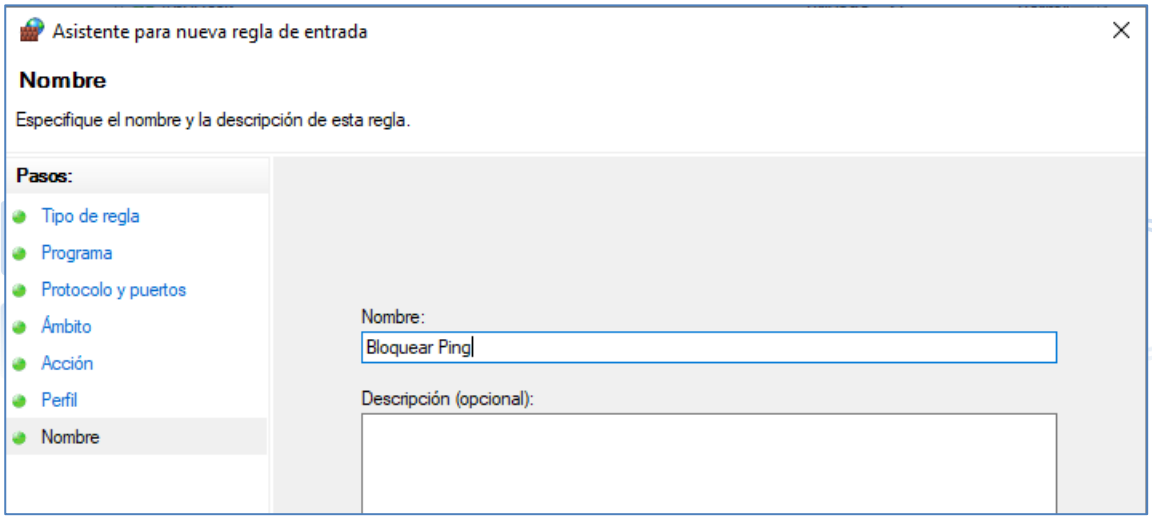


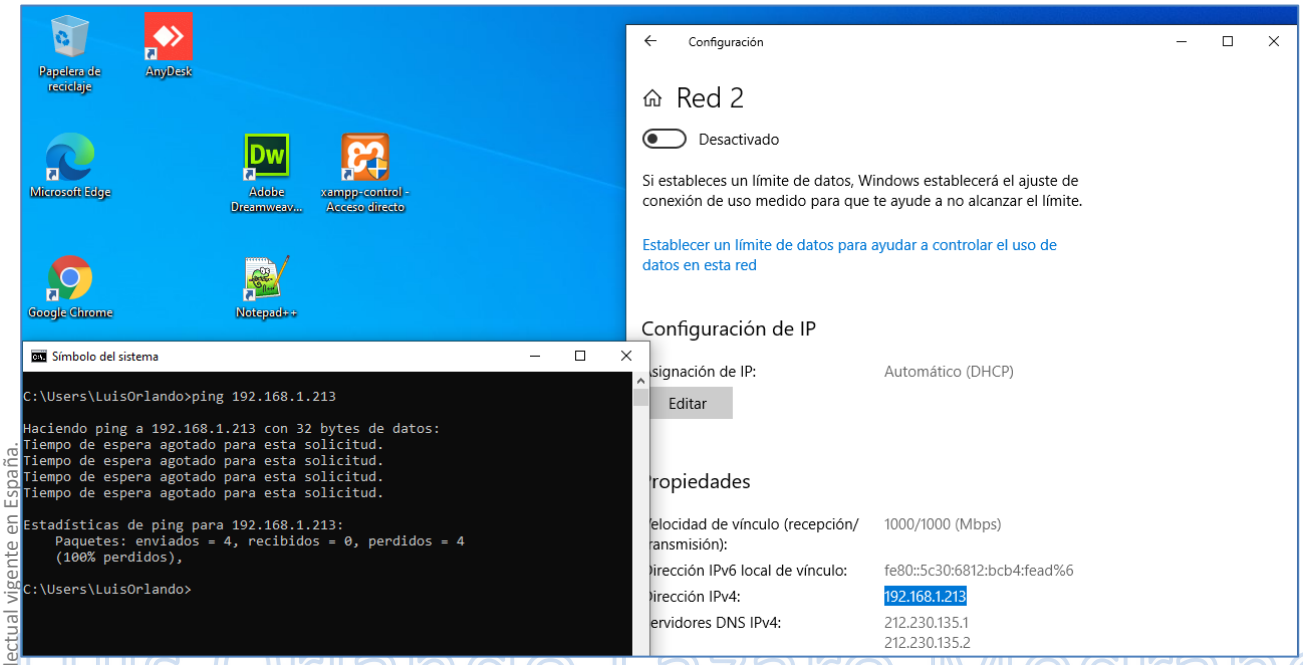


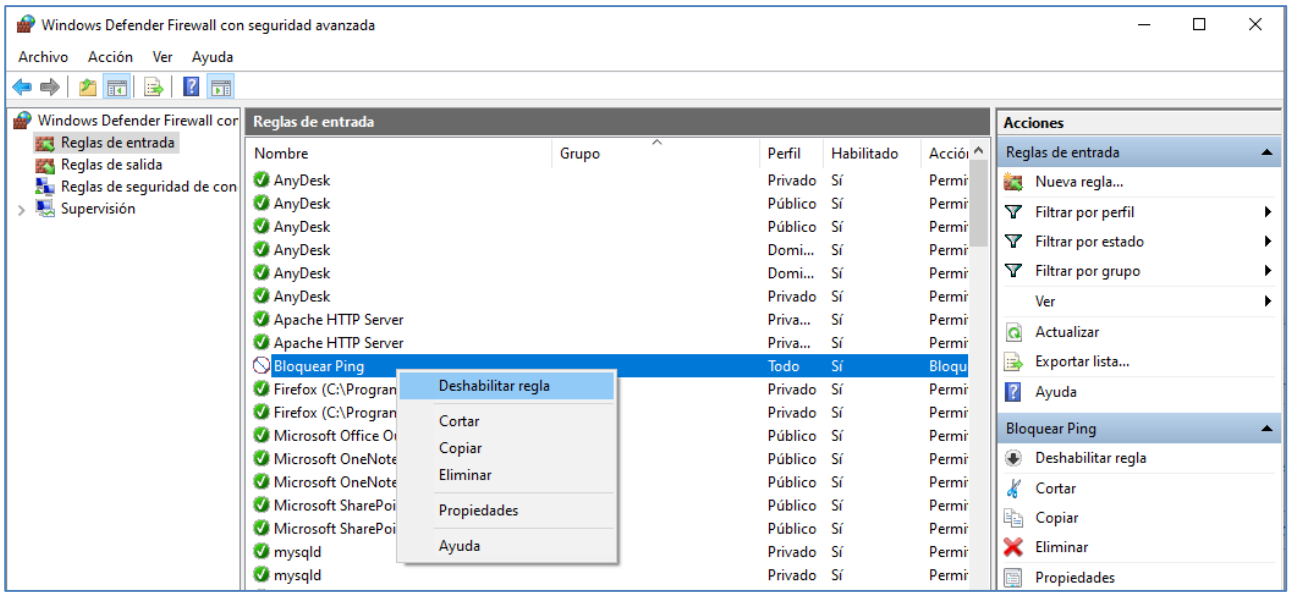












UTM (Gestión unificada de amenazas)

Una evolución a los cortafuegos son los sistemas UTM (Gestión unificada de amenazas): es un cortafuegos de red que engloba múltiples funcionalidades en una máquina. Algunas de las funcionalidades que puede incluir son:

- VPN.
- Antivirus.
- IDS/IPS.
- Anti-spam.
- Filtro de contenido.
- Antiphising.

Se trata de cortafuegos a nivel de capa de aplicación que pueden trabajar de dos modos:

- Modo proxy: hacen uso de proxies para procesar y redirigir todo el tráfico interno.
- Modo Transparente: no redirigen ningún paquete que pase por la línea, simplemente lo procesan y son capaces de analizar en tiempo real los paquetes. Este modo, como es de suponer, requiere de unas altas prestaciones de hardware.

Para explicar el funcionamiento de un cortafuego, como ejemplo veremos cómo funciona iptables, que su funcionamiento es similar a cualquier cortafuego.

La configuración de iptables se realiza mediante una serie de reglas, cada regla especifica una acción a realizar a un tráfico de datos. Las acciones básicas en iptables son permitir o denegar.

Las reglas se almacenan en una serie de tablas en función de qué tipo de flujo de datos se aplican. En iptables las tablas que utilizan son.

- Filter: esta tabla almacena regla de filtrado de paquetes, en cada regla se especifica una cadena entre tres opciones.
  - INPUT: reglas que se aplican para tráfico entrante.
  - OUTPUT: reglas para tráfico saliente.
  - FORWARD: reglas para tráfico que son redirigidos o encaminados.

  Esta es la tabla donde se almacenarán la mayoría de nuestras reglas, pero hay más tablas en iptables, como:
- NAT: almacena las reglas de reescritura de direcciones.
  - PREROUTING: se aplica al tráfico entrante antes de realizar NAT.
  - POSTROUTING: se aplica al tráfico saliente después de realizar NAT.
  - OUTPUT: permite realizar DNAT.
- Mangle: esta tabla se utiliza para ajustar opciones de los paquetes, es para un uso avanzado. Las cadenas que se definen son.

- PREROUTING: Todos los paquetes que logran entrar a este sistema, antes de que el ruteo decida si el paquete debe ser reenviado o si tiene destino local.
- INPUT: Todos los paquetes destinados para este sistema pasan a través de esta cadena.
- FORWARD: Todos los paquetes que exactamente pasan por este sistema pasan a través de esta cadena.
- OUTPUT: Todos los paquetes creados en este sistema pasan a través de esta cadena.
- POSTROUTING: Todos los paquetes que abandonan este sistema pasan a través de esta cadena.

Estas son las tablas donde se almacenarán las reglas en función de la cadena que especifiquemos.
Los primero que debemos realizar para configurar una cortafuegos, es crear las políticas por defecto. Esta políticas se aplican cuando un flujo de datos no tiene un regla asignada en el cortafuegos, entonces el cortafuegos al no encontrar una regla que le indique como actuar, se aplicará la política por defecto. Esta política solo tiene dos acciones por defecto permitir o denegar.
En iptables para crear la política por defecto, escoger la acción y donde se aplica, por ejemplo.

Iptables –P INPUT DROP

Esta política se aplica al tráfico entrante y la acción a realizar es denegar (DROP).
Para crear una regla vemos un ejemplo de una regla para iptables.

Iptables -A INPUT -p tcp --dport 80 -j ACCEPT

Esta regla permite todo el tráfico que entrante, no importa el origen, al puerto de sitio 80.
El comando iptables permite crear reglas, la opción –A indica que se añade, lo siguiente se especifica la cadena, que es trafico entrante (INPUT), se puede especificar un origen y un destino, como esta en blanco se considera cualquier origen y destino. Por último, se especifica que solo se filtre el tráfico destinado por el puerto 80 TCP (-p tcp –dport 80) y la acción que realiza que es permitir ese tráfico.
Netfilter/Iptables es un cortafuegos que funciona a nivel red, permite filtrar paquetes de red mediante un IP y un puerto de destino u origen, no examina los datos del tráfico.

Copia de Seguridad

Cuando surge un error en la red puede provocar una pérdida de datos y si no se realiza una copia previa, esos datos no se pueden recuperar. Si esos datos son importantes, su pérdida puede tener efectos muy negativos, para evitar este tipo de errores es conveniente tener una política de copia de seguridad.
Una copia de seguridad o backup es un conjunto de datos originales que son almacenados en algún medio de almacenamiento. Estos datos almacenados serán recuperados en caso de pérdida de los datos originales, al proceso de recuperar los datos de una copia de seguridad se denomina restauración.
Las copias de seguridad se pueden almacenar en diferentes dispositivos de almacenamiento, entre los que tenemos:

- Cinta: dispositivo de acceso secuencial, es barato pero su acceso es lento.
- Sistemas de copia de seguridad RDX: discos duros extraíbles, tienen todas las ventajas de los discos duros pero son más manejables, por contra tienen un elevado precio.
- CD/DVD/Blu-ray: sobre todo en formatos regrabables puedes ser una opción muy interesante puesto que permiten reutilizar los discos, son baratos y su capacidad es limitada.
- Discos duros: el formato más utilizado, en combinación con RAID es un formato bastante fiable.
- Copia en la nube: una opción a tener en cuenta en algunos ámbitos, su precio cada vez en más bajo. El problema es la velocidad de subida que en copias de gran tamaño puede resultar muy lento.

Una política de copias de seguridad, son los diferentes métodos, incluyendo la forma en que se realiza y el tipo de copia, que se utilizan para realizar las copias de seguridad.
Para crear una política de seguridad debemos tener en cuenta los siguientes aspectos.

- Calendario: Escoger el día y la hora para realizar la copia. Hay que tener en cuenta que el proceso de realizar una copia de seguridad puede influir de manera negativa en la red. Es aconsejable que las copias se realicen cuando la red tenga poca carga de trabajo, por ejemplo de madrugada, para que afecte lo menos posible al rendimiento de la red.
- Datos: Pensar a que equipos se le va a realizar una copia, y dentro de los equipo cuales serán los datos (archivos y directorios).

- Lugar de almacenamiento: Dependiendo de los datos escogidos para la copia, la copias de seguridad pueden ser muy grandes, debemos escoger un lugar de almacenamiento y en que medio, en función del tamaño.

Las copias que se generen no se deben almacenar en un equipo de un usuario, se deben almacenar en un equipo que solo sirva de almacenamiento, aunque es muy recomendable almacenar copias fuera de la red para evitar que un fallo en red afecte a las copias.

Para crear una política de seguridad debemos escoger que tipo de copias. Hay varios tipos de copia de seguridad.

- Copia de Seguridad Total: Es una copia de todos los archivos seleccionados. A cada archivo se le pone una marca que indica que se ha realizado una copia de seguridad del mismo.
- Copia de Seguridad Incremental: Se copian todos los archivos creados o modificados desde la última copia de seguridad, sea total o incremental. Marca los archivos como copiados.
- Copia de Seguridad Diferencial: Solo copia los archivos creados o modificados desde la ultima copia de seguridad total. No marca los archivos como copiados

Utilizando la combinación de algunos de estos tipos de copias, podemos obtener conjunto de Copias que ahorran tiempo y espacio, pero esto no siempre es beneficioso. Por ejemplo, una copia de seguridad combinando copias totales e incrementales, utilizan el mínimo espacio de almacenamiento y es rápida, pero la restauración puede ser difícil y laborioso, si las copias de seguridad se encuentran en varios medios.

Si la copia de tus datos ha empleado una combinación de copias de seguridad totales y diferenciales consumirá más tiempo, especialmente si los datos sufren cambios frecuentes, aunque será más fácil de restaurar los datos.

Dependiendo de los tipos de copias realizadas la restauración será diferente. Si las copias que se han realizado son una copia total y varias incrementales, el proceso de restauración implica la copia total y todas las incrementales. Si se realiza una copia total y varias diferenciales, el proceso de restauración implica la copia total y la última copia diferencial.

Para optimizar tanto el proceso de copia como de almacenamiento podemos manipular los datos de las siguientes.

- Compresión: Se permite disminuir el espacio de almacenamiento necesario.
- Cifrado: Si el medio de almacenamiento es robado o se pierde. Si los datos son cifrados, estos datos no serán legibles para una tercera persona. Como inconvenientes del cifrado, es el consumo de recursos y la pérdida de eficacia de la compresión.
- Redundancia: copias duplicadas en la red. El sistema de almacenamiento solo debe disponer una sola copia de seguridad.
- Des-duplicación: Algunas veces las copias de seguridad están duplicadas en un segundo soporte de almacenamiento. Esto puede hacerse para cambiar de lugar imágenes, para optimizar velocidades de restauración, o incluso para disponer de una segunda copia a salvo en un lugar diferente o en soportes de almacenamiento diferentes.

Para realizar copias de seguridad se realiza herramientas software o una combinación de hardware y software, también tenemos herramientas para usuarios que nos permite realiza copias del equipo del usuario, son herramientas que son fáciles de utilizar y su funcionamiento es sencillo pudiendo programar copias seguridad de diferentes tipos de forma rápida, como ejemplo de este tipo de software tenemos Dejá Dup o Cobian Backup.

Las soluciones de copias de seguridad para ambientes corporativos son herramientas para realizar copias de seguridad en red, nos permite realizar copias de seguridad de equipos en una red. Son herramientas soluciones software que incluyen muchas opciones, como diferentes protocolos de comunicación y otro tipo de características. Ejemplos de este de herramientas son Amanda o BackupPC.

Las soluciones hardware incluyen un conjunto componentes para realizar copias de seguridad, muchos de esos componentes son medios de almacenamiento, como varias bahías para introducir discos duros o unidades de cintas y diferentes conexiones.

Algunas soluciones software son distribuciones de Linux personalizadas para tareas de backup que son administradas mediante una interfaz web. Como ejemplo tenemos FreeNAS u OpenMediaVault.

SAI

Todos los dispositivos de una red están alimentados por una corriente eléctrica, un fallo en el suministro eléctrico provocará un apagado de todos los dispositivos, si algún dispositivo estaba ejecutando una aplicación y se produce un corte de suministro de corriente eléctrica, la ejecución se cortará y todo el trabajo realizado puede perderse, incluso puede provocar un fallo en la aplicación de forma permanente.
Hay que controlar los diversos problemas con el suministro eléctrico en la red.
Para evitar los posibles daños de los cortes en el suministro eléctrico tenemos un dispositivo hardware denominado SAI (Sistemas de Alimentación Ininterrumpida).
Un SAI es un dispositivo hardware compuesto por unas baterías que proporcionan suministro eléctrico por un periodo limitado, que se denomina autonomía y también incluyen otro tipo de conexiones. El funcionamiento es el siguiente, se conecta el SAI al suministro eléctrico y se conectan los equipos al SAI, depende del número de conexiones se podrán conectar uno o varios dispositivos, cuando se produce un corte en el suministro, el SAI proporciona suministro eléctrico de sus baterías a los equipos conectados. Dependiendo de la autonomía, tendremos un tiempo para cerrar las aplicaciones y realizar el apagado del equipo correctamente.
Algunos modelos de SAI proporcionan diferentes conexiones, aparte de las conexiones eléctricas para los equipos, como USB, entrada de red o conexiones RJ11 para proteger dispositivos telefónicos. Los SAI pueden proporcionar un software para su gestión a través de la red.
Los SAI protegen de diferentes fallos de suministro:

- Corte suministro eléctrico.
- Sobretensión.
- Bajada de tensión.
- Pico de tensión.
- Ruido eléctrico.

Hay tres tipos de SAI según el modo de funcionamiento.

Off-Line	La carga está alimentada directamente por la red eléctrica a través de unos filtros contra picos de tensión, en el momento que surge un problema eléctrico las baterías proporcionan el suministro.
On-line	Toman la corriente alterna de la red eléctrica, la convierten a corriente directa la cual carga las baterías. La corriente directa se convierte entonces en alterna a través de un inversor, y se lleva entonces a los aparatos conectados. Debido a que el inversor está siempre conectado a la salida de corriente del SAI. Esta corriente es limpia y con unos niveles perfectamente regulados.
Interactivo	La carga está alimentada por la red eléctrica. La diferencia es que existe un elemento acondicionador, que permite una mayor calidad de la tensión de salida en lo que respecta a la tensión. Este sistema permite regular la tensión de salida, de modo que tenga un valor constante, con lo que la tolerancia de la tensión entrada podría ser mayor, para una misma tolerancia de tensión de salida.

Auditoría de Seguridad

Uno de los aspectos más importantes de una red y que conviene controlar es la seguridad. Aunque se aplican políticas de seguridad, es conveniente realizar un estudio más detallado de la seguridad.
Una auditoría de seguridad consiste en un examen profundo y detallado que se realiza para validar las medidas de seguridad implementadas, para identificar diversas vulnerabilidades de los componentes de la red. Posteriormente se presenta un informe detallado con el resultado y otro informe con las medidas preventivas o de corrección para solucionar las vulnerabilidades encontradas.
Las auditorias se realizan por empresas externas y con personal especializado, para realizar una auditoría se revisan los siguientes aspectos.

- Gestión de los sistemas instalados.
- Análisis de los sistemas operativos y aplicaciones instaladas.
- Análisis del hardware.
- Análisis de seguridad de los equipos.
- Análisis de la red.
- Vulnerabilidades que se presentan en equipos, sistemas, operativos, aplicaciones, servidores, conexiones de red, etc.
- Revisión de equipos, servidores, aplicaciones y sistemas operativos.

Las auditorias de seguridad pueden estar orientadas a ciertos, los diferentes tipos que podemos encontrar.

Tipo	Descripción
Seguridad interna	Contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno.
Seguridad perimetral	Revisa la red perimetral de red local, comprobando la seguridad de los accesos externos.
Test de intrusión	Revisa la seguridad realizando intento de acceso al sistema mediante diferentes técnicas, comprobando la resistencia a los ataques externos o internos.
Análisis forense	Estudio y análisis de un incidente, para conocer como ha realizado la intrusión al sistema.
Página web	Análisis de una página, realizando diferentes técnicas de ataque y ver cómo responde.
Código de aplicaciones	Análisis del código de una aplicación, independiente del lenguaje utilizado.

Para realizar una auditoría de seguridad se siguen una serie de normas, existen una serie de estándar que sirven para realizar una auditoría de forma más eficiente, están normas son:

- COBIT.
- ISO 27002.
- ISO 27001.

Por último para realiza una auditoría de seguridad se utiliza n una serie de herramientas que realizan las pruebas. Hay software específico, que son distribuciones de Linux que contiene un conjunto de herramientas de seguridad como BackTrack o WifiSlax.

Documentación

Toda red necesita una documentación para conocer todos los detalles de la red y otras especificaciones, aunque cada administrador decidirá que documentación es necesaria para la red. Entre los documentos que se puede crear tenemos.

- Mapa de red: Representación que describe la topología de la red, incluye todos los elementos de la red, incluyendo las conexiones internas y externas. Se puede crear un mapa lógico donde se indica la funcionalidad de cada elemento, o un mapa físico donde se especifican sobre todo las especificaciones del cableado.
- Mapa de nodos: Descripción del hardware y software que se instala en cada nodo, también se detalla los parámetros de configuración, direcciones de red, marca y modelo, etc.
- Mapa de protocolos: Descripción de la organización lógica de la red, donde de describen los protocolos utilizados, configuración de router, grupos de trabajo o creación de dominios.
- Mapa de grupos y usuarios. Describe los grupos y usuario que pertenecen a la red, así como los permisos de acceso a los diferentes recursos de la red.
- Mapa de recursos y servicios: Muestras todos los recursos disponibles y servicios que proporcionan, el lugar donde se encuentran, los usuarios o grupos que tienen permiso de acceso, etc.
- Calendario de averías: Un registro de averías de la red, tanto software como hardware, describiendo el componente averiado, la causa y la solución. Esto nos permitirá realizar un análisis de donde es más probable que falle la red.
- Informe de costes: Describe los costes económico que provocado el mantenimiento de la red y de las inversiones realizadas.
- Plan de contingencias. Contiene medidas técnicas, humanas y organizativas necesarias para garantizar el funcionamiento de la red. Este plan se aplica cuando surgen diversas amenazas graves en la red. El objetivo de este plan es garantiza en la medida de lo posible el funcionamiento de la red.

Esta documentación nos permitirá conocer diferentes aspectos de la red y en caso de desastre en la red poder dar una respuesta optima.

El proceso de mantenimiento

- El objetivo de los usuarios de un sistema es, obviamente, mantener dicho sistema en Estado de Funcionamiento tanto tiempo como sea posible. Por lo tanto hay que «ayudar» al sistema a mantener dicha funcionalidad realizando las acciones apropiadas para tal fin.
- Esta es una de las diferencias principales entre un elemento creado por la naturaleza, que normalmente es capaz de «ayudarse» a sí mismo y un elemento creado por el hombre, que necesita ayuda «externa». Estas tareas, para dar soporte, son impuestas o propuestas por los propios diseñadores o fabricantes.
- Hay que tomar las decisiones necesarias de forma que el sistema no deje de funcionar.
- Ahora bien, si esto ocurriera hay que realizar todas las acciones que sean necesarias para conseguir recuperar su funcionalidad.
- Estamos hablando del concepto de mantenimiento, que incluye todas las tareas o acciones que realiza el usuario para conservar el elemento o sistema en el Estado de Funcionamiento, o para recuperarlo a ese estado.
- Podemos considerar que todos los sistemas creados por el hombre necesitan conservar su funcionalidad, esto lo realizará el usuario a lo largo de su utilización.
- El proceso por el que se mantiene la capacidad del sistema para realizar una función determinada, se denomina proceso de mantenimiento, y se define como: el conjunto de tareas realizadas por el usuario para mantener la funcionabilidad del sistema durante su vida operativa.
- Es imprescindible la acción humana en cualquier proceso de mantenimiento, que deberá ser realizada por el usuario con el objetivo de conseguir al final del proceso un sistema que funcione correctamente.

Vamos a enumerar los OBJETIVOS de las tareas realizadas durante un proceso de mantenimiento:

1. Reducción del cambio de condición, con lo que se consigue un alargamiento de la vida operativa del sistema.
2. Garantizar la fiabilidad y seguridad exigidas, esto reduce la probabilidad de que aparezcan fallos. Las actividades más comunes de este tipo son: inspección, detección, exámenes, pruebas.
3. Conseguir una tasa óptima de consumo de elementos tales como combustible, lubricantes, neumáticos, etc., lo que contribuye al a un equilibrio en coste - eficacia del proceso.
4. Recuperación o vuelta al estado de funcionamiento del sistema, una vez que se ha llegado al Estado de Fallo.

Las actividades más frecuentemente realizadas para volver a un sistema a su estado de funcionamiento normal son: sustitución, reparación, restauración, renovación, etc.

Haremos hincapié en el hecho de que se necesitan ciertos recursos para facilitar este proceso de mantenimiento. Como el objetivo principal de estos recursos es facilitar y llevar a buen fin el proceso de mantenimiento, se les designará con el nombre de recursos de mantenimiento (Maintenance Resources, MR).

Los RECURSOS necesarios para la realización, con éxito, de una tarea de mantenimiento pueden clasificarse en los siguientes grupos:

A. Abastecimiento o aprovisionamiento. Con este nombre genérico nos referimos al suministro de todos los repuestos, elementos de reparación, consumibles, suministros especiales y artículos de inventario necesarios para apoyar y realizar los procesos de mantenimiento.
B. Personal. Incluiremos el personal necesario para la instalación, comprobación, manejo y realización del mantenimiento del elemento o sistema y de todos los equipos necesarios de prueba y apoyo. Deberá tenerse en cuenta la formación específica del personal necesario para cada una de las tareas de mantenimiento.
C. Datos técnicos. Procedimientos de comprobación, instrucciones de mantenimiento de equipos, procedimientos de inspección y calibración, procedimientos de revisiones generales, instrucciones de modificación, información sobre las instalaciones, planos y especificaciones técnicas que son necesarios para realizar las funciones de mantenimiento del sistema.

Los procesos de mantenimiento, también tienen sus propias restricciones, como todas los demás procesos. Las más frecuentes son las siguientes:

1. Presupuesto
2. Tiempo disponible, Programación
3. Reglas de seguridad
4. Entorno y clima
5. Cultura y costumbres tradicionales

Cuando se analiza un proceso de mantenimiento hay que considerar tanto los recursos como las restricciones, para conseguir un control óptimo de unas operaciones tan complejas. Tienen una gran influencia en la seguridad, fiabilidad, coste, prestigio y otras características imprescindibles en el funcionamiento correcto de las operaciones a fin de que estas sean competitivas.

La TAREA de mantenimiento

- Es el conjunto de actividades que debe realizar un usuario para garantizar asegurar la labor de mantenimiento de un vehículo, de una parte del elemento o sistema.
- Por lo tanto diremos que, la entrada para el proceso de mantenimiento está representada por la necesidad de ejecución de una tarea específica con el propósito de que el usuario conserve la funcionabilidad del elemento o sistema, mientras que la salida es la realización de la tarea de mantenimiento propiamente dicha.
- Hay que tener en cuenta que cada tarea específica requiere recursos específicos para su finalización, llamados recursos para la tarea de mantenimiento.
- También es importante recordar que cada tarea se realiza en un entorno específico, por ejemplo a bordo de un barco, bajo lluvia o nieve, en condiciones de guerra, radiación solar, humedad, temperatura y situaciones similares o adversas, que pueden tener una influencia decisiva en la seguridad, precisión y facilidad para terminar la tarea.

Mantenimiento correctivo.

Las tareas de mantenimiento correctivo (Corrective Tasks, CRT) son las se realizan con la intención de recuperar el funcionamiento del elemento o sistema, una vez que ha perdido su capacidad para realizar la función para la que estaba destinado.

Normalmente una tarea de mantenimiento correctivo consta de las siguientes actividades:

⇨ Detección del fallo.
⇨ Localización del fallo.
⇨ Desmontaje del sistema, elemento o aparato.
⇨ Recuperación después del fallo o sustitución del elemento fallido.
⇨ Montaje de los elementos o piezas.
⇨ Pruebas de funcionamiento.
⇨ Verificación.

Mantenimiento preventivo

El mantenimiento preventivo (Preventive Task, PRT) es una tarea que se realiza para reducir la probabilidad de fallo del elemento o sistema, o para maximizar la operatividad de dicho elemento. Una tarea de mantenimiento preventivo típica consta de las siguientes actividades de mantenimiento:

- ⇨ Desmontaje del aparato o elemento en cuestión.
- ⇨ Recuperación de los elementos o sustitución en caso necesario.
- ⇨ Montaje correcto del elemento o sistema.
- ⇨ Pruebas de funcionamiento.
- ⇨ Verificación final.

La duración de la tarea se representa por DMTp, que representa el tiempo necesario para la finalización con éxito de la tarea de mantenimiento preventivo.

Las tareas de mantenimiento de este tipo se realizan antes de que tenga lugar la transición al Estado de Fallo, con el objetivo principal de reducir costes: los más comunes son sustituciones, renovaciones, revisiones generales, etc.

Mantenimiento autónomo

Es el mantenimiento realizado por el servicio de producción de la maquinaria (generalmente, el mismo operario de la máquina).

El servicio de producción es responsable de la prevención del deterioro en la máquina, detectar y medir el deterioro una vez que se ha producido y restaurar dicho deterioro.

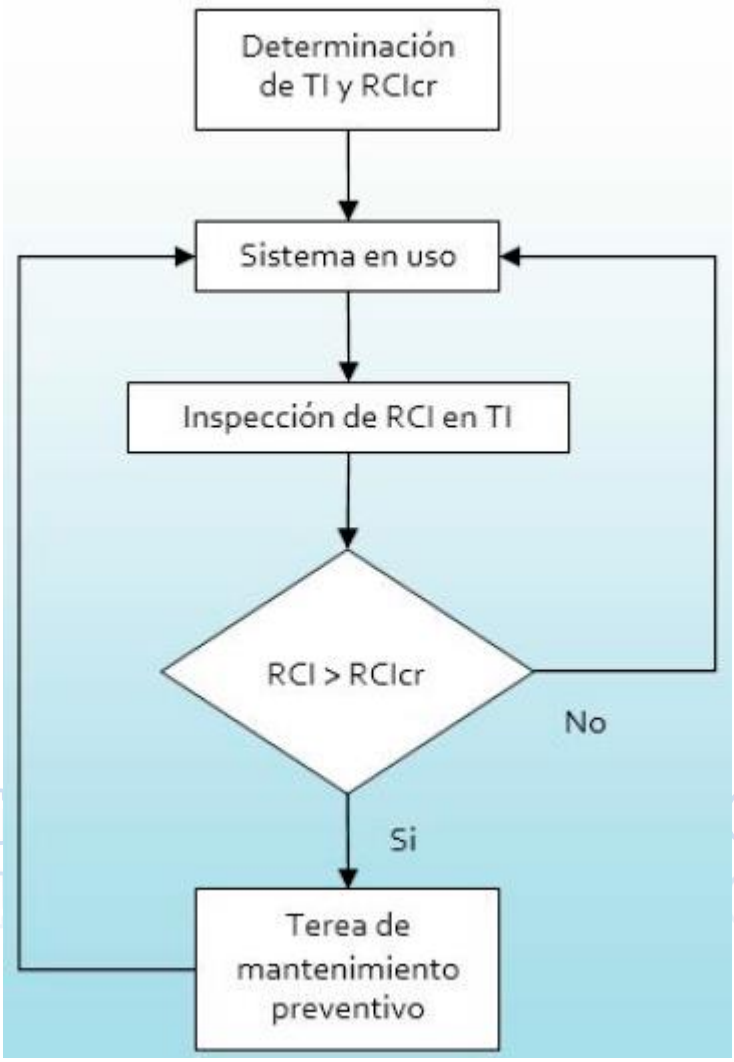
Este tipo de mantenimiento se aplica de forma clara cuando se implementa el mantenimiento con el recurso humano que está adjudicado a dicha máquina. Puede decirse que es la primera fase en el desarrollo del mantenimiento de una empresa.

Mantenimiento BASADO EN LA INSPECCIÓN (Inspection-Based, IB)

Tradicionalmente, las políticas de mantenimiento preventivo y correctivo han sido las más aplicadas entre los directores de mantenimiento. Sin embargo, durante los últimos veinte años, muchas organizaciones industriales han reconocido los ciertos inconvenientes en estos métodos.

La necesidad de garantizar la seguridad y de reducir los costes de mantenimiento ha propiciado el desarrollo de políticas de mantenimiento alternativas. El método que, hoy por hoy, se presenta más eficaz y útil para minimizar las limitaciones de las tareas de mantenimiento actuales es la política de mantenimiento basado en la condición.

- Este procedimiento de mantenimiento se basa en que la razón principal para realizar el mantenimiento en un sistema es el cambio en la condición y/o las prestaciones, y que la realización de tareas de mantenimiento preventivo se debe basar en el estado real del elemento o sistema.
- Mediante el control de ciertos parámetros se puede identificar el momento más adecuado para realizar las tareas de mantenimiento preventivo.
- La ventaja de este procedimiento es que permite utilizar el elemento considerado de una forma más adecuada que en el caso de la aplicación de mantenimiento preventivo, manteniendo el nivel de seguridad o de utilidad establecido.
- La inspección es una tarea del mantenimiento condicional. El resultado de esta inspección es un informe sobre la condición del elemento, es decir, determina si tiene una condición satisfactoria o no, lo que se determina a través del RCI (Resultado del Costo de la Inspección).
- El rasgo común de todas estas tareas es que los resultados obtenidos no influyen sobre la programación de la siguiente inspección. Antes de que el elemento o sistema se ponga en servicio se determina la frecuencia más adecuada para las inspecciones.
- Las inspecciones se llevan a cabo en intervalos fijos especificados hasta que se alcanza el nivel crítico, RCI(TIi) > RCIcr, en este momento se realizan las tareas de mantenimiento preventivo prescritas.
- Si el elemento falla entre dos inspecciones, se realizará un mantenimiento correctivo.
- En el siguiente esquema tenemos el algoritmo correspondiente al procedimiento de mantenimiento cuando se usa la inspección para vigilar la condición. (TI->Intervalo de la inspección)



Ventajas de la política de mantenimiento IB

Los sistemas cuya política de mantenimiento sigue una técnica de vigilancia de la condición producirán además información acerca de la condición de cada uno de sus elementos componentes.
Los ingenieros de mantenimiento valoran esta información cada vez más.
Pasamos a enumerar los beneficios de la vigilancia de la condición:

1. Cuanto antes se detecte el deterioro en la condición y/o en las prestaciones de un elemento o sistema mucho mejor.
2. Se tiende a reducir el tiempo de inmovilización de los sistemas, ya que los ingenieros de mantenimiento determinarán el intervalo de mantenimiento óptimo, haciendo un seguimiento de la condición de los elementos componentes del sistema. Esto permite una planificación más adecuada del mantenimiento y un uso más eficaz de los recursos de los que se dispone.
3. Mejora de la seguridad, ya que las técnicas de vigilancia permiten prever fallo, y detener el sistema antes de que dicho fallo se produzca.
   Esta técnica de mantenimiento permite mantener los sistemas más tiempo funcionando a pleno rendimiento, con lo que aumenta su disponibilidad.

Un análisis de criticidad eficiente pretende obtener un método para poder determinar la jerarquía de unos procesos determinados, de unos sistemas o de unos equipos de una planta compleja. Se podrán subdividir los elementos analizados en secciones más fáciles de manejar, de controlar y de estudiar.
Desde el punto de vista matemático la criticidad se puede expresar como:

Criticidad = Frecuencia x Consecuencia

Definiremos la frecuencia como el número de eventos o fallos que presenta el sistema o proceso estudiado.

En cambio la consecuencia la relacionaremos con el impacto y flexibilidad operacional, los costes de reparación y los impactos en seguridad y ambiente.

Por lo tanto podemos establecer los siguientes criterios fundamentales para realizar un análisis de criticidad adecuado:

- Servicio
- Calidad
- Mantenimiento (costos y horas paradas)
- Seguridad y medio ambiente

En el esquema anterior se muestra un modelo básico de análisis de criticidad.
Para el establecimiento de criterios se basará en los cuatro criterios fundamentales nombrados en el párrafo anterior.
Para la selección del método de evaluación se toman criterios de ingeniería, factores de ponderación y cuantificación.
Para la aplicación de un procedimiento definido habrá que cumplir la guía de aplicación que se haya diseñado.
La lista jerarquizada es el resultado que se obtiene del análisis.

Cuando se plantea un análisis de criticidad hay que asegurar su aplicación por alguna de las siguientes necesidades:

- Establecer prioridades en sistemas complejos
- Aprovechar y administrar recursos escasos
- Crear valor
- Establecer impacto determinado en el negocio
- Aplicar metodologías de confiabilidad operacional

Un análisis de criticidad se puede aplicar en cualquier conjunto de procesos, sistemas, equipos y/o componentes que haya que jerarquizar en función de su impacto o influencia en el proceso o entidad de la que formen parte.

Su aplicación se orienta básicamente a establecer programas de implantación y prioridades en los siguientes campos:

- En el ámbito de **mantenimiento**: Una vez determinado que sistemas son más críticos, se puede establecer una prioridad para los programas y planes de mantenimiento predictivo, preventivo, correctivo. Incluso puede ser conveniente rediseñar procedimientos y establecer prioridades para la programación y puesta en marcha de órdenes de trabajo.
- En el ámbito de **inspección:** La implantación de un programa de inspección viene determinada por el estudio de criticidad.
  La lista jerarquizada determina donde hay que realizar inspecciones, ayuda a la hora de seleccionar los intervalos y el tipo de inspección adecuada para sistemas de protección y control (temperatura, presión, velocidad, flujo, etc.) y para equipos dinámicos, estáticos y estructurales.
- En el ámbito de **materiales**: Los estudios de criticidad de los sistemas ayudan decidir sobre el nivel de equipos y piezas de repuesto que debe haber en el almacén central, así como los partes, materiales y herramientas necesarios que deben estar disponibles en los almacenes de planta.
  Por lo tanto, podemos actualizar el stock de materiales y repuestos de cada sistema y/o equipo consiguiendo un coste óptimo de inventario.
- En el ámbito de **disponibilidad** de planta. Los datos obtenidos de los estudios de criticidad permiten un punto de partida seguro en la ejecución de proyectos. Nos aporta un buen respaldo a la hora de realizar estudios de inversión de capital y renovaciones en los procesos, sistemas o equipos de una instalación, basados en el área con el mayor nivel de criticidad.
- A nivel del **personal** Un buen estudio de criticidad hará que se potencien el adiestramiento y desarrollo de habilidades en el personal. Se puede diseñar un plan de formación técnica, manual y de crecimiento personal, basado en las necesidades reales de la instalación, teniendo en cuenta primero las áreas más críticas, que será donde, a priori, hay más posibilidades de mejora y de agregar el máximo valor.

Operaciones y registro del mantenimiento

Un sistema eficaz de operación y control del mantenimiento es la columna vertebral, el eje central de una robusta administración del mantenimiento.

Un sistema eficaz de operación y control debe incorporar todas y cada una de las siguientes características:

- Demanda de mantenimiento, es decir, qué trabajo tiene que hacerse y cuándo.
- Recursos de mantenimiento, es decir, quién hará el trabajo y qué materiales y herramientas son necesarios para la realización del trabajo.
- Procedimientos y medios necesarios para coordinar, programar y ejecutar el trabajo.
- Normas de rendimiento y calidad, es decir, cuánto tiempo se requerirá para hacer un trabajo y las especificaciones necesarias y aceptables.
- Retroalimentación, seguimiento y control, es decir, el sistema debe generar información e informes para el control del coste, de la calidad y la condición de la planta; también es esencial un mecanismo de recopilación de datos y un seguimiento regular de estos.

El sistema de órdenes de trabajo es el medio apropiado para planear y controlar el trabajo de mantenimiento.

También proporciona la información necesaria para controlar, vigilar e informar sobre el trabajo de mantenimiento.

Unos procedimientos específicos y una meta clara son imprescindibles para la implantación del sistema de órdenes de trabajo y el control de las actividades de mantenimiento.

El primer paso en la planificación y el control del trabajo de mantenimiento es el establecimiento de un sistema eficaz de órdenes de trabajo. En una orden de trabajo se detallan las instrucciones escritas para el trabajo que se va a realizar y debe de haber una rellenada por cada uno de los trabajos.

En la industria se utilizan distintos nombres para hacer referencia a ellas, como solicitud de trabajo, solicitud de servicio, orden, etc.

Con el sistema de órdenes de trabajo se pretende proporcionar medios para:

- Solicitar por escrito el trabajo que va a realizar el departamento de mantenimiento.
- Seleccionar el trabajo solicitado por operación.
- Asignar el mejor método y los trabajadores más calificados para el trabajo.
- Reducir el coste mediante la utilización eficaz de los recursos (mano de obra, material).
- Mejorar la planificación y la programación del trabajo de mantenimiento.
- Mantener y controlar el trabajo de mantenimiento.
- Mejorar el mantenimiento en general mediante los datos recopilados de la orden de trabajo que serán utilizados para el control y el programa de mejora continua.

La administración del sistema de órdenes de trabajo es responsabilidad de las personas que están a cargo de la planificación y la programación. La orden de trabajo debe diseñarse con detalle teniendo en cuenta dos puntos:

- El primero consiste en incluir toda la información necesaria para facilitar una planificación y una programación eficaces.
- El segundo punto consiste en hacer hincapié en la claridad y facilidad de uso.

Parte de trabajos realizados.

- ⇨ Para obtener los datos correctos para el trabajo, el coste y el control de la condición de la planta, es esencial contar con mecanismos exactos para la recopilación de datos y el mantenimiento de registros. Es necesario tener en cuenta tres aspectos importantes: tiempo de reparación, costes y tiempo muerto.
- ⇨ El parte de trabajos realizados es un documento donde se refleja el trabajo realizado y la condición del equipo.
- ⇨ Cada trabajador, que desempeñe una función en un trabajo determinado, puede tener una tarjeta de trabajo. Puede ser de forma manual o automatizada.
- ⇨ La información contenida en la tarjeta se puede obtener de la orden de trabajo.
- ⇨ En algunas empresas cada empleado registre su trabajo diario en una tarjeta de tiempo de trabajo, es decir queda reflejado el tiempo consumido en cada orden de trabajo.

Registro de la historia del equipo

En el archivo de la historia del equipo se registra toda la información acerca del trabajo realizado en un equipo o instalación determinado. Este documento contiene información acerca de todas las reparaciones realizadas, su coste, el tiempo muerto, y las especificaciones del mantenimiento.

Es necesario registrar lo siguiente:

1. Especificaciones del equipo y ubicación del mismo.
2. Inspecciones, reparaciones, servicio y ajustes realizados, y los fallos con sus causas y las acciones correctivas aplicadas.
3. Trabajo realizado con el equipo, componentes reparados o reemplazados, condición de desgaste o rotura, erosión, corrosión, etc.
4. Mediciones o lecturas tomadas, tolerancia, resultados de pruebas e inspecciones.
5. Hora del fallo y tiempo empleado en llevar a cabo la reparación.

   Existen muchos sistemas para registrar y almacenar información. Es importante que dicha información debe ser completa y estar registrada en una forma organizada para poder acceder a ella en el futuro.

Plan de mantenimiento y verificación de equipos de red

A continuación en las siguientes páginas vamos a detallar en profundidad un plan de mantenimiento y verificación para una oficina en la que se sitúan las siguientes salas:

- **Sala 1**: Con 10 ordenadores de sobremesa y una impresora láser.
- **Despacho 1**: Con dos ordenadores de sobremesa y una impresora de inyección de tinta.
- **Despacho 2**: Con dos ordenadores de sobremesa y una impresora de inyección de tinta.
- **Sala acondicionada**: Con un armario rack vertical en cuyo interior se sitúan todos los elementos necesarios para la red.

Sala 1:

Descripción:

La sala se compone de 10 ordenadores de sobremesa conectados a la red de área local mediante latiguillos y rosetas RJ-45 hembras, fijadas a la pared mediante tacos y tornillos. Además hay una impresora IP láser conectada a la red.

El subsistema de cableado horizontal sale desde las rosetas RJ-45 hembras a través de canaletas de P.V.C. Hasta el falso techo. A través de este discurre hasta la sala en la que se encuentra el armario rack con el resto de elementos de red.

Personal que realiza la verificación:

El plan de mantenimiento y verificación de equipos de red lo realizará el personal de la propia empresa, con el administrador de redes a la cabeza.

Periodicidad de verificación:

Debido a que la naturaleza y exposición a eventualidades de cada elemento de la red es diferente, la periodicidad en la que se efectúa el plan, también será diferente para cada uno de ellos.

Elementos susceptibles de verificación:

- Ordenadores: Periodicidad: mensual
  - Monitor: Estado, Funcionamiento
  - Ratón: Estado, Funcionamiento
  - Teclado: Estado, Funcionamiento
  - CPU: Estado, Funcionamiento
  - Cableado: Estado, Funcionamiento, Conectividad
  - Tarjeta de red: Conectividad
  - Configuración de la red: IP, DNS
- Rosetas: Periodicidad: mensual
  - Elementos: Conectividad, Estado, Anclajes
- Latiguillos: Periodicidad: mensual
  - Elementos: Conectividad, Cableado, Pestañas
- Subsistema de cableado horizontal: (periodicidad: anual)
  - Cableado: Estado, Conectividad
  - Canaletas: Estado, Anclajes
- Impresora (periodicidad: mensual)
  - Elementos: Configuración de la red (IP), Funcionamiento, Estado, Consumibles

Despacho 1:

Descripción:

El despacho se compone de 2 ordenadores de sobremesa conectados a la red de área local mediante latiguillos y rosetas RJ-45 hembras, fijadas a la pared mediante tacos y tornillos. También posee una impresora de chorro de tinta y un escáner A3.

El subsistema de cableado horizontal sale desde las rosetas RJ-45 hembras a través de canaletas de P.V.C. Hasta el falso techo. A través de este discurre hasta la sala en la que se encuentra el armario rack con el resto de elementos de red.

Personal que realiza la verificación:

El plan de mantenimiento y verificación de equipos de red lo realizará el personal de la propia empresa, con el administrador de redes a la cabeza.

Periodicidad de verificación:
Debido a que la naturaleza y exposición a eventualidades de cada elemento de la red es diferente, la periodicidad en la que se efectúa el plan, también será diferente para cada uno de ellos.

- Ordenadores: Periodicidad: mensual
  - Monitor: Estado, Funcionamiento
  - Ratón: Estado, Funcionamiento
  - Teclado: Estado, Funcionamiento
  - CPU: Estado, Funcionamiento
  - Cableado: Estado, Funcionamiento, Conectividad
  - Tarjeta de red: Conectividad
  - Configuración de la red: IP, DNS
- Rosetas: Periodicidad: mensual
  - Elementos: Conectividad, Estado, Anclajes
- Latiguillos: Periodicidad: mensual
  - Elementos: Conectividad, Cableado, Pestañas
- Subsistema de cableado horizontal: (periodicidad: anual)
  - Cableado: Estado, Conectividad
  - Canaletas: Estado, Anclajes
- Impresora (periodicidad: mensual)
  - Elementos: Configuración de la red (IP), Funcionamiento, Estado, Consumibles
- Escáner A3 Periodicidad: mensual
  - Elementos: Funcionamiento, Estado

Despacho 2:

Descripción:
El despacho se compone de 2 ordenadores de sobremesa conectados a la red de área local mediante latiguillos y rosetas RJ-45 hembras, fijadas a la pared mediante tacos y tornillos. También posee una impresora de chorro de tinta.
El subsistema de cableado horizontal sale desde las rosetas RJ-45 hembras a través de canaletas de P.V.C. Hasta el falso techo. A través de este discurre hasta la sala en la que se encuentra el armario rack con el resto de elementos de red.
Personal que realiza la verificación:
El plan de mantenimiento y verificación de equipos de red lo realizará el personal de la propia empresa, con el administrador
de redes a la cabeza.
Periodicidad de verificación:
Debido a que la naturaleza y exposición a eventualidades de cada elemento de la red es diferente, la periodicidad en la que se efectúa el plan, también será diferente para cada uno de ellos.
Elementos susceptibles de verificación:

- Ordenadores: Periodicidad: mensual
  - Monitor: Estado, Funcionamiento
  - Ratón: Estado, Funcionamiento
  - Teclado: Estado, Funcionamiento
  - CPU: Estado, Funcionamiento
  - Cableado: Estado, Funcionamiento, Conectividad
  - Tarjeta de red: Conectividad
  - Configuración de la red: IP, DNS
- Rosetas: Periodicidad: mensual
  - Elementos: Conectividad, Estado, Anclajes
- Latiguillos: Periodicidad: mensual
  - Elementos: Conectividad, Cableado, Pestañas

- Subsistema de cableado horizontal: (periodicidad: anual)
  - Cableado: Estado, Conectividad
  - Canaletas: Estado, Anclajes
- Impresora (periodicidad: mensual)
  - Elementos: Configuración de la red (IP), Funcionamiento, Estado, Consumibles

Sala acondicionada

Descripción:
En la sala acondicionada, hay un armario rack vertical. En su interior se disponen todos los elementos necesarios para garantizar la conectividad de la red: Paneles de Parcheo, Switch, un servidor local, una fuente de alimentación ininterrumpida, los latiguillos necesarios y una regleta de alimentación.

Personal que realiza la verificación:
El plan de mantenimiento y verificación de equipos de red lo realizará el personal de la propia empresa, con el administrador de redes a la cabeza.

Periodicidad de verificación:
Debido a que la naturaleza y exposición a eventualidades de cada elemento de la red es diferente, la periodicidad en la que se efectúa el plan, también será diferente para cada uno de ellos.

Elementos susceptibles de verificación:

- Servidor: Periodicidad: mensual
  - Monitor: Estado, Funcionamiento
  - Ratón: Estado, Funcionamiento
  - Teclado: Estado, Funcionamiento
  - CPU: Estado, Funcionamiento
  - Cableado: Estado, Funcionamiento, Conectividad
  - Tarjeta de red: Conectividad
  - Configuración de la red: IP, DNS
- Rack: Periodicidad: trimestral
  - Elementos: Puerta, Sistema De Ventilación, Alimentación, Toma De Tierra, Anclajes Interiores, Anclajes Exteriores, Elementos Extraños
- Paneles de parcheo: Periodicidad: trimestral
  - Elementos: Estado, Crimpado Hembra, Anclajes, Conectividad
- Latiguillos: Periodicidad: trimestral
  - Elementos: Conectividad, Cableado, Pestañas
- Switch: Periodicidad: trimestral
  - Elementos: Estado, Anclajes, Conectividad, Alimentación
- S.A.I: Periodicidad: mensual
  - Elementos: Alimentación E / S, Tiempo De Descarga, Estado, Anclajes
- Router: Periodicidad: mensual
  - Elementos: Alimentación, Conectividad Con Internet, Conectividad LAN, Wifi, Configuración, Anclajes
- Regleta de alimentación: Periodicidad: trimestral
  - Elementos: Conectividad, Estado, Anclajes

Herramientas y sistemas de medida:

Descripción:
Se dispone de multitud de herramientas para llevar a cabo las labores de mantenimiento. Cabe desatacar un ordenador portátil para comprobar la configuración u conectividad de los demás elementos.

Personal que realiza la verificación:
El plan de mantenimiento y verificación de equipos de red lo realizará el personal de la propia empresa, con el administrador de redes a la cabeza.

Periodicidad de verificación:
Debido a que la naturaleza y exposición a eventualidades de cada elemento de la red es diferente, la periodicidad en la que se efectúa el plan, también será diferente para cada uno de ellos.

- Crimpadora: Periodicidad: trimestral
  - Elementos: Estado, Funcionamiento
- Pinzas crimpadoras: Periodicidad: trimestral
  - Elementos: Estado, Funcionamiento
- Polímetro: Periodicidad: trimestral
  - Elementos: Batería, Estado, Funcionamiento, Calibrado de medidas, Puntas de Prueba
- Soldador de estaño: Periodicidad: trimestral
  - Elementos: Estado, Funcionamiento, Estaño
- Tester RJ-45: Periodicidad: Trimestral
  - Elementos: Batería, Estado, Funcionamiento
- Ordenador portátil: Periodicidad: mensual
  - CPU: Estado, Funcionamiento
  - Cableado: Estado, Funcionamiento, Conectividad
  - Tarjeta de red: Conectividad
  - Configuración de la red: IP, DNS

A continuación vamos a ver las plantillas que usaremos para verificar cada Sala y Elemento…

Sala: Sala 1			Mes:		
Equipo	Elemento	Punto de verificación	Verificador	Fecha	Resultado
Ordenador 1	Monitor	Estado			
		Funcionamiento			
	Ratón	Estado			
		Funcionamiento			
	Teclado	Estado			
		Funcionamiento			
	CPU	Estado			
		Funcionamiento			
	Cableado	Estado			
		Funcionamiento			
		Conectividad			
	Tarjeta de Red	Conectividad			
	Configuración de red	IP			
		DNS			
Roseta 1	Andajes				
	Conectividad				
	Estado				
Latiguillo 1	Pestaña				
	Cableado				
	Conectividad				
REPETIR PARA LOS 10 ORDENADORES					
Subsistema de cableado horizontal	Canaletas	Andajes			
		Estado			
	Cableado	Estado			
		Conectividad			
Impresora	Configuración de red (IP)				
	Funcionamiento				
	Consumibles				

Plantilla de verificación de la sala 1

Sala: Despacho 1			Mes:		
Equipo	Elemento	Punto de verifica-ción	Verificador	Fecha	Resultado
Subsistema de cableado hori-zontal	Canaletas	Andajes			
		Estado			
	Cableado	Estado			
		Conectividad			
Impresora	Configuración de red (IP)				
	Funcionamiento				
	Consumibles				
Escáner A3	Funcionamiento				
	Estado				

Para el despacho 1, lo mismo en ordenador 1 y 2 y además:

Plantilla de verificación del despacho 1

Lo mismo para el Despacho 2… también ordenador 1 y 2 y además:

Sala: Despacho 2			Mes:		
Equipo	Elemento	Punto de verifica-ción	Verificador	Fecha	Resultado
.....					
Subsistema de cableado hori-zontal	Canaletas	Anclajes			
		Estado			
	Cableado	Estado			
		Conectividad			
Impresora	Configuración de red (IP)				
	Funcionamiento				
	Consumibles				

Plantilla de verificación del despacho 2

Luego la Sala acondicionada

Sala: Sala acondicionada			Mes:		
Equipo	Elemento	Punto de verificación	Verificador	Fecha	Resultado
Servidor	Monitor	Estado			
		Funcionamiento			
	Ratón	Estado			
		Funcionamiento			
	Tedado	Estado			
		Funcionamiento			
	CPU	Estado			
		Funcionamiento			
	Cableado	Estado			
		Funcionamiento			
		Conectividad			
	Tarjeta de Red	Conectividad			
	Configuración de red	IP			
		DNS			
Rack	Puerta				
	Sistema de ventilación				
	Alimentación				
	Toma de tierra				
	Anclajes interiores				
	Anclajes exteriores				
	Elementos Extraños				

Paneles de Parcheo	Estado				
	Crinpado hembra				
	Andajes				
	Conectividad				
Switch	Estado				
	Andajes				
	Conectividad				
	Alimentación				
Latiguillos	Pestaña				
	Cableado				
	Conectividad				
SAI	Alimentación E/S				
	Tiempo de descarga				
	Estado				
	Andajes				
Regleta de alimentación	Estado				
	Conectividad				
	Andajes				
Router	Estado				
	Alimentación				
	conectividad con internet				
	Conectividad LAN				
	Wi-Fi				
	Andajes				
	Configuración				
Paneles de parcheo	Canaletas	Anclajes			
		Estado			
	Cableado	Estado			
		Conectividad			

Plantilla de verificación de la sala acondicionada

Herramientas y Equipos De Medida			Mes:		
Equipo	Elemento	Punto de verificación	Verificador	Fecha	Resultado
Crimpadora	Estado				
	Funcionamiento				
Pinzas Crimpadoras	Estado				
	Funcionamiento				
Polímetro	Batería				
	Estado				
	Funcionamiento				
	Calibrado de medidas				
	Puntas de Prueba				
Soldador de Estaño	Estado				
	Funcionamiento				
	Estaño				
Tester RJ-45	Batería				
	Estaño				
	Funcionamiento				
Ordenador Portatil	CPU	Estado			
		Funcionamiento			
	Cableado	Estado			
		Funcionamiento			
		Conectividad			
	Tarjeta de Red	Conectividad			
	Configuración de red	IP			
		DNS			
Resto de herramientas	Disponibilidad				
	Estado				

Plantilla de verificación de las herramientas y los equipos de medida

Ejemplo de Plan de Mantenimiento del Sistema de Cableado de una oficina de una empresa de ventas ubicada en la primera planta de un edificio. Que tiene un sistema de videovigilacia, wifi invitados y wifi empleados.

1º Describimos todos los equipos activos y pasivos presentes:

- Activos: Switch, Router, Puntos de Acceso (AP), cámaras de Videovigilancia y los grabadores de las cámaras (NVR)
- Pasivos: Armario (Rack), Patch panel, cables de red de la instalación, latiguillos, tomas de usuario (rosetas), canaletas, bandejas, puntos de consolidación

2º Especificamos todos los elementos susceptibles de verificación y su periodicidad:

Equipos	Elementos	Periodicidad
Switch	Estado Conectividad Alimentación	Mantenimiento autónomo Quincenal (Apagamos los Switch cada 2 fines de semana) Mantenimiento preventivo trimestral: verificar la configuración y los puertos
Router	Alimentación Conectividad WAN, Conectividad LAN, Wifi, Configuración, Anclajes	Mantenimiento autónomo Semanal (Apagamos el Router cada fin de semana) Mantenimiento preventivo trimestral: verificar la configuración y los puertos
AP PoE	Conectividad LAN, Wifi, Configuración, Anclajes	Mantenimiento autónomo No tiene Mantenimiento preventivo Semestral: verificar la configuración y los puertos
Cámaras PoE	Conectividad LAN, Configuración y Funcionamiento, Anclajes	Mantenimiento autónomo mensual: mover camara y verificar funcionamiento. Mantenimiento preventivo Semestral: verificar la configuración y los puertos
NVR	Conectividad LAN, Configuración y Funcionamiento Discos	Mantenimiento autónomo mensual: verificar funcionamiento. Mantenimiento preventivo Anual: recuperar, borrar grabaciones…
Rack	Puerta, Sistema de Ventilación, Alimentación, Toma de Tierra, Anclajes Interiores, Anclajes Exteriores, Elementos Extraños	Mantenimiento autónomo No tiene Mantenimiento preventivo Mensual: verificar niveles, elementos externos y limpieza
Patch Panel	Estado, Crimpado Hembra, Anclajes, Conectividad	Mantenimiento autónomo No tiene Mantenimiento preventivo Anual: verificar elementos externos, conexiones y limpieza
Cables de Red	Estado, Crimpado Hembra, Tensiones, Conectividad	Mantenimiento autónomo No tiene Mantenimiento preventivo Anual: verificar elementos externos, tensiones, conexiones y limpieza

Latiguillos	Conectividad, Cableado, Pestañas y Crimpado Macho	Mantenimiento autónomo quincenal: comprobar conectores y integridad del cable. Mantenimiento preventivo Mensual: comprobar conectores, tensiones, conexiones y limpieza
Tomas de Usuario	Conectividad, Estado, Anclajes	Mantenimiento autónomo quincenal: comprobar conectores. Mantenimiento preventivo Mensual: comprobar conectores, tensiones, conexiones y limpieza
Canaletas	Estado, Anclajes, Elementos Externos y Limpieza, Estanqueidad	Mantenimiento autónomo No tiene Mantenimiento preventivo Anual: verificar elementos externos, tensiones y limpieza
Bandejas	Estado, Anclajes, Elementos Externos y Limpieza	Mantenimiento autónomo No tiene Mantenimiento preventivo Anual: verificar elementos externos, tensiones y limpieza
Puntos de Consolidación	Estado, Anclajes, Elementos Externos y Limpieza, Estanqueidad	Mantenimiento autónomo No tiene Mantenimiento preventivo Anual: verificar elementos externos, tensiones y limpieza

Resumen

Ya visto en módulos anteriores.

- *Enlaces:*
  - *Enlaces físicos: medios guiados-> cables: Par trenzado, Coaixal, Fibra Óptica*
  - *Enlaces inalámbricos: no guiados-> ondas de radio, microondas e infrarojos*
- *Datos: analógicos y digitales*
- *Nodos:*
  - *Punto a punto y de Difusión*
  - *Protocolos*
  - *Capa TCP/IP*
  - *IPv4*
  - *IPv6*
  - *Mascara de SubRed*
- *Elementos de Hardware:*
  - *Switch, Router, Repetidores, Puntos de Acceso, Modem, Gateway…*

1.3 Elementos de Software:

- Sistema Operativo. Funciones y Partes
  - Tipos de sistema Operativo: Usuario y Servidor
  - Linux: Kernel y Distribuciones
- Aplicaciones Informáticas: En el campo de las redes categorías
- Servidor:
  - Concepto de Servidor
  - y funciones que ofrece: Web, FTP, Base de datos…
  - Formatos: Rack, Torre y Blade
- Firmware: software especifico para un hardware determinado, integrado en el hardware y almacenado en la memoria del dispositivo

2. Mantenimiento y actualización:

- Herramientas de acceso remoto:
  - Escritorio Remoto
  - Terminal: Putty (SSH), Teamviewer y Anydesk
- Protocolos de Acceso remoto: RDP, SSH

Tipos de Mantenimiento:

- Correctivo.
  - Pasos
  - Estados de una incidencia: Abierta/Asignada/En Proceso/Cerrada
- Preventivo
  - Actualizaciones y Parches de Seguridad
  - Virus Informáticos
  - Intrusiones (IDS, IPS)
  - Cortafuegos:
    - Permitir-Denegar
    - Políticas Permisivas-Restrictivas
    - Categorías: Lateral, DMZ de una Pata, DMZ Dual
  - UTM (Gestión unificada de amenazas)
  - Copia de Seguridad
  - SAI
  - Auditoria de Seguridad
  - Documentación

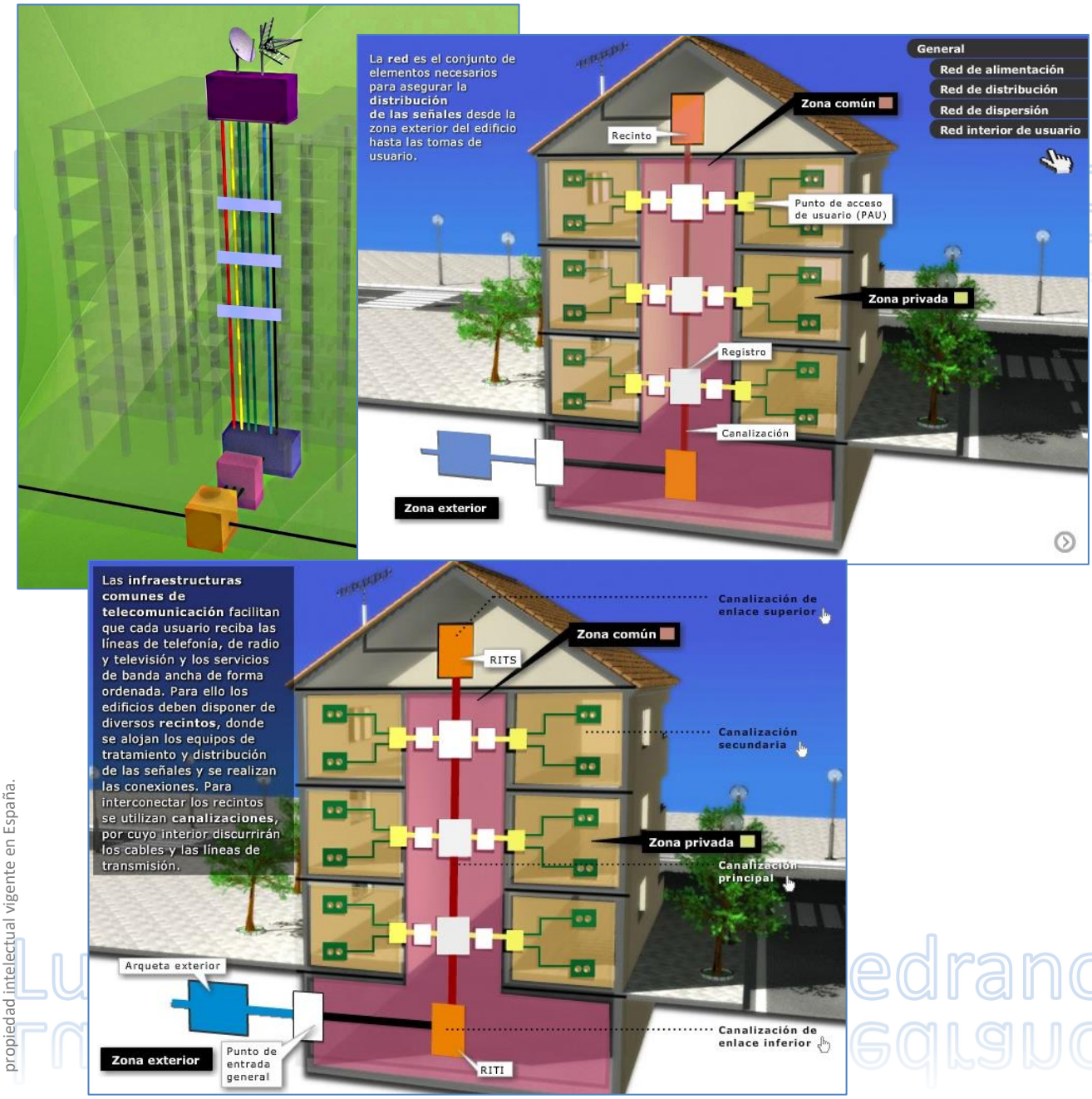
ICT – Infraestructura Común de Telecomunicaciones

ICT – Reglamento 2003
ICT2 – Reglamento 2011
Debido al cumplimiento de la Orden Ministerial ECE/983/2019 (normativa ICT3), todas las viviendas entregadas desde el 3 de octubre de 2020 deben incorporar una toma de fibra óptica en el hogar.

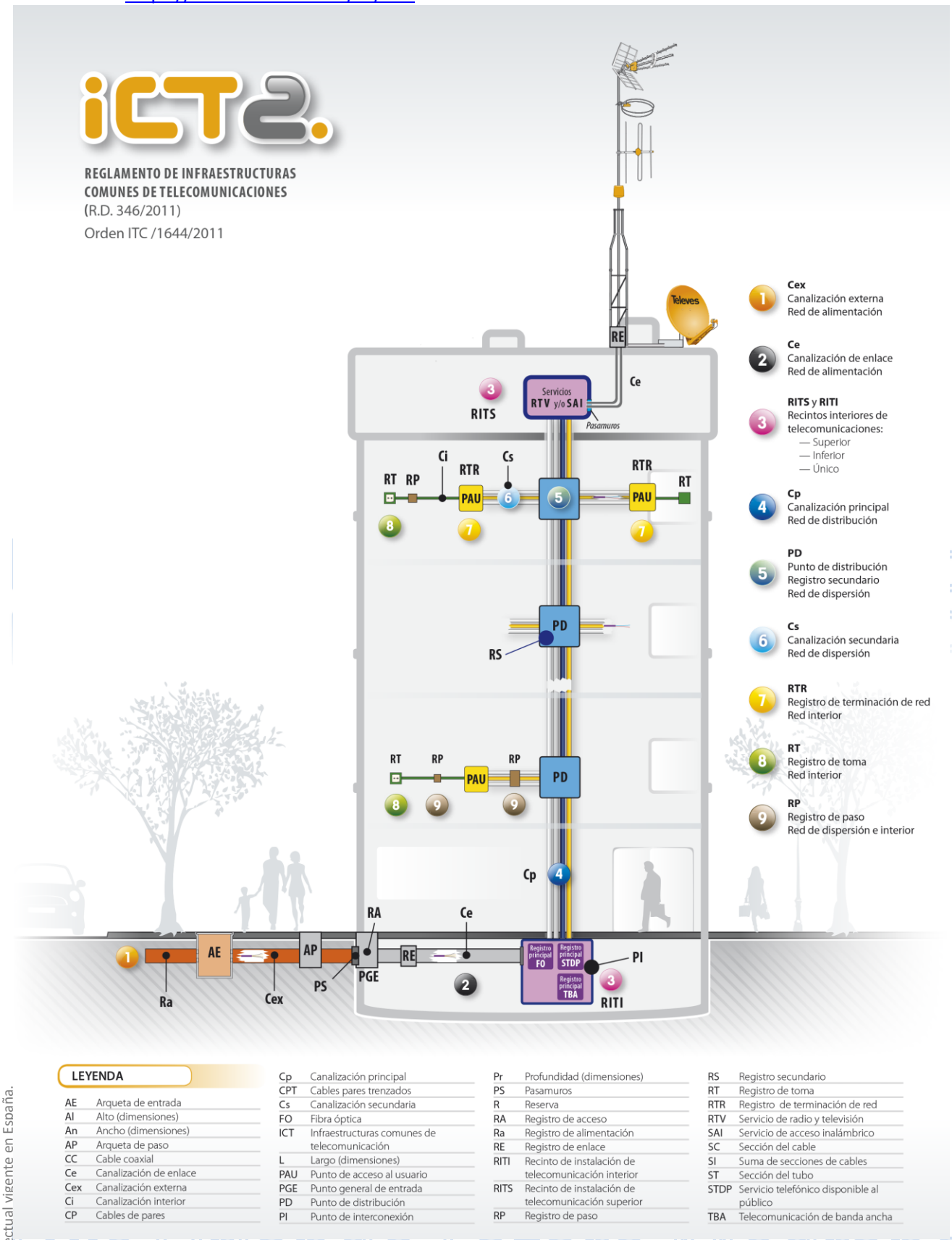
Si existiese una autorización previa por parte de la propiedad, en el recinto se podrían ubicar instalaciones para dar servicio de telecomunicación a otras edificaciones de la zona. Si la autorización ha sido concedida durante la fase de construcción de la edificación ésta deberá ser ratificada por la comunidad de propietarios o por el propietario final de la edificación para que tenga validez.
Dependiendo del tipo y ubicación del recinto, éstos podrán ser de cuatro tipos diferentes:

- Recinto Inferior (RITI)
- Recinto Superior (RITS)
- Recinto Único (RITU)
- Recinto Modular (RITM)

En este vídeo vamos a ver una simulación de una instalación ICT: https://www.youtube.com/watch?v=y_t3goA19R0

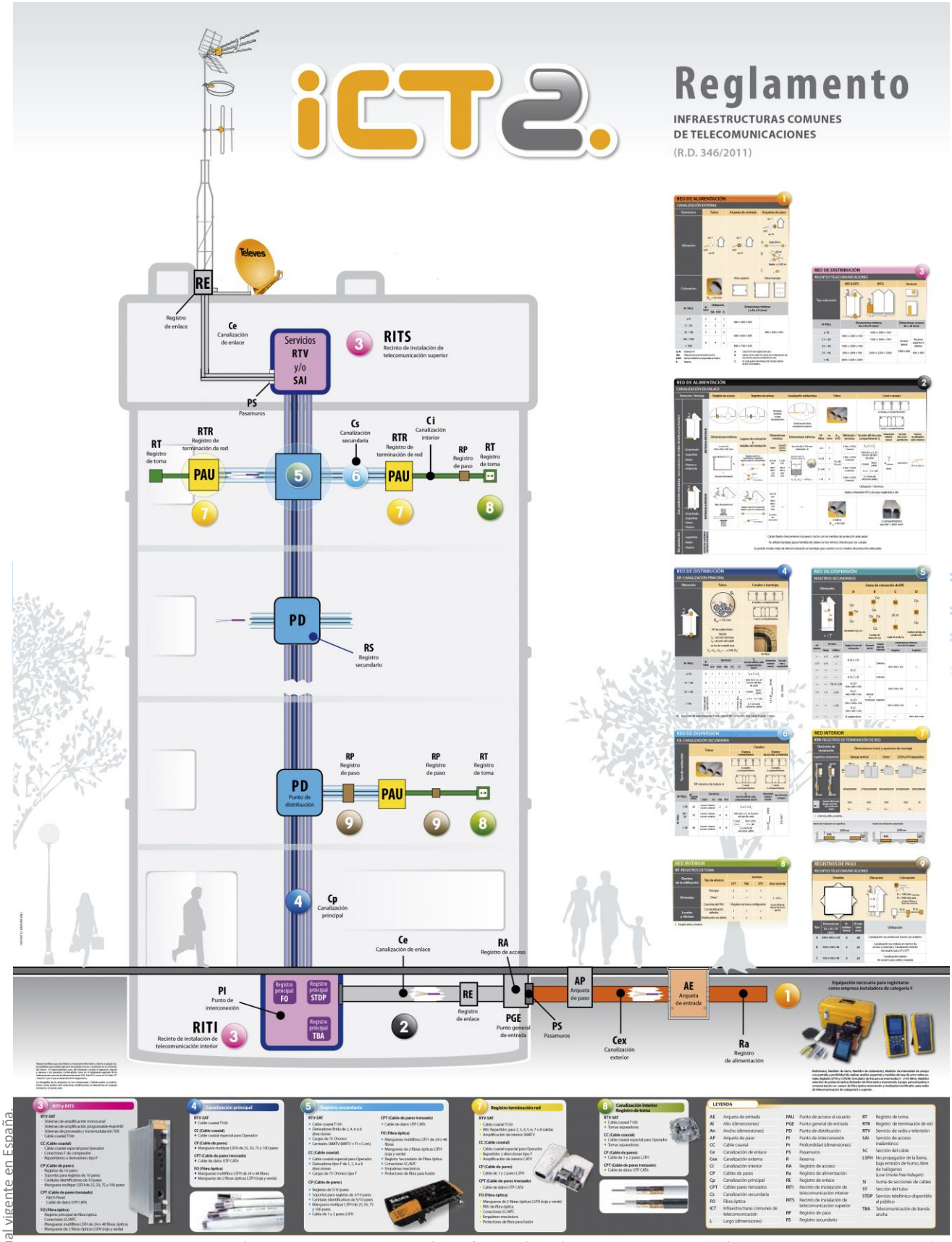


Mas info en: https://www.televes.com/es/ict2



LEYENDA

AE	Arqueta de entrada
Al	Alto (dimensiones)
An	Ancho (dimensiones)
AP	Arqueta de paso
CC	Cable coaxial
Ce	Canalización de enlace
Cex	Canalización externa
Ci	Canalización interior
CP	Cables de pares
Cp	Canalización principal
CPT	Cables pares trenzados
Cs	Canalización secundaria
FO	Fibra óptica
ICT	Infraestructuras comunes de telecomunicación
L	Largo (dimensiones)
PAU	Punto de acceso al usuario
PGE	Punto general de entrada
PD	Punto de distribución
PI	Punto de interconexión
Pr	Profundidad (dimensiones)
PS	Pasamuros
R	Reserva
RA	Registro de acceso
Ra	Registro de alimentación
RE	Registro de enlace
RITI	Recinto de instalación de telecomunicación interior
RITS	Recinto de instalación de telecomunicación superior
RP	Registro de paso
RS	Registro secundario
RT	Registro de toma
RTR	Registro de terminación de red
RTV	Servicio de radio y televisión
SAI	Servicio de acceso inalámbrico
SC	Sección del cable
SI	Suma de secciones de cables
ST	Sección del tubo
STDP	Servicio telefónico disponible al público
TBA	Telecomunicación de banda ancha



El Recinto para la Instalación de Telecomunicación Inferior (RITI) es el local o habitáculo en que se instalarán los registros principales para los distintos operadores de los servicios de telefonía disponible al público y de telecomunicaciones de banda ancha así como los posibles elementos necesarios para el suministro de estos servicios. De este recinto también saldrá la canalización principal de la ICT de la edificación.

Los registros principales para los servicios de telefonía disponible al público y de banda ancha son las envolventes que contienen los puntos de interconexión entre las redes de alimentación de los diferentes operadores y la de distribución de la edificación. En el caso particular de que la red de distribución de la edificación atienda a un número reducido de PAU, puede contener directamente el punto de distribución.
El Recinto para la Instalación de Telecomunicación Superior (RITS) es el local o habitáculo en el que se instalarán los elementos necesarios para el suministro de los servicios de RTV . si se diese el caso, elementos de los servicios de acceso inalámbrico (SAI).
En él se alojarán los elementos necesarios para adecuar las señales procedentes de los sistemas de captación de emisiones radioeléctricas de RTV, para su distribución por la ICT de la edificación, en el caso de servicios de acceso inalámbrico, los elementos necesarios para trasladar las señales recibidas hasta el RITI.
Cuando se trata de edificios de tres pisos y planta baja con un máximo de diez PAU o se trata de viviendas unifamiliares se establece la posibilidad de construir un Recinto para la Instalación de Telecomunicación Único que reúna las características aportadas a las edificaciones que cuentan con RITI y RITS.
Cuando se trata de edificaciones que cuentan con hasta cuarenta y cinco PAU y conjuntos de viviendas unifamiliares con hasta veinte PAU los RITI, RITS y RITU pueden ser realizados mediante armarios de tipo modular que cuenten entre sus características el ser no propagadores de llama en caso de incendio.
La canalización principal es aquella que soporta la red de distribución de la ICT de la edificación conecta el RITI y el RITS entre sí además de conectarlos con los registros secundarios.
En esta canalización se pueden intercalar los registros secundarios que conectan la canalización principal y las canalizaciones secundarias. Los registros secundarios pueden servir también para seccionar la canalización principal o para conseguir un cambio de dirección en la misma.
Cuando el acceso inalámbrico es de servicios distintos al de radiodifusión y televisión esta canalización principal tiene como objetivo extra la de conseguir el traslado de señales desde el RITS hasta el RITI.
Según establece la normativa al respecto, cuando se trata edificaciones en altura, la canalización principal deberá ser rectilínea, fundamentalmente vertical y de una capacidad suficiente para alojar todos los cables necesarios para los servicios de telecomunicación de la edificación. Cuando el número de usuarios (viviendas, oficinas, locales o estancias comunes de la edificación) por planta sea superior a ocho se dispondrá de más de una distribución vertical en número suficiente para que cada una de ellas atienda a un máximo de ocho usuarios por planta.
En edificaciones con distribución en varias verticales, cada vertical tendrá su canalización principal independiente, y partirán todas ellas del registro principal único tal y como se contempla en la normativa aplicable de especificaciones técnicas. Para una edificación o conjunto de edificios, con canalización principal compuesta de varias verticales, se garantizará la continuidad de los servicios a toda la edificación o conjunto.
En general, las canalizaciones principales deberán unir los recintos superior e inferior. Ahora bien, en el caso de varias escaleras o bloques de viviendas en las que se instale una ICT común para todas ellas y con características constructivas que supongan distintas alturas de las escaleras o bloques de viviendas, cubiertas inclinadas de teja, existencia de viviendas tipo dúplex en áticos, azoteas privadas, en general, condicionantes que imposibiliten el acceso y la instalación de la canalización principal de unión de los recintos, las canalizaciones principales que correspondan a escaleras donde no esté ubicado el RITS, finalizarán en el registro secundario de la última. La canalización discurrirá próxima al hueco de ascensores o escalera.
Cuando la canalización deba realizarse en tramos a la intemperie los sistemas de conducción de cables deberán tener una adecuada resistencia a las influencias externas meteorológicas, climáticas, ambientales o cualquier otra que pueda incidir en el buen estado de los materiales empleados. Cuando la canalización principal esté construida mediante conductos de obra de fábrica la resistencia de las paredes deberá tener una resistencia al fuego EI 12. es decir, en caso de incendio debe poder conservar su integridad y aislamiento durante al menos 120 minutos.
En caso de que pueda producirse un incendio y teniendo en mente la idea de evitar en la medida de lo posible la caída de objetos y la propagación de las llamas, se dispondrá de elementos cortafuegos como mínimo cada tres plantas En el caso de viviendas unifamiliares, la canalización deberá ser lo más rectilínea posible y con capacidad suficiente para alojar todos los cables necesarios para los servicios de

telecomunicación. Que incluirá la ICT. Discurrirá. siempre que sea razonable, por la zona común y en cualquier caso por zonas accesibles.
En el caso de los registros secundarios éstos estarán situados en las zonas comunitarias que sean de fácil acceso, y deberán estar dotados con el correspondiente sistema de cierre . en los casos en los que en su interior se aloje algún elemento de conexión dispondrá de llave que deberá estar en posesión de la propiedad de la edificación.

Existe una serie de situaciones reglamentadas en las que se hace necesaria la instalación de registros secundarios para asegurar el buen funcionamiento de la instalación:
En el caso de edificaciones de viviendas se instalarán registros secundarios en el punto de encuentro entre una canalización principal y una secundaria. Cuando se trate de viviendas unifamiliares se instalarán registros secundarios en los puntos de segregación de la red hacia las viviendas. Deberán disponer de espacios delimitados para cada uno de los servicios. Deberán tener la capacidad de alojar como mínimo los derivadores de la red de RTV y de la red de cables coaxiales de TBA cuando proceda, así como las regletas o cajas de segregación que constituyen el punto de distribución de cables de pares y de fibra óptica o el paso de cables de pares trenzados, coaxiales y de fibra óptica.

- En cada cambio de dirección o bifurcación de la canalización principal.
- En cada tramo de 30 m de canalización principal.
- En los casos de cambio en el tipo de conducción.

Los cambios de dirección con canales y bandejas se harán mediante los accesorios adecuados garantizando el radio de curvatura necesario de los cables. En los casos en que se utilicen un RITI situado en la planta baja, o un RITS situado en la última planta de viviendas, podrá habilitarse una parte de éste en la que se realicen las funciones de registro secundario de planta desde donde saldrá la red de dispersión de los distintos servicios hacia las viviendas, oficinas, locales o estancias comunes de la edificación situados en dichas plantas.
La canalización secundaria es la que soporta la red de dispersión de la edificación uniendo los registros secundarios con los registros de terminación de red. En esta canalización se intercalan los registros de paso, que son aquellos registros que facilitan el tendido del cableado entre los registros secundarios y los registros de terminación de red.
Los registros de terminación de red conectan las canalizaciones secundarias con las canalizaciones interiores de usuarios. Estos registros proporcionan el punto de acceso a los usuarios por lo que se colocarán en el interior de la vivienda, oficina o estancia común de la edificación.
Algunos de los elementos que conforman los PAU que se alojan en ellos podrán ser suministrados por los operadores de los servicios después de haber alcanzado un acuerdo con ellos por parte de los usuarios de las viviendas, oficinas, locales y estancias comunes.
El registro secundario deberá dar salida a varias canalizaciones secundarias que deberán tener capacidad suficiente para albergar en su interior el cableado necesario para los servicios de telecomunicación de las viviendas a las que provea servicio. Esta canalización podrá hacerse mediante la utilización de tubos o de canales. En caso de realizarse mediante tubos, en aquellos tramos comunitarios será de 4 tubos como mínimo para alojar los siguientes cables:

- Un tubo para cables de pares o pares trenzados.
- Un tubo para cables coaxiales de servicios TBA (Banda Ancha).
- Un tubo para cables coaxiales de servicios RTV (radio y televisión)
- Un tubo para cables de fibra óptica.

Si el sistema de canalización elegido es mediante canales en ese caso los tramos comunitarios tendrá 4 espacios independientes con la asignación y dimensiones establecidas legalmente. En los tramos de acceso a las viviendas, se dispondrán de tres espacios independientes y se dimensionarán de acuerdo a lo establecido legalmente.

Para la distribución o acceso a las viviendas en edificaciones de pisos, se colocará en la derivación un registro de paso tipo A del que saldrán a la vivienda 3 tubos de 25 mm de diámetro exterior, con la siguiente utilización:

- Un tubo para cables de pares o pares trenzados y para los cables de fibra óptica.
- Un tubo para cables coaxiales de servicios TBA.
- Un tubo para cables coaxiales de servicios RTV.

Cuando se trate de edificaciones con un número de viviendas o locales por planta inferior a seis o cuando se trate de viviendas unifamiliares se podrá prescindir del registro de paso, por lo que las canalizaciones se establecerán entre los registros secundario y de terminación de red mediante 3 tubos de 25 mm de diámetro, o canales equivalentes con tres espacios delimitados, cuya utilización será la siguiente:

- Un tubo para cables de pares o pares trenzados y para los cables de fibra óptica.
- Un tubo para cables coaxiales de servicios TBA.
- Un tubo para cables coaxiales de servicios RTV.

Esta simplificación podrá ser efectuada siempre que la distancia entre dichos registros no supere los 15 metros; en caso contrario habrán de instalarse registros de paso que faciliten las tareas de instalación y mantenimiento.

En los casos en que existan curvas en la canalización secundaria, el radio de curvatura será tal, que los cables en la instalación no tengan un radio de curvatura inferior a 2 cm.

En cuanto a la canalización interior del usuario estará realizada con tubos o canales y utilizará configuración en estrella, generalmente con tramos horizontales y verticales. En el caso de que se realice mediante tubos, éstos serán rígidos o curvos, que irán empotrados por el interior de la vivienda, y unirán los registros de terminación de red con los distintos registros de toma, mediante tubos independientes de 20 mm de diámetro exterior como mínimo.

En el caso de que se realice mediante canales, éstos se instalarán en montaje superficial o enrasado, uniendo los registros de terminación de red con los distintos registros de toma.

Deberán tener un mínimo de 3 espacios independientes que alojarán únicamente cables para servicios de telecomunicación uno para cables de pares trenzados para servicios de TBA, otro para cables coaxiales para servicios de TBA y otro para servicios de RTV.

En el caso particular de canalizaciones interiores de usuario en locales comerciales u oficinas se admite también el uso de bandejas Las bandejas deberán tener las mismas dimensiones y compartimentos que tiene la estructura formada por canales.

La Norma Técnica para Telefonía recoge el dimensionamiento mínimo que debe tener la red de distribución.

En cuanto a las redes de cables de pares trenzados establece que en edificaciones con un vertical, una vez que se conozcan o estimen las necesidades que puedan surgir a largo plazo tanto por plantas como en el total de la edificación se dimensionará la red de distribución multiplicando la cifra de demanda prevista por el factor .2. De esta manera se logre asegurar una reserva suficiente para prever posibles averías de alguna acometida o alguna desviación por exceso en la demanda de acometidas.

Si se trata de edificaciones que cuentan con varias verticales, la red de cada vertical edificada se tratará como una red de distribución independiente y se realizarán los mismos cálculos que se realizan en casa de edificaciones con una sola vertical.

Cuando se trate de redes de cables de pares en edificaciones con una sola vertical, una vez que se conozcan o estimen las necesidades que puedan surgir a largo plazo tanto por plantas como en el total de la edificación se dimensionará la red de distribución multiplicando la cifra de demanda prevista por el factor .2. De esta manera se logre asegurar una reserva suficiente para prever posibles averías en alguno de los pares o alguna desviación por exceso en la demanda de líneas. Una vez que se haya realizado el cálculo y se haya obtenido el número de pares, se utilizará cable normalizado de capacidad igual o superior al valor obtenido en el cálculo realizado. También es posible realizar combinaciones de cables para llegar a dicho valor.

Hay que tener en cuenta que el cable máximo será para de 100 pares y se debe utilizar el menor número posible de cables.

Para el dimensionado de la red de distribución se proyectará con cables multipares que estarán todos conectados en la regleta de salida del punto de interconexión.

En el caso de edificios que cuenten con una red de distribución/ dispersión igual o inferior a treinta (30) pares, se podrá realizar utilizando cables de uno o dos pares desde el punto de distribución instalado en el registro principal. De este registro partirán los cables de acometida que subirán por las distintas plantas hasta acabar directamente en los PAU.
Los puntos de distribución estarán formados por las regletas de conexión en cantidad suficiente para agotar con holgura toda la posible demanda de conexiones de cada planta. El número de regletas se hallará calculando el cociente entero redondeado por exceso que resulte de dividir el total de pares del cable de distribución por el número de plantas y por cinco o diez, según el tipo de regleta que se vaya a utilizar.
Cuando se trate de edificios con varias verticales, la red de cada vertical será tratada como una red de distribución independiente, y se diseñará, por tanto, de acuerdo con lo indicado anteriormente.
El dimensionamiento de las redes de dispersión de cables de pares trenzados será el suficiente para instalar los cables de pares trenzados de acometida que cubran la demanda prevista como prolongación de la red de distribución (en paso en los registros secundarios), y terminarán en el PAU de cada vivienda en la roseta correspondiente.

Cuando se trate de redes de dispersión de cables de pares se realizará la instalación de cables de pares de acometida que cubran la demanda prevista, se conectarán al correspondiente terminal de la regleta del punto de distribución y terminarán en el PAU de cada vivienda en la roseta correspondiente.

El dimensionamiento que debe tener como mínimo la red interior de pares trenzados se hará teniendo en cuenta el uso al que se vaya a destinar el habitáculo.

Cuando se trata de viviendas, el número de registros de toma equipados con BAT será de uno por cada estancia, excluidos baños y trasteros, con un mínimo de dos. De igual modo, en al menos dos de los registros de toma se equiparán BAT con dos tomas o conectores hembra, alimentadas por acometidas de pares trenzados independientes procedentes del PAU.
Para los locales y oficinas cuyo interior esté dividido en estancias, el número de registros de toma será de uno por cada estancia, excluidos baños y trasteros, equipados con BAT con dos tomas o conectores hembra, alimentadas por acometidas de pares trenzados independientes procedentes del PAU. Cuando no esté definida su distribución en estancias habrá que tener en cuenta no instalar red interior de usuario, puesto que el diseño y dimensionamiento de la red interior de usuario, así como su realización futura, será responsabilidad de la propiedad del local u oficina, cuando se ejecute el proyecto de distribución en estancias.

Para estancias o instalaciones comunes del edificio el proyectista definirá el dimensionamiento de la red interior en estas estancias teniendo en cuenta la finalidad de las estancias y las prestaciones previstas para la edificación.

En cuanto a los materiales que se pueden utilizar en la ICT, se debe tener en cuenta que existen una serie de parámetros y características técnicas para definir cuales utilizar. Estos parámetros y características son una referencia de mínimos, por lo que se pueden utilizar otros que ofrezcan mejores prestaciones a las indicadas a continuación.

Los cables de pares trenzados utilizados en las redes de distribución y dispersión serán Como mínimo:

- de 4 pares de hilos conductores de cobre con aislamiento individual sin apantallar clase E (cat. 6)
- deberán cumplir las especificaciones de la norma UNE-EN 50288-6-1 (Cables metálicos con elementos múltiples utilizados para la transmisión y el control de señales analógicas y digitales.

Redes de cables de pares o cables multipares utilizados en las redes de distribución y dispersión deberá. como mínimo:

- cumplir con las especificaciones del tipo ICT+100 de la norma UNE 212001 (Especificación particular para cables metálicos de pares utilizados para el acceso al servicio de telefonía disponible al público. Redes de distribució. dispersión e interior de usuario)
- deberán poseer cubierta no propagadora de la llama, libre de halógenos y con baja emisión de humos.

Cuando se trate de viviendas unifamiliares se deberá tener en cuenta que, normalmente, ésta se considerará red exterior y los cables deberán tener aislamiento de polietileno, una cubierta formada por una cinta de aluminio y copolímero de etileno, así como de una capa continua de polietileno colocada por extrusión para formar un conjunto totalmente estanco.
En el caso de viviendas unifamiliares se deberán tener en cuenta que los cables de acometida de uno o dos pares de la red de distribución podrán ser de exterior. En tal caso, deberán llevar como protección metálica una malla de alambre de acero galvanizado.
La red de cables de pares trenzados para la red interior de usuario utilizará como mínimo:

- Cables de cuatro pares de hilos conductores de cobre con aislamiento individual clase E (categoría 6) y cubierta de material no propagador de la llama, libre de halógenos y baja emisión de humos.
- Deberán ser conformes a las especificaciones de la norma UNE-EN 50288-6-1 (Cables metálicos con elementos múltiples utilizados para la transmisión y el control de señales analógicas y digitales.
- Deberán ser conformes a las especificaciones de la norma UNE-EN 50288-6-2 (Cables metálicos con elementos múltiples utilizados para la transmisión y el control de señales analógicas y digitales. Especificación intermedia para cables sin apantallar aplicables hasta 250 MHz.

Cables para instalaciones en el área de trabajo y cables para conexionado).
La red de cables coaxiales para la red interior de usuario utilizará como mínimo cables que serán del tipo RG-59 y cumplirán los requisitos de dimensiones, características eléctricas y mecánicas especificadas en la normativa ICT.
Para proceder a la conexión de cables se necesita de una serie de elementos auxiliares que proporcionen el servicio. Cuando se trata de la conexión de cables de pares trenzados se necesita una serie de elementos mínimos como son:

- El panel para conexión de cables de pares trenzados.
- La roseta para cables de pares trenzados.
- Los conectores para cables de pares trenzados.
- Las bases de acceso de los terminales.

El panel de conexión para cables de pares trenzados, en su punto de interconexión alojará tantos puertos como cables constituyen la red de distribución. Cada uno de estos puertos, tendrá un lado preparado para conectar los conductores de cable de la red de distribució. y el otro lado estará formado por un conector hembra miniatura de 8 vías (RJ45). De esta forma se permitiría la conexión de los cables de acometida de la red de alimentación o de los latiguillos de interconexión. Los conectores cumplirán la norma UNE-EN 50173-1 (Tecnología de la información. Sistemas de cableado genérico. Parte 1: Requisitos generales y áreas de oficina).
El panel que aloja los puertos indicados será de material plástico o metálico, permitiendo la fácil inserción-extracción en los conectores y la salida de los cables de la red distribución.

El conector de la roseta de terminación de los cables de pares trenzados será un conector hembra miniatura de 8 vías (RJ45) con todos los contactos conexionados. Este conector cumplirá las normas UNE-EN 50173-1 (Tecnología de la información. Sistemas de cableado genérico. Parte 1: Requisitos generales y áreas de oficina).

Las diferentes ramas de la red interior de usuario partirán del interior del PAU equipados con conectores macho miniatura de ocho vías (RJ45). Deberán cumplir la norma UNE-EN 50173-1 (Tecnología de la información. Sistemas de cableado genérico. Parte 1: Requisitos generales y áreas de oficina).

Las bases de acceso de los terminales estarán dotadas de uno o varios conectores hembra miniatura de ocho vías (RJ45) y deberán cumplir también lo establecido en la norma UNE-EN 50173-1 (Tecnología de la información. Sistemas de cableado genérico. Parte 1: Requisitos generales y áreas de oficina).

Para la conexión de la red de cables pares también se necesitan una serie de elementos como son:

- Las regletas de conexión
- La roseta para cables de pares.

Las regletas de conexión para cables de pares estarán constituidas por un bloque de material aislante provisto de un número variable de terminales. Cada uno de estos terminales tendrá un lado preparado para conectar los conductores de cable, y el otro lado estará dispuesto de tal forma que permita la conexión de los cables de acometida o de los hilos puente.

El sistema de conexión será por desplazamiento de aislante, y se realizará la conexión mediante las herramientas especiales necesarias para no provocar daños en la instalación. En el punto de interconexión la capacidad de cada regleta será de 10 pares y en los puntos de distribución como máximo de 5 ó 10 pares. En el caso de que ambos puntos coincidan, la capacidad de la regleta podrá ser de 5 ó de 10 pares. Las regletas de interconexión y de distribución estarán dotadas de la posibilidad de medir hacia ambos lados sin levantar las conexiones.

El conector de la roseta de terminación de los pares de la red de dispersión en el PAU, situado en el registro de terminación de red, será un conector hembra miniatura de ocho vías (RJ45) en el que, como mínimo, estarán equipados los contactos centrales 4 y 5. La realización mecánica de estos conectores roseta podrá ser individual o múltiple