ESPECIALIDAD FORMATIVA
GESTIÓN DE REDES DE VOZ Y DATOS

IFCM0310

UF1869: Análisis del mercado de productos de comunicaciones

* Bibliografía usada en este documento:

UF1869: Análisis del mercado de productos de comunicaciones, Autor: Gopal Bijani Chiquero, EDITORIAL ELEARNING S.L. Edición: 6.1

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

Luis Orlando Lázaro Medrano

Contenido

La finalidad de esta Unidad Formativa es conocer los diferentes productos de comunicaciones, para ello se hará una introducción a las comunicaciones y redes computadoras, se recordará los principales principios acerca de la transmisión de datos y posteriormente nos centraremos en medios de transmisión guiados e inalámbricos, control de enlace de datos, protocolos y equipos de interconexión de red.
Al finalizar esta Unidad Formativa aprenderás a:

- ⇨ Diferenciar las características de los medios de transmisión existentes en el mercado.
- ⇨ Conocer los niveles existentes en el conjunto de protocolos TCP/IP.
- ⇨ Conocer las características técnicas y el modo de funcionamiento de los diferentes equipos de interconexión de red.

1. Introducción a las comunicaciones y redes de computadoras

1.1. Tareas de un sistema de telecomunicaciones

En primer lugar, definiremos lo que es telecomunicación, que no es más que un término que se refiere a toda comunicación que se quiera establecer a larga distancia empleando para ellos diversos medios físicos y técnicos.
Definimos un sistema de telecomunicación, como una colección de elementos hardware y software perfectamente entrelazado y capaz de enviar y/o comunicar datos o información de un punto a otro.
Estos sistemas pueden transportar textos, videos, imágenes, voz, archivos, etc.
Como todo sistema, el sistema de telecomunicaciones está compuesto de una serie de elementos:

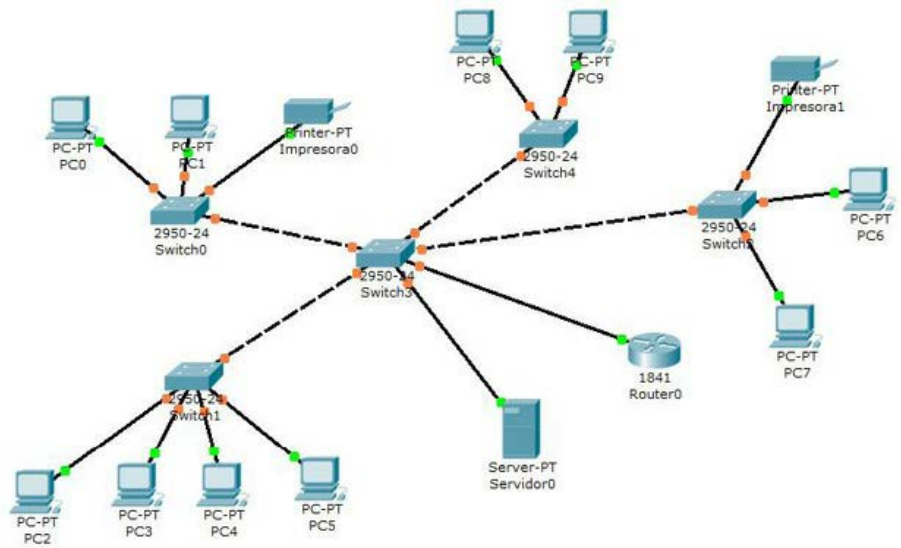
- Elementos **hardware**:
  Conjunto de elementos físicos como equipos electrónicos, ordenadores, controladores, elementos de interconexión, etc.
- Elementos **software**:
  Conjunto de programas y aplicaciones que controlan todo el proceso y permiten la comunicación.
- Medio de **transmisión**:
  Es el canal (bien aire, agua o cables) por el que se transmite la información.
- **Protocolos**:
  Conjunto de reglas y normativa que permite la interoperabilidad de todos los componentes del sistema para permitir la comunicación.
- **Proveedores** de comunicación:
  Conjunto de operadores de telecomunicaciones que ofrecen sus servicios o medios para permitir la comunicación de un lugar a otro

1.2. Comunicación a través de las redes

Una red se define como un conjunto de equipos o elementos interconectados entre sí por algún medio de transmisión.

El ejemplo más típico es una red de ordenadores en la cual se interconectan diferentes PC o equipos informáticos mediante uno o varios enlaces de transmisión.

También existen numerosas redes como redes de telefonía móvil, redes de datos, redes de televisión, etc. Todas ellas comparten los mismos conceptos de redes



1.2.1. Clasificación a través de las redes

Las redes de ordenadores se pueden clasificar atendiendo a muchos criterios, pero uno de los más populares es el ámbito físico que ocupan.
Según el espacio que ocupan o ámbito podemos distinguir:

Redes de área local (LAN)

Son redes de propiedad privada, de hasta unos cuantos kilómetros de extensión. Por ejemplo una oficina o un centro educativo.
Se usan para conectar ordenadores personales o estaciones de trabajo, con objeto de compartir recursos e intercambiar información

Redes de área metropolitana (MAN)

Las redes metropolitanas son redes de ordenadores de un tamaño superior a las LAN, abarcando generalmente ciudades con un radio de unos 10 – 15 km. Son típicas de empresas y organizaciones privadas o públicas que quieren interconectar sus equipos ubicados en diferentes oficinas o sedes en diferentes emplazamientos.
También son las empleadas por los operadores de telecomunicaciones locales para ofrecer sus servicios a empresas.

Redes de área extensa (WAN)

Son redes que se extienden sobre un área geográfica extensa, generalmente mundial. Consisten en un conjunto de nodos o de redes LAN interconectadas entre sí formando una gran red.
El ejemplo más claro es Internet, que no es más que un conjunto de redes LAN y MAN interconectadas.
En este tipo de redes existen en una serie de equipos dedicados a ejecutar aplicaciones de los usuarios, es decir, son los denominados Hosts. Para ello se emplean equipos de interconexión o encaminadores como router o módems.
Cada host estará conectado a uno de estos equipos de interconexión que se encargará de enviar la información por la red.
Una WAN contiene numerosos cables conectados a un par de encaminadores. Si dos encaminadores que no comparten cable desean comunicarse, han de hacerlo a través de encaminadores intermedios.
El paquete se recibe completo en cada uno de los intermedios y se almacena allí hasta que la línea de salida requerida esté libre: redes de área local.

1.3. Protocolos y arquitecturas de los protocolos

Las redes de comunicaciones, como veremos a continuación, se rigen por una serie de protocolos y arquitecturas donde se definen cómo se debe diseñar y la topología que tienen.
Los protocolos regulan cómo se debe realizar la interconexión e interfaces entre los diferentes elementos que componen una red de comunicaciones.
La arquitectura define la topología de la red de comunicaciones, así como su estructura y mantenimiento.
Ambos protocolos y arquitectura son imprescindibles para cualquier red de comunicaciones.

1.3.1. Definición y características

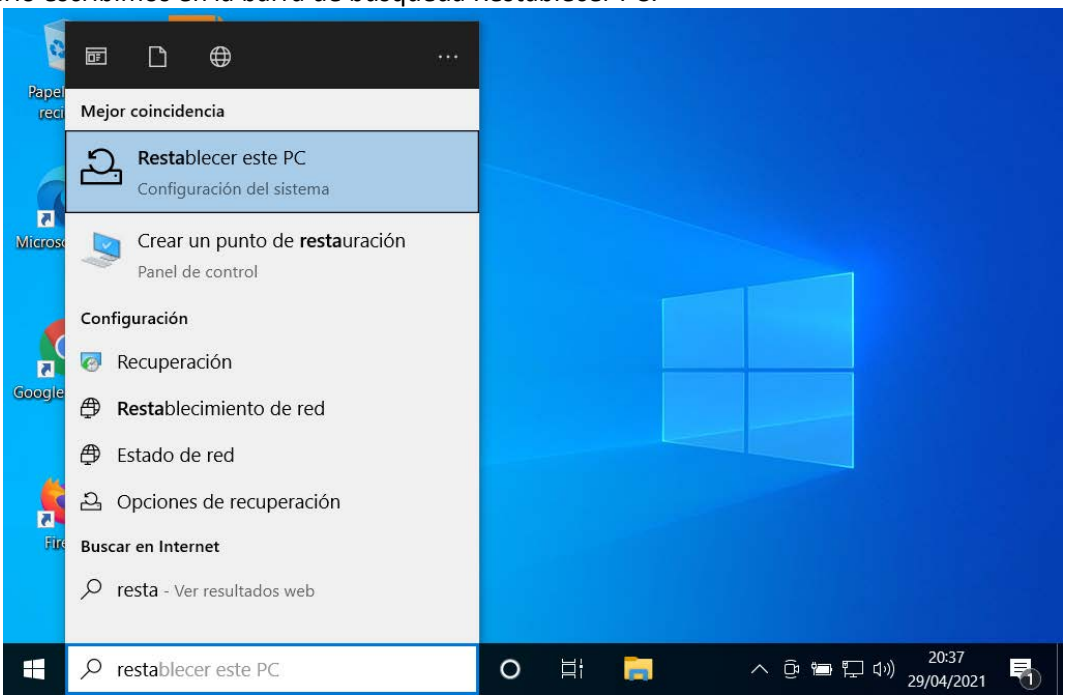
Los protocolos son un conjunto de normas o reglas que se utilizan en los sistemas de comunicaciones para su correcto funcionamiento.
Debido a la gran complejidad que conlleva la interconexión de ordenadores, se han tenido que dividir todos los procesos necesarios para realizar las conexiones en diferentes niveles.
Cada nivel se ha creado para dar una solución a un tipo de problema particular dentro de la conexión.
Cada nivel tendrá asociado un protocolo, el cual entenderán todas las partes que formen parte de la conexión.
Las empresas han dado diferentes soluciones a la conexión entre ordenadores, implementando distintas familias de protocolos, y dándoles diferentes nombres (DECnet, TCP/IP, IPX/SPX, NETBEUI, etc.).

Preparar PC

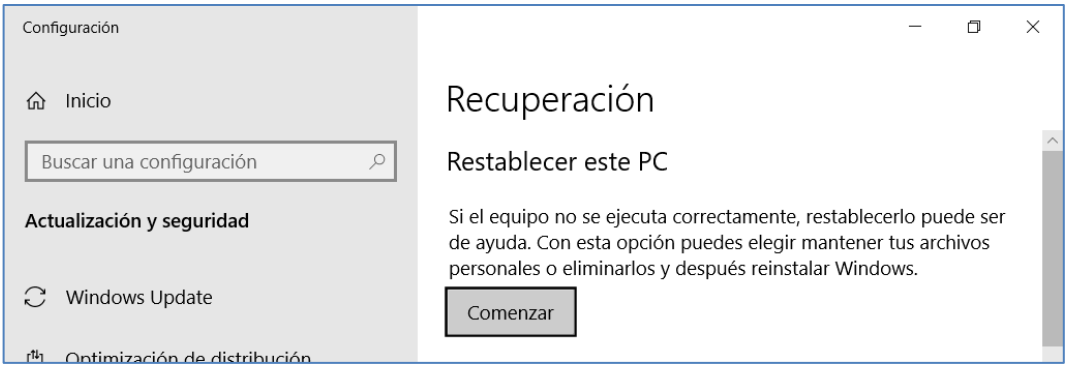
Restablecer PC

Vamos a empezar el curso dejando limpio el ordenador que vamos a usar durante todo el curso, para lo cual vamos a restablecer el PC. Este proceso lo que hace es borrar todos los documentos, archivos… y volver a reinstalar el sistema operativo, en nuestro caso Windows 10 Professional.

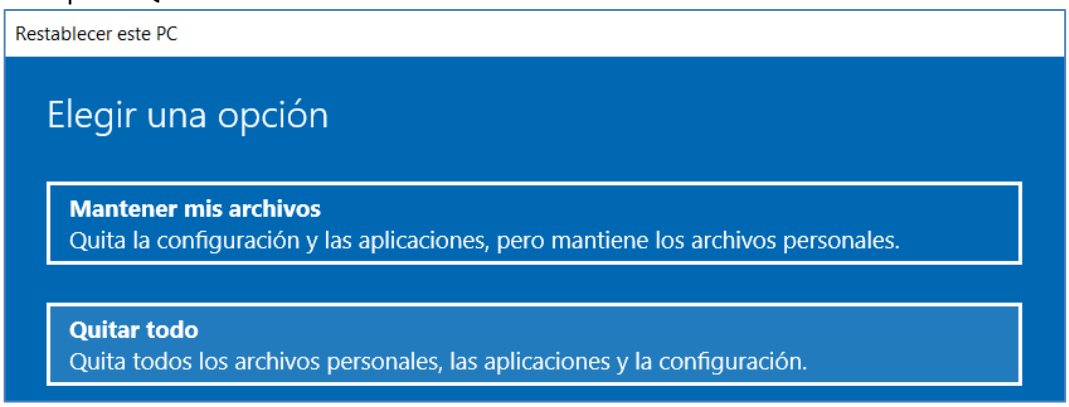
Para hacerlo escribimos en la barra de búsqueda Restablecer PC:



Luego pulsamos sobre **Comenzar**



Y elegimos la opción **Quitar todo**



Y pulsamos sobre **Restablecer**…

Máquinas virtuales

Con el PC limpio vamos a preparar el entorno de trabajo, antes de montar una red con otros ordenadores, vamos a crear una red en nuestro propio ordenador usando máquinas virtuales, para hacer pruebas….
Una máquina virtual es una emulación software de un equipo informático tal y como si se tratara de uno real. De esta manera, buscando un nodo que funcione correctamente podemos hacer que ejecute una máquina virtual con la configuración precargada del recurso que se ha caído y así solventar temporalmente la caída de este hasta poder darle una solución correcta. Esta solución implica más carga de trabajo sobre dicho nodo o equipo, con lo cual dotarle de una correcta configuración hardware y software es vital.
Una máquina virtual, pese a ser una emulación, consume recursos del equipo que la emula como si de un ordenador real se tratara, con lo cual hay que dotar al ordenador que ejecuta máquinas virtuales de una buena configuración hardware.
Es como montar varios ordenadores dentro del nuestro, estos ordenadores consumirán los recursos de nuestro ordenador, es decir si tenemos un equipo con varios procesadores (núcleos), 16 Gb de RAM y 500 Gb de disco duro, si montamos 2 máquinas virtuales con 1 procesador +4Gb de RAM+80Gb de disco duro, nuestra máquina física (real) cuando estén trabajando las máquinas virtuales se queda con 8Gb de RAM y 340Gb de disco duro.
Para manejar las máquinas virtuales necesitamos un programa que las administre, en nuestro caso vamos a usar **VirtualBox** por ser gratuito y muy sencillo de usar.

Descarga e Instalación de Virtual Box

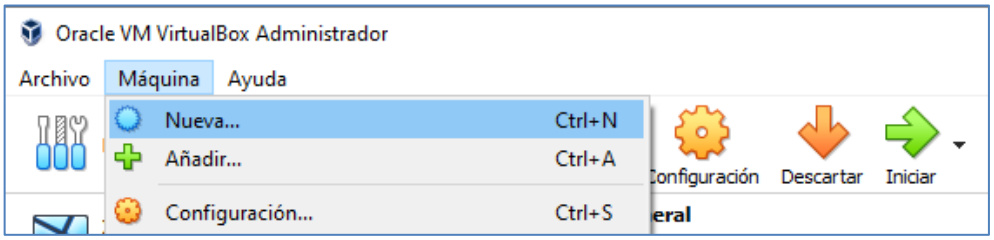
Vamos a la página del fabricante y descargamos la última versión estable para Windows hosts y la instalamos: https://www.virtualbox.org/wiki/Downloads

Creación de la Máquina Virtual Windows 10 – Servidor Web

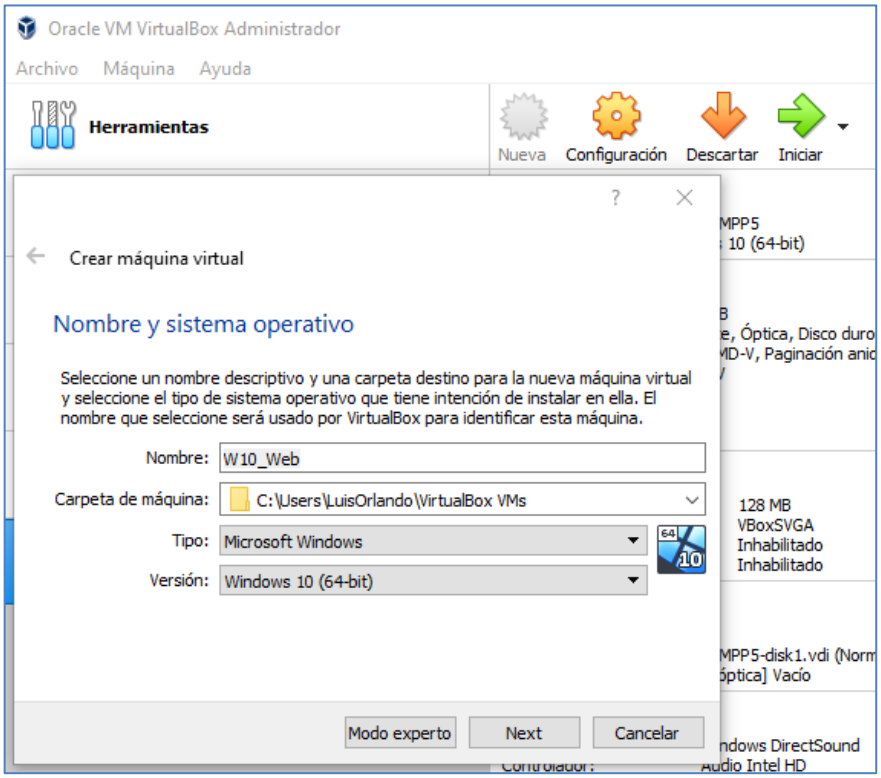
Para empezar a trabajar con una red de ordenadores que usen algún tipo de servicio compartido vamos a crear un servidor web, porque es muy sencillo de configurar y además es muy gráfico ver cómo podemos acceder a los equipos de los compañeros para ver su contenido compartido, en este caso páginas web… veremos como apagar encender servicios y que dejen de estar disponibles…

Este servidor web estará ubicado en una máquina virtual con Windows 10 y le daremos 4 Gb de RAM y 80Gb de disco duro dinámico (es decir que se irá ocupando a medida que nos haga falta).

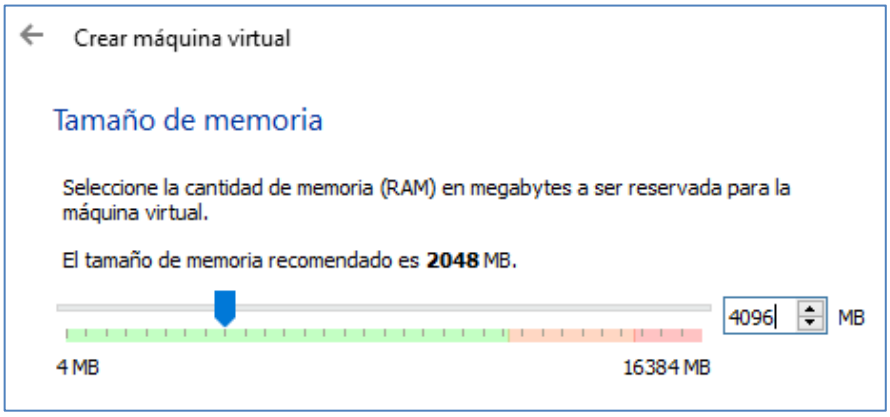
Abrimos Virtual Box y pulsamos sobre el botón **Nueva…** que está accesible en la barra de herramientas o en el menú **Máquina/Nueva…**



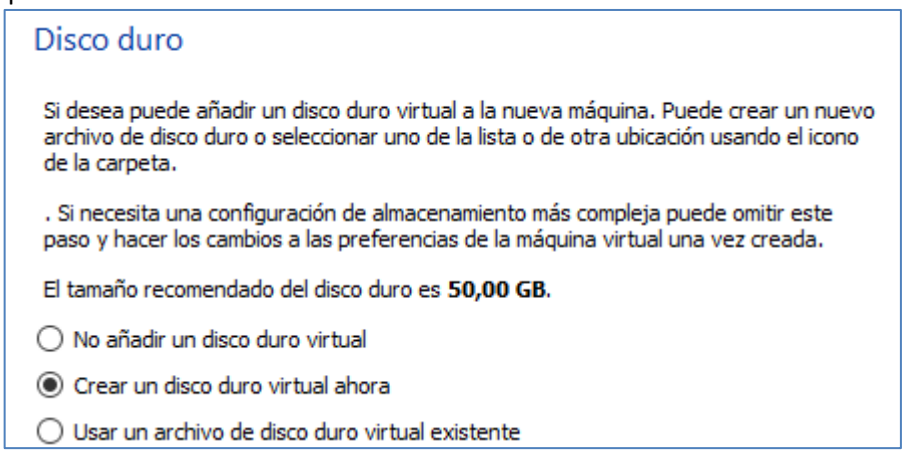
Le llamamos **W10_Web** y pulsamos sobre **Next**



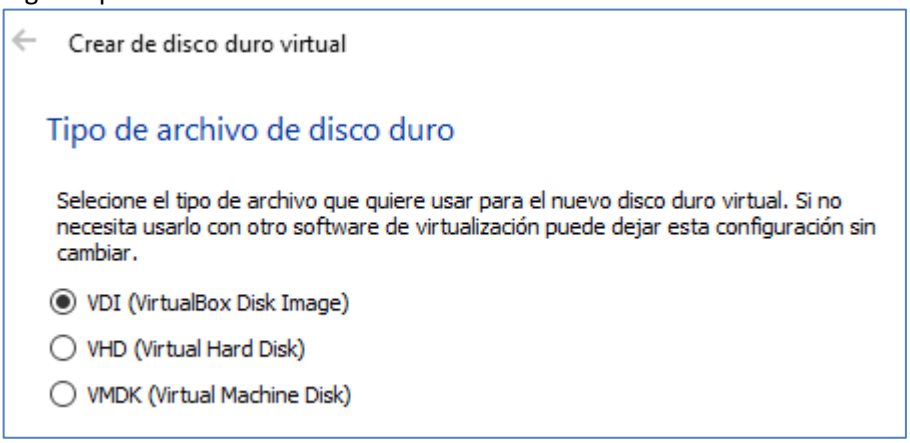
Le asignamos el tamaño de la memoria RAM, en este caso **4Gb ⇨ 4096 MB**



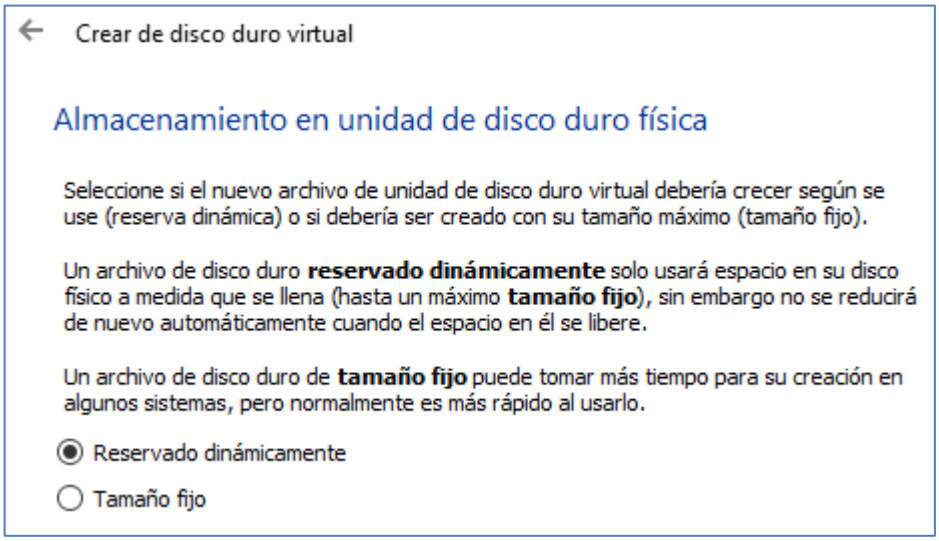
Le decimos que queremos crear un **Disco Duro** virtual nuevo

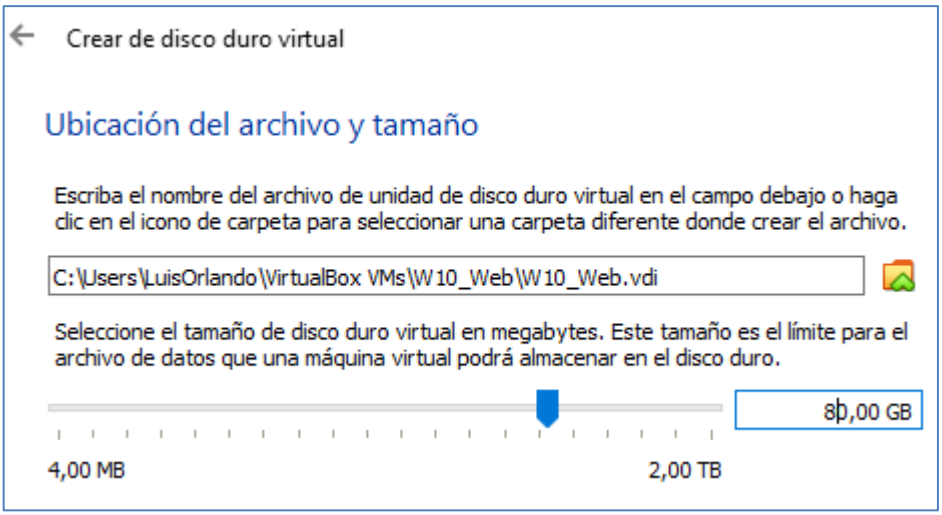


Elegimos el **Tipo de archivo del disco duro Virtual**, ahora mismo este paso nos da igual un tipo u otro, pero más adelante cuando queramos navegar por el disco duro virtual desde fuera o queramos compartirlos tendremos qie elegir el que nos interese en cada momento:

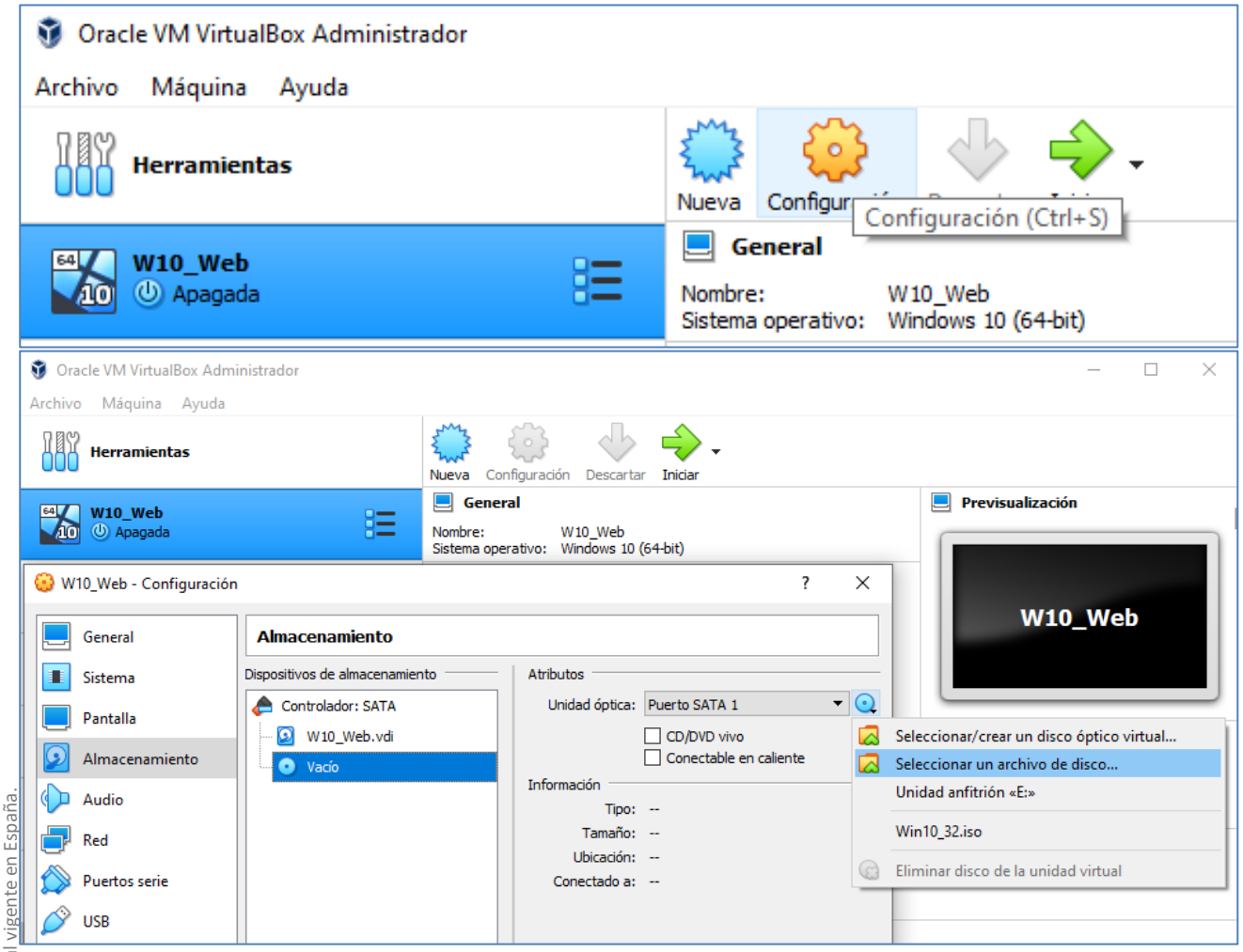


El tamaño será **dinámico**, es decir se irá llenando a medida que se vaya ocupando en la máquina virtual:





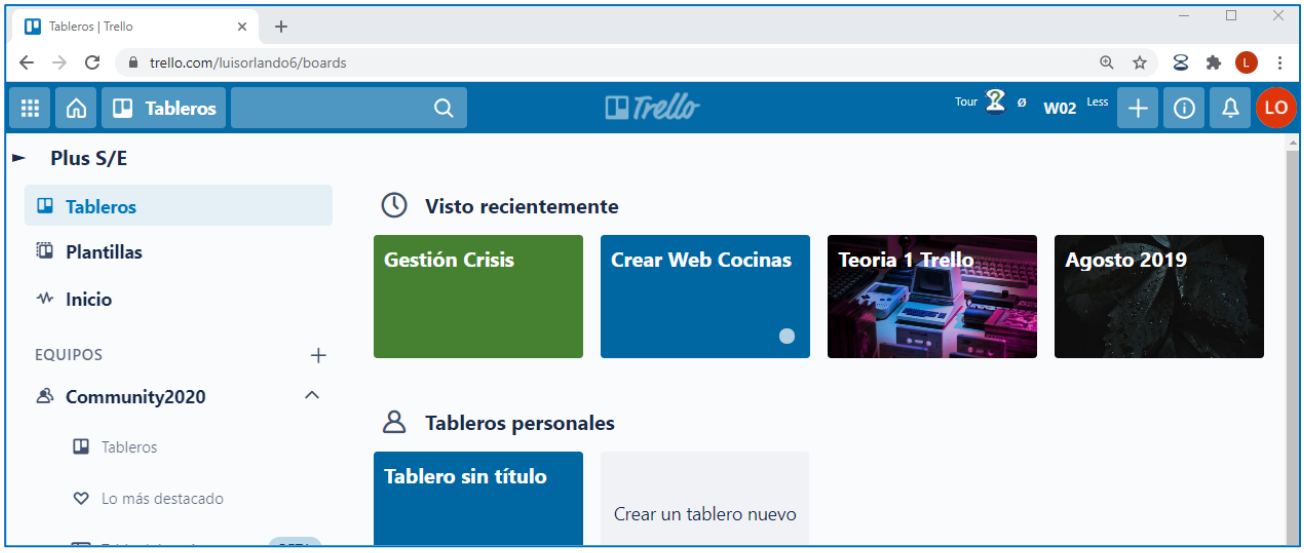
Con la máquina "vacía" creada, vamos a instalar Windows 10 para lo cual tenemos que descargar la imagen ISO del Windows 10, en el siguiente enlace explica como hacerlo
https://www.adslzone.net/esenciales/windows-10/descargar-imagen-iso-windows-10/
Luego cambiamos la **Configuración** de la máquina virtual para que use como unidad de CD/DVD la imagen ISO que nos hemos descargado



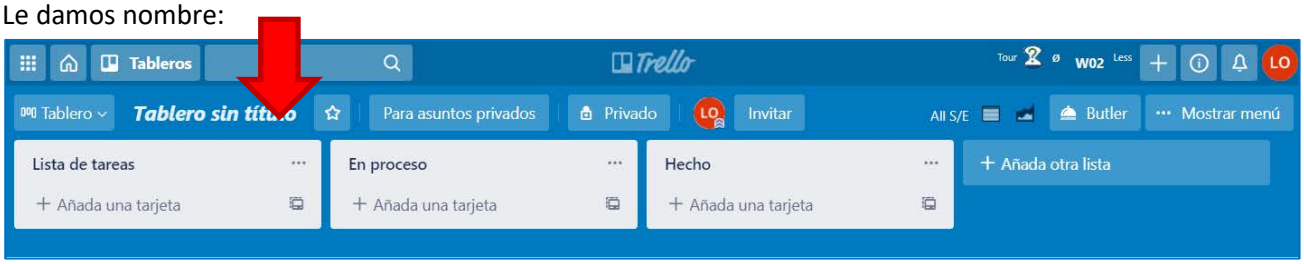
Primer Proyecto – Creación y puesta en Marcha Sitio Web

Tableros colaborativos con Trello

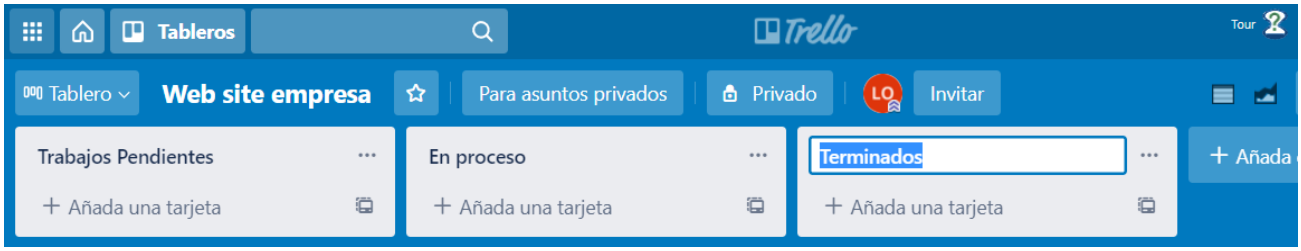
Son espacios virtuales donde distintos usuarios pueden compartir información, imágenes, y vídeos. Nosotros vamos a usar **Trello**. Nos damos de alta en Trello.com Pulsamos sobre el apartado **Tableros** y creamos uno nuevo pulsando sobre la opción **Tablero sin título** de Tableros Personales



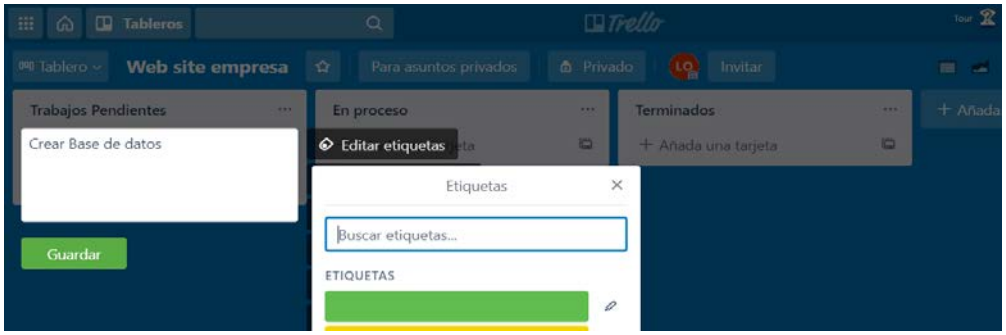
Le damos nombre:



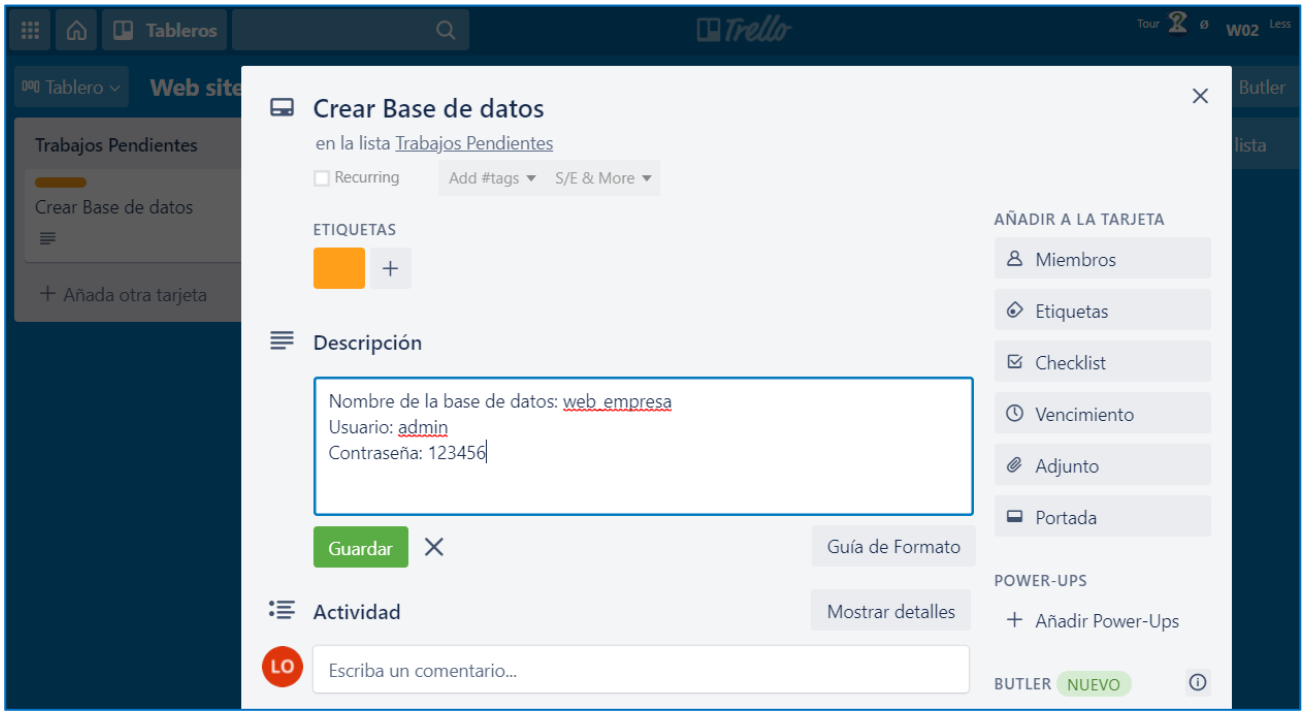
Y podemos ir añadiendo Tarjetas (tareas) a las Listas existentes: Lista de Tareas ➔En Proceso ➔Hecho
Crear nuevas Listas, o incluso cambiar el nombre de las Listas existentes, simplemente haciendo doble clic sobre el texto de las mismas.



Para crear Tarjetas simplemente hacemos click sobre: "+ Añada una tarjeta" y le ponemos un texto resumen. Si hacemos clic con el botón derecho podemos darle un color distintivo (Editar etiquetas) …



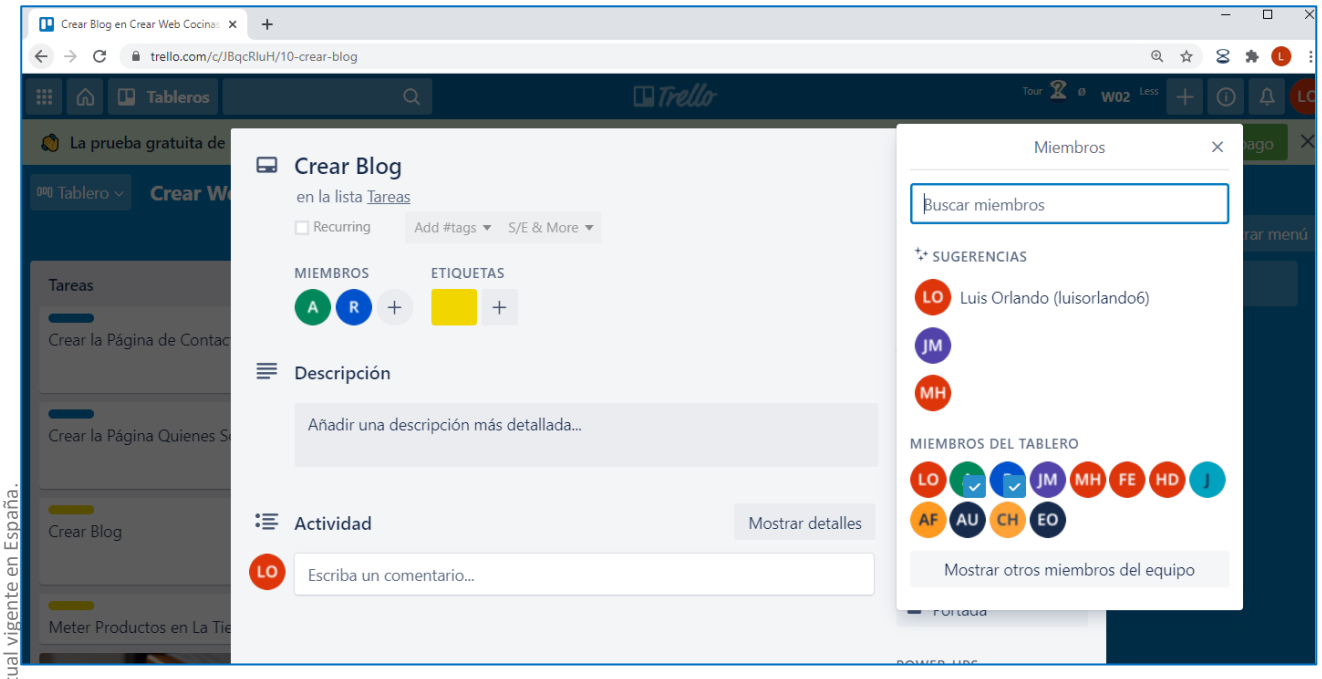
Y si hacemos clic sobre la tarea, podemos añadir más información, como Descripción, Vencimiento, meter adjuntos… incluso podemos añadir palabras claves (tags) y vemos la Actividad que ha tenido la Tarea:



Podemos asignar más de una Etiqueta (colores) por tipos de tareas… y cuando las vamos terminando simplemente las arrastramos de una Lista a otra: Pendiente ➔En Proceso ➔ Terminadas

También podemos crear Equipos de trabajo e invitar a usuarios de Trello al Equipo, pulsando sobre el "+" a la derecha de EQUIPOS y una vez dentro pulsando sobre **Invitar a miembros del equipo**

Así cuando creemos un tablero podemos decirle que pertenece a un Equipo y asignar Tareas a las personas que forman parte de él, haciendo clic sobre cada tarea:



Para borrar tareas haremos click con el botón derecho y pulsaremos sobre archivar y cuando hayamos terminado un tablero podemos archivarlo (eliminarlo) pulsando sobre **Mostrar Menu/…Mas** y luego sobre **Cerrar Tablero**

Crear sitio web con WordPress

WordPress es un CMS, sus siglas en ingles son Content Management System o "traducido" un Sistema de Gestión de Contenidos para Páginas Web, es decir un software desarrollado para que cualquier usuario pueda administrar y gestionar contenidos de una web con facilidad y sin conocimientos de programación Web.

Los CMS más importantes se pueden dividir en dos grandes grupos:

CMS para páginas web:

- ⇨ WordPress
- ⇨ Drupal
- ⇨ Joomla

CMS para tiendas on-line:

- ⇨ Prestashop
- ⇨ WordPress + WooCommerce
- ⇨ Magento

Y como WordPress es el más usado y es muy sencillo de utilizar he decidido explicaros como crear un sitio web mediante este gestor de contenidos.

Servidor Web

Antes de seguir tenemos que entender lo que es un **sitio web**, que básicamente es un conjunto de páginas web, imágenes, vídeos… alojados en un servidor web. Un **servidor**, como la misma palabra indica, es un ordenador o máquina informática que está al "servicio" de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a estos, todo tipo de información.

Y como estamos hablando de un servidor web, pues lo que sirve son páginas web, que básicamente son documentos donde los usuarios pueden acceder a informaciones con texto, videos, imágenes, etc y navegan a través de enlaces o hipervínculos a otras webs. Estos documentos también se llaman páginas de hipertexto o html (HyperText Markup Language o lenguaje de marcas de hipertexto), porque contienen texto marcado e hipervínculos, que son enlaces (vínculos) con otras partes del mismo documento o a otros documentos.

Por lo tanto para crear un sitio web lo primero que necesitamos en un servidor web, dónde alojar el sitio, podríamos usar uno de tantos servidores web gratuitos que tenemos en el mercado o instalar un servidor web local, que es usar nuestro ordenador como servidor de páginas web.

Para convertir nuestro ordenador en un servidor tenemos que instalar un programa. En nuestro caso WordPress trabaja con un lenguaje llamado PHP, y existe un servidor gratuito llamado Apache que administra este tipo de páginas. Además cuando vallamos creando las páginas las irá guardando un una base de datos con lo cual también necesitaremos instalar la base de datos que usa WordPress: MySQL o MariaDB… bueno todo esto que parece tan complicado es más sencillo de lo que parece, ya que existe un "paquete" de código abierto, que contiene todo lo que necesita WordPress y se llama XAMPP.

Descargar Programas

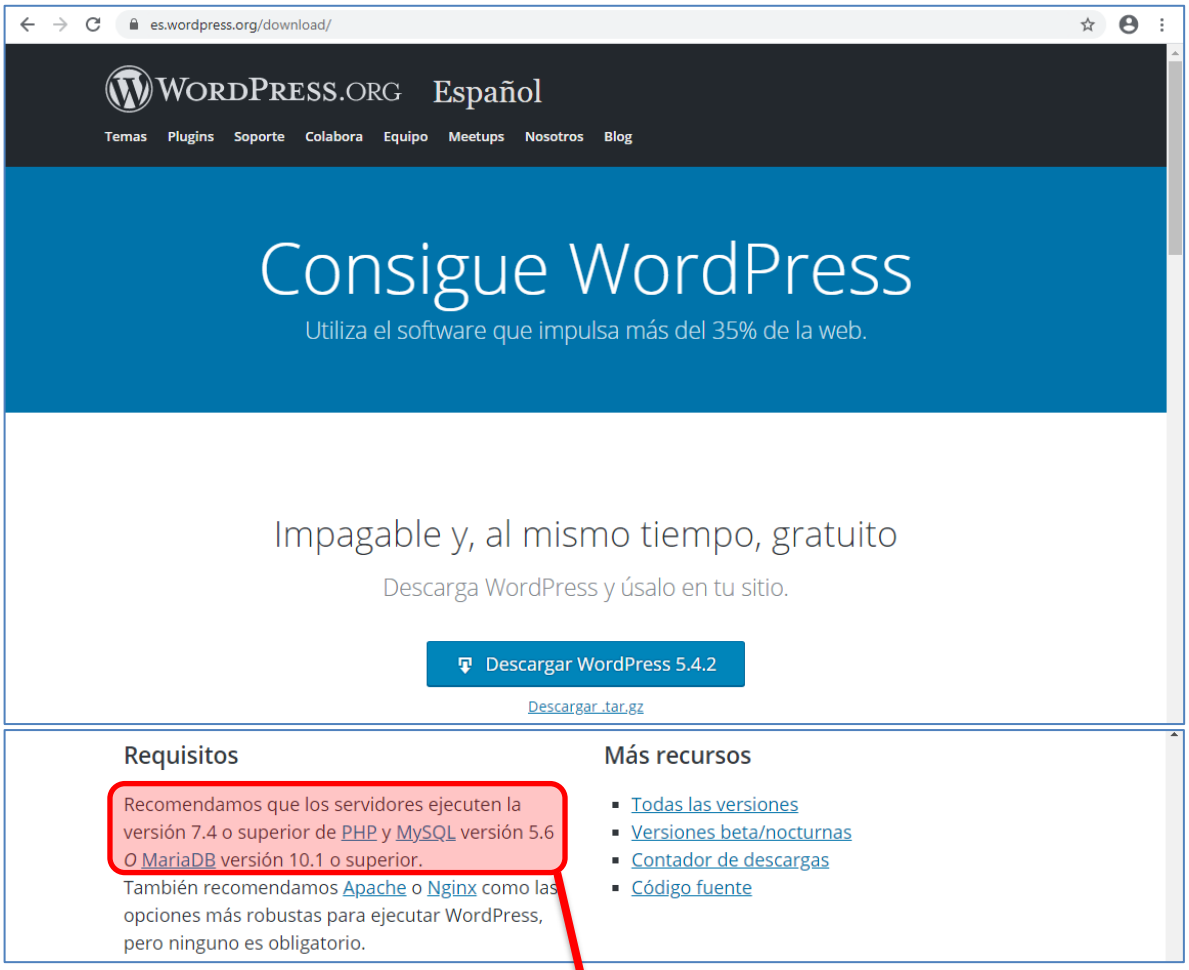
Dentro de WordPress hay dos sitios y sistemas diferenciados: ***wordpress.com*** y ***wordpress.org***

Con wordpress.com podemos crear un sitio web sin tener que contratar un hosting. Este sitio web estará alojado en los propios servidores de WordPress. El nombre del dominio estará vinculado a WordPress y tu web será realmente un subdominio.

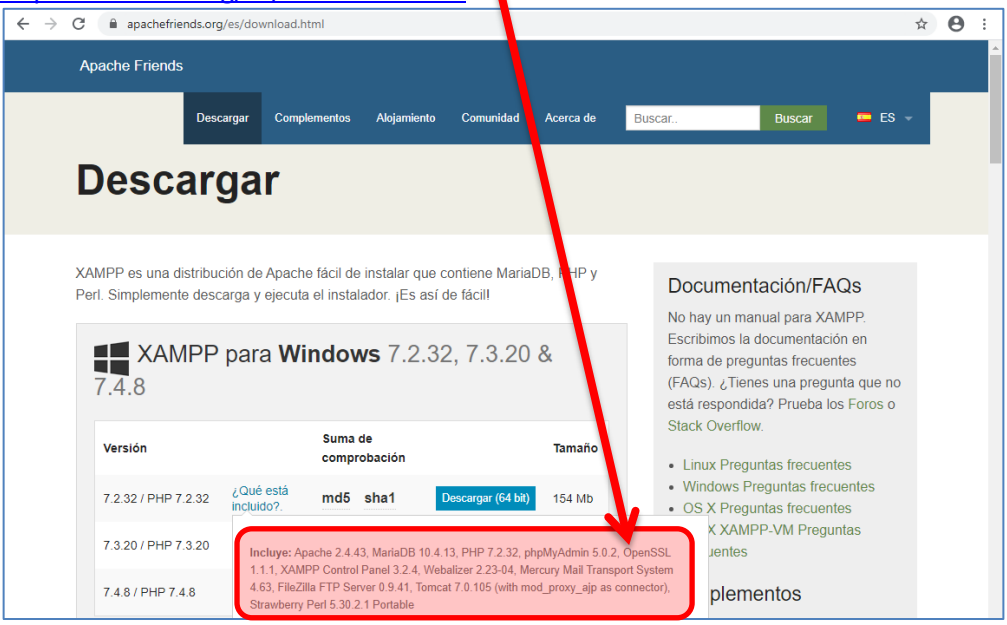
Esta opción es totalmente gratuita, pero también tendrás muchas limitaciones a todos los niveles.

Con wordpress.org podemos crear un sitio web y alojarlo en nuestro propio servidor. En este caso, el dominio no estará ligado a WordPress y tendremos todas las posibilidades que queramos a la hora de crear, personalizar y monetizar nuestra web.

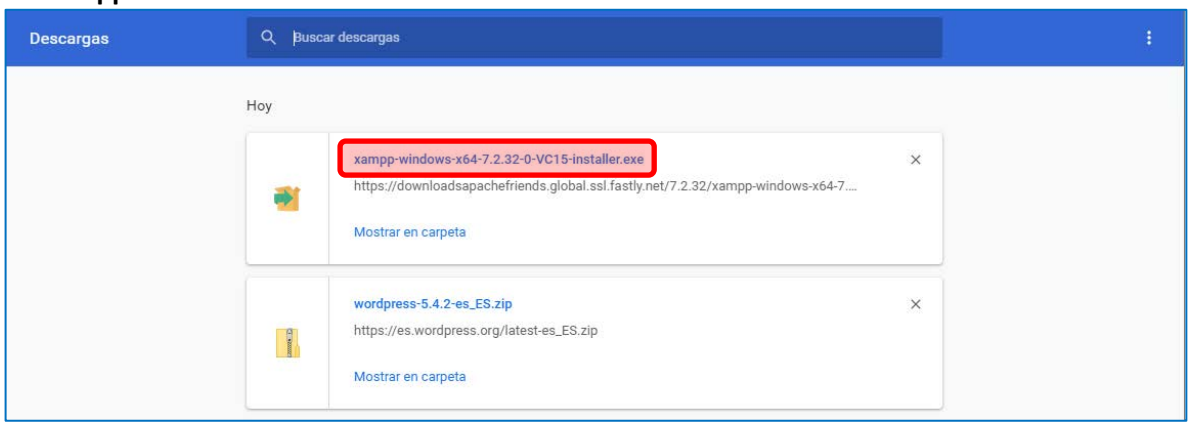
Así que en nuestro caso iremos a la página https://es.wordpress.org/download/ y descargaremos la última versión estable:



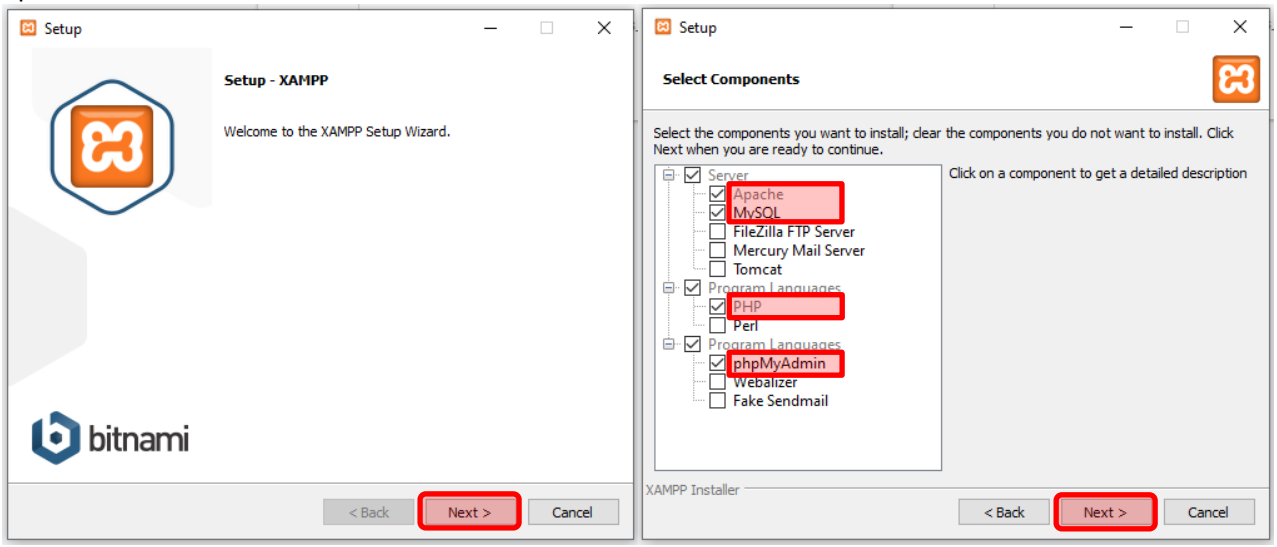
Y luego descargaremos la versión de XAMPP que cumpla con los requisitos de WordPress desde la página: https://www.apachefriends.org/es/download.html



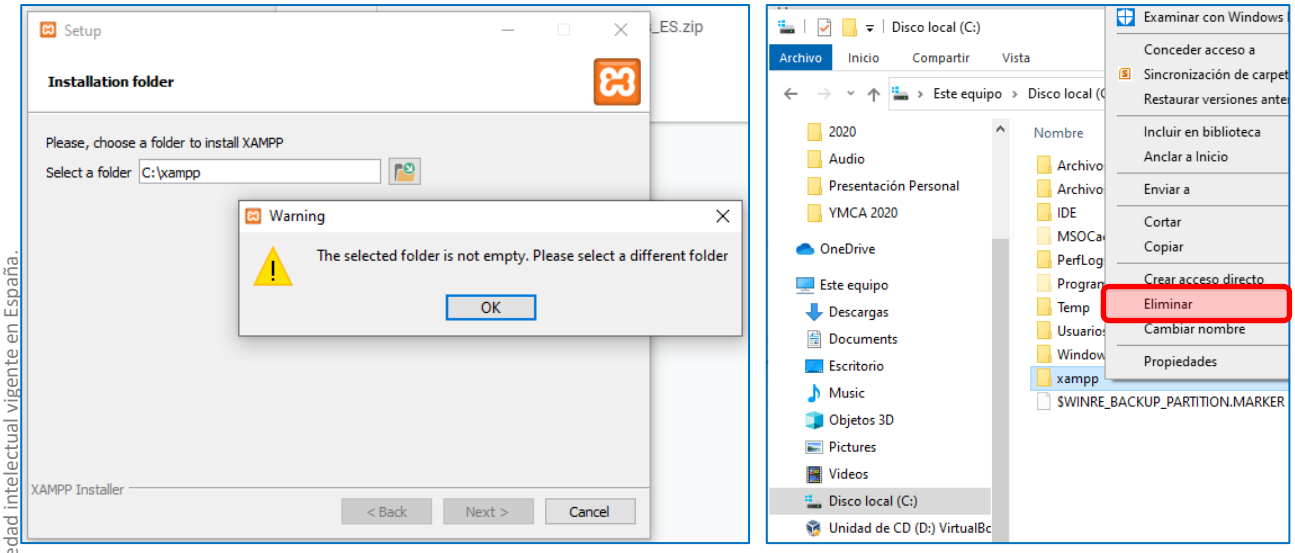
Con los archivos descargados tenemos que instalar primero el servidor web, por lo que ejecutamos el archivo **xampp-windows…**



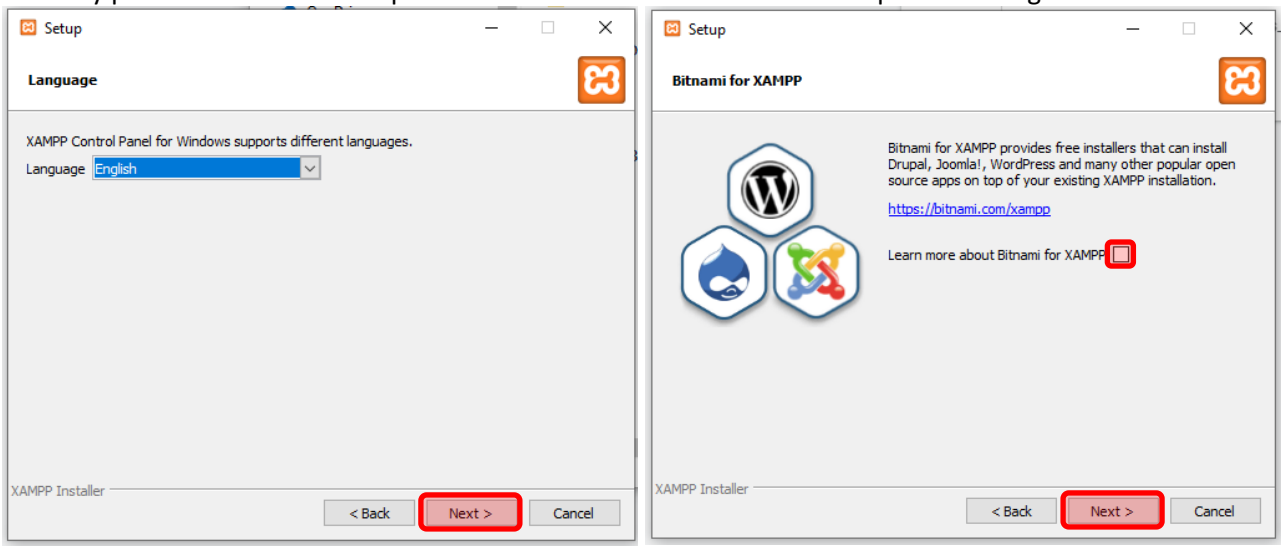
Los pasos son muy sencillos, en la primera pantalla pulsamos sobre **Next >** y en la segunda marcamos solo lo que necesitamos que en este caso es Servidor **Apache**, Base de datos **MySQL**, **PHP** y para que sea más sencillo manejar la base de datos usamos un programa llamado **phpMyAdmin**, así que solo marcamos esas opciones:



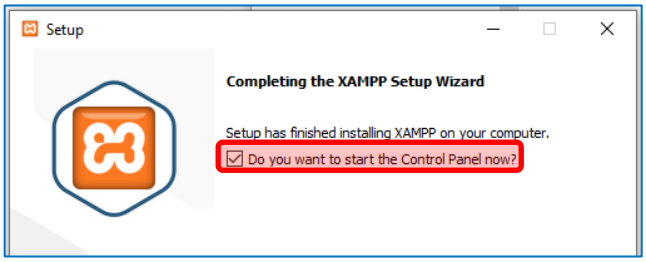
Después nos preguntará en que carpeta de nuestro disco duro queremos instalar xampp, por defecto la dejamos en **c:\xampp** si no nos deja es que puede ser que alguien ya haya instalado xampp con anterioridad, si no queremos mantener la otra instalación basta con que borremos la carpeta y sigamos:



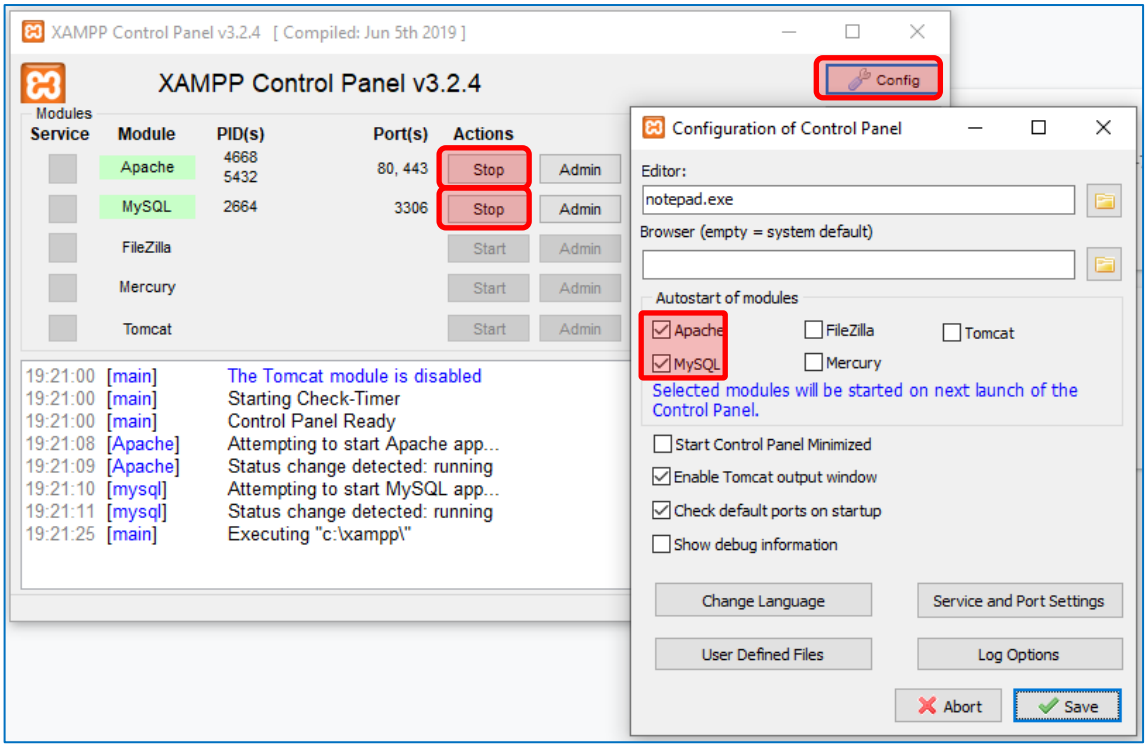
Si no hay ninguna otra instalación simplemente nos dejará seguir.
Luego seleccionamos el lenguaje de los 2 posibles: **Ingles** o Alemán, desactivamos la casilla saber más de Binami y pulsamos sobre **Next >** para comenzar la instalación de XAMPP que llevará algunos minutos.



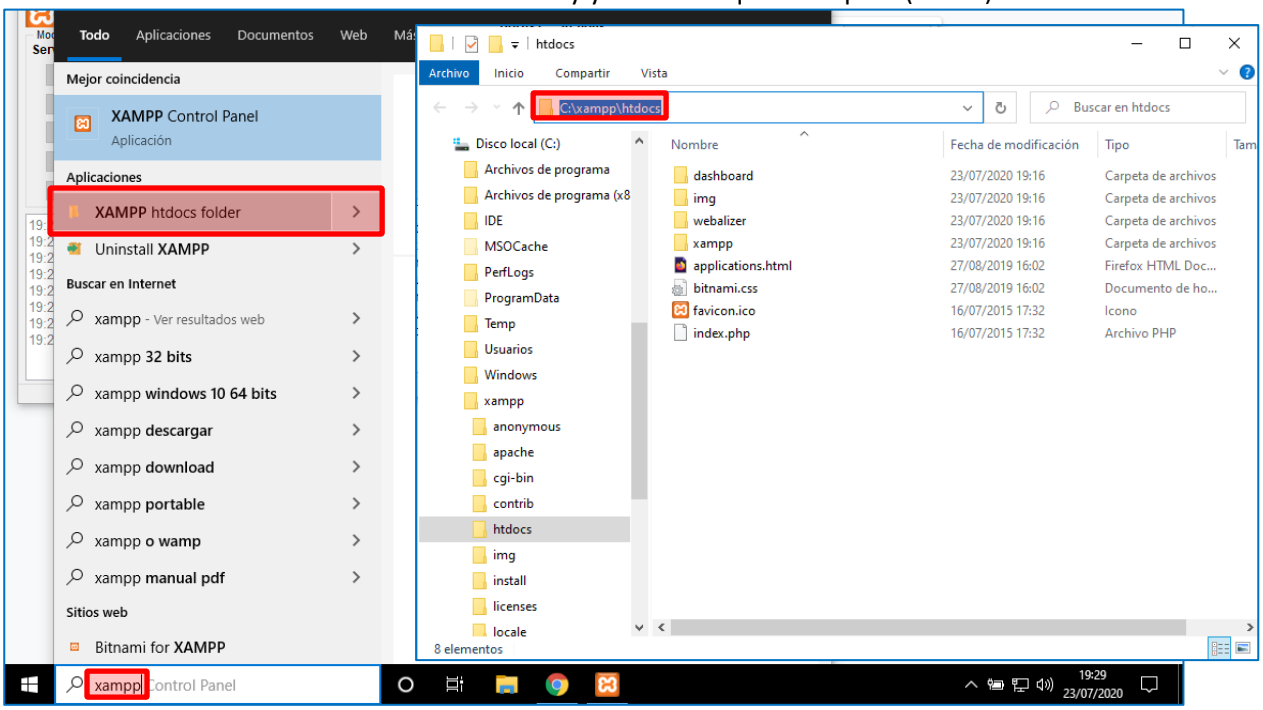
Con la instalación terminada ejecutamos el Panel de control de XAMPP, dejando activada esa casilla de verificación y pulsando sobre el botón **Finish**



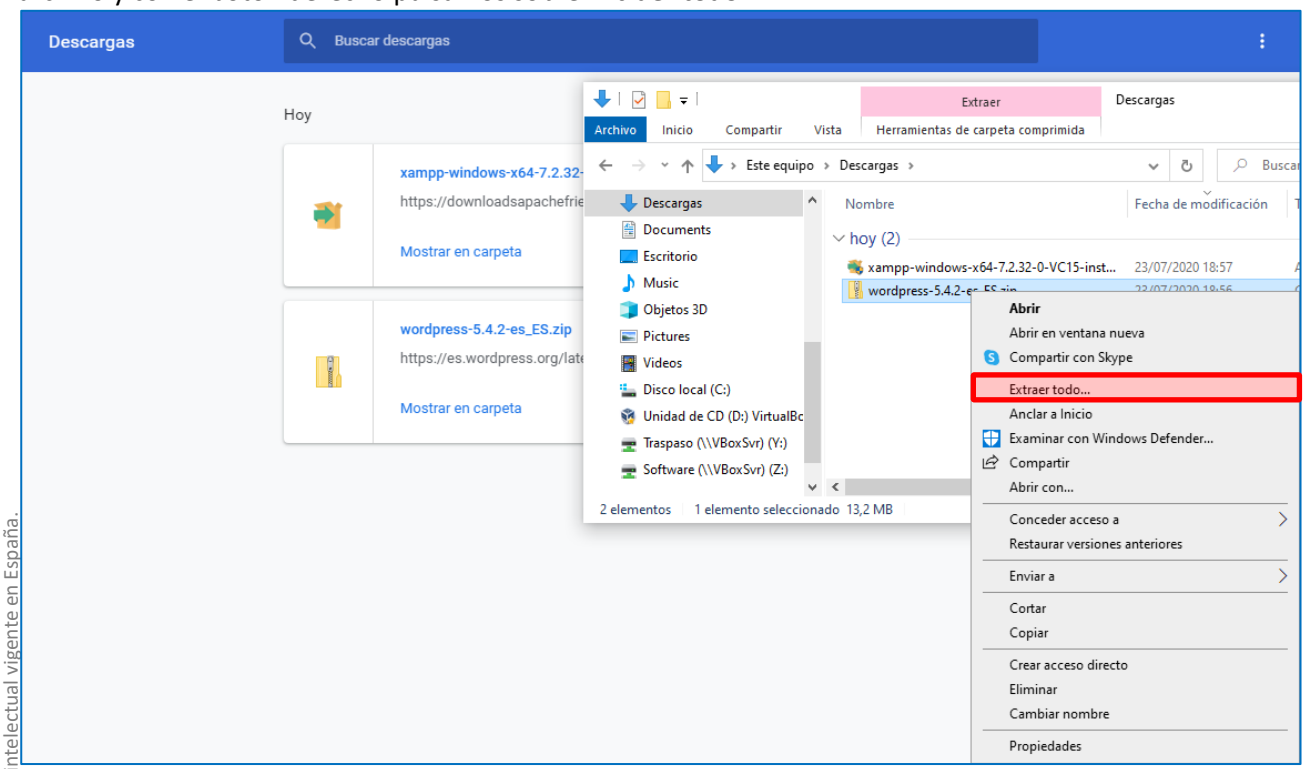
Con el panel de control visible, encendemos los Servicios de Apache (Servidor Web) y el de la Base de datos (MySQL) pulsando sobre los botones **Start** a la derecha de su nombre. Esto "**montará**" el Servidor Web para poder usarlo, y si queremos que se encienda siempre de forma automática pulsamos sobre el botón **Config**:



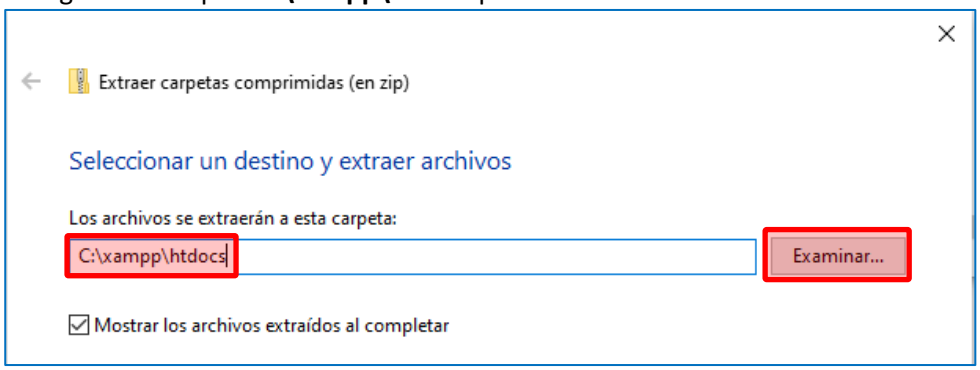
Ahora tenemos que acceder a la carpeta del servidor web "pública" la que podemos ver desde el cualquier navegador, esa carpeta está situada en **c:\xampp\htdocs** si no recordamos su nombre simplemente escribimos **XAMPP** en el buscador de Windows y ya nos dice que la carpeta (folder) de XAMPP es **htdocs**.



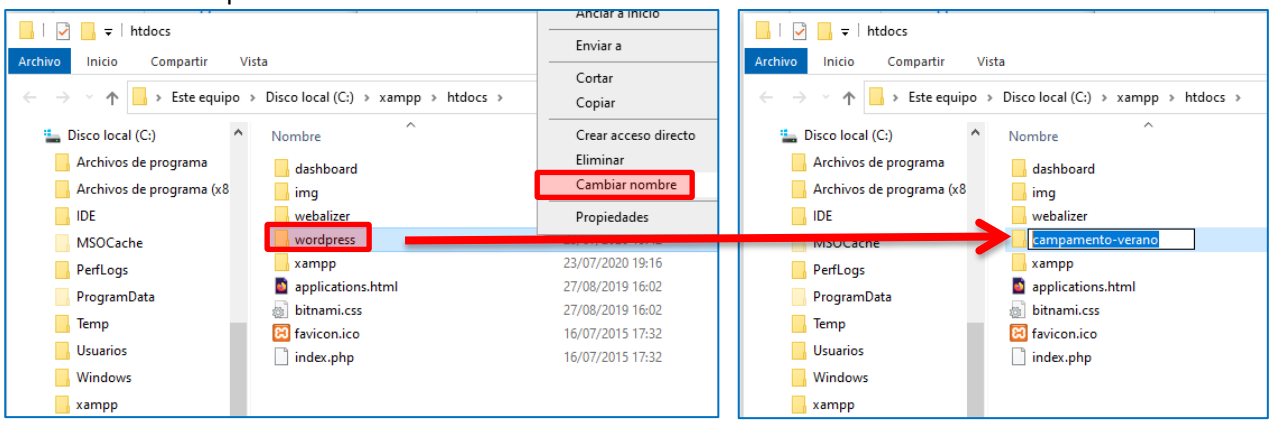
Así que todo lo que *metamos* en esta carpeta podremos verlo desde cualquier navegador.
El siguiente paso es crear nuestro sitio web con WordPress, para hacerlo solo hay que descomprimir el archivo descargado en esa carpeta y le vamos a dar el nombre del sitio que estamos creando, en este caso **campamento-verano**.
Para hacerlo en la página de descargas del navegador abrimos la carpeta donde hemos descargado el archivo y con el botón derecho pulsamos sobre **Extraer todo…**



Y elegimos la carpeta **c:\xampp\htdocs** pulsando sobre el botón **Examinar**

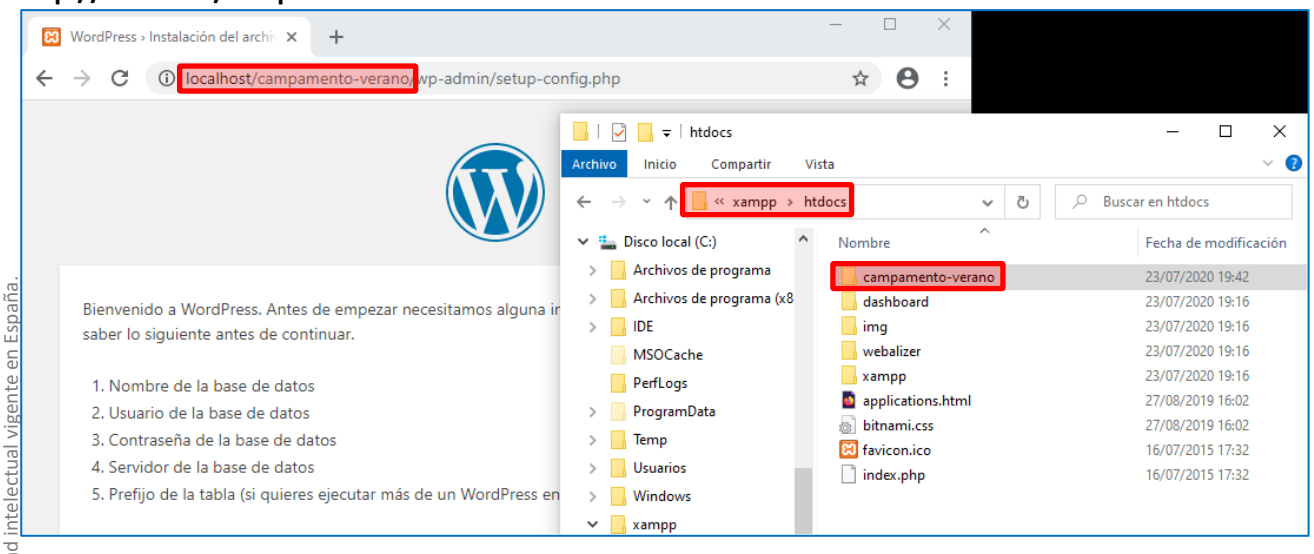


Esto hará que se cree una nueva carpeta llamada **wordpress** dentro de xampp, si vamos a crear más de un sitio web sólo tenemos que seguir los pasos anteriores (extraerlo en la carpeta htdocs), pero crearía un conflicto porque ya existe la carpeta llama wordpress así que Windows lo solucionaría poniéndole como nombre wordpress(1), (2)… así que lo mejor sería cambiarle el nombre de esa carpeta y llamarle por ejemplo campamento-verano, así que hacemos clic con el botón derecho encima de la carpeta y seleccionamos la opción **Cambiar nombre**:

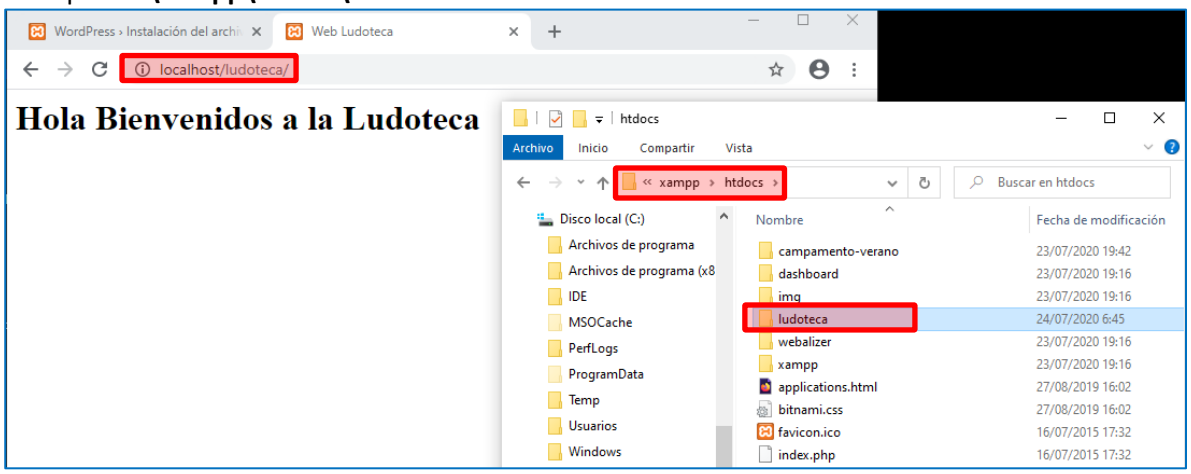


Crear sitio Web

Ahora ya podemos crear la página web, para lo cual abrimos cualquier navegador, si escribimos la dirección del servidor local: **localhost** esto nos lleva hasta la carpeta **c:\xampp\htdocs** como a la carpeta que queremos realmente acceder es a la carpeta **campamento-verano** escribimos entonces **http://localhost/campamento-verano**

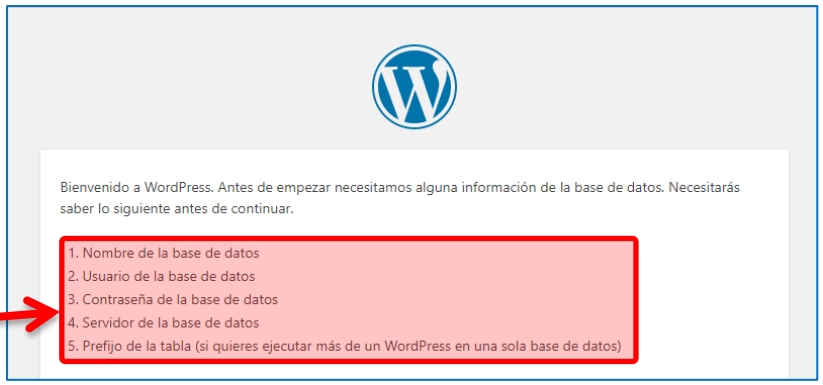


Igualmente, si quisiésemos crear otro sitio llamado ludoteca seguiríamos los pasos anteriores y accederíamos al sitio web a través del navegador escribiendo **http://localhost/ludoteca** y eso nos llevaría a la carpeta **c:\xampp\htdocs\ludoteca**



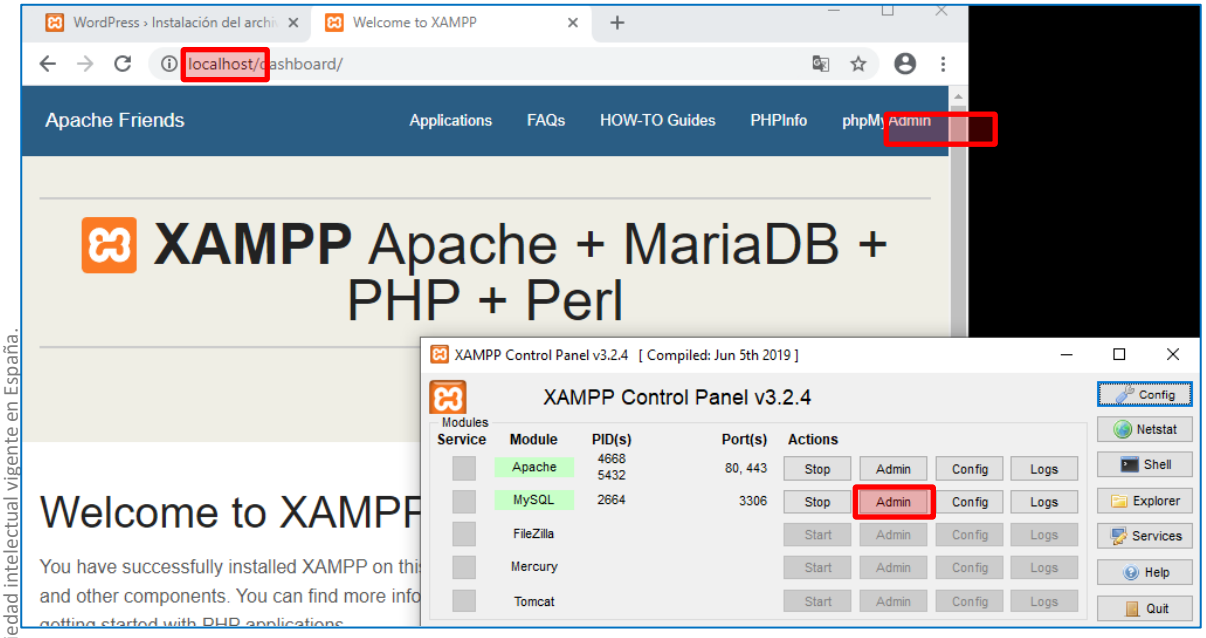
Crear base de datos para el sitio WordPress

Con el sitio web creado ahora tenemos que generar el contenido de las páginas web que serán guardados en una base de datos, con lo cual el siguiente paso es crear la base de datos usando el programa que hemos instalado antes durante el proceso de instalación de XAMPP llamado **phpMyAdmin**.

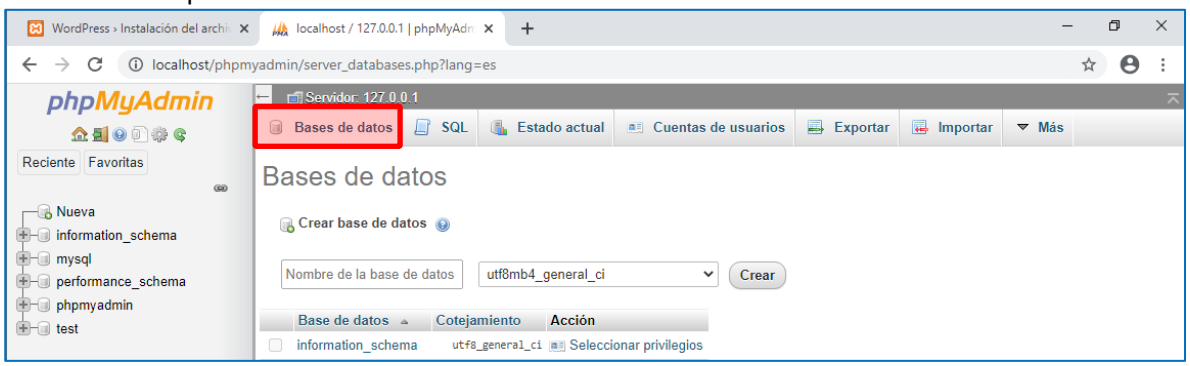


Como podemos ver en la página anterior el propio WordPress nos está pidiendo esos datos para poder empezar a trabajar

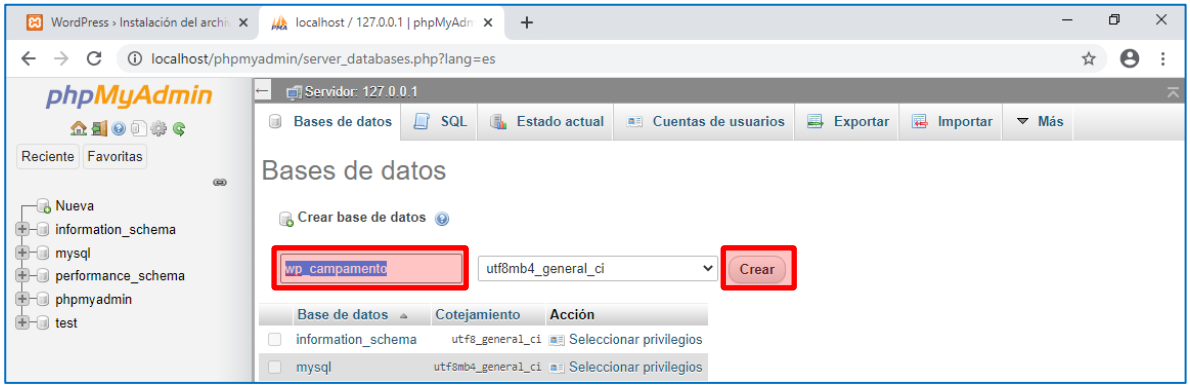
Para acceder al programa phpMyAdmin, pulsamos sobre el botón **Admin** del panel del control de XAMPP o escribimos **localhost** en el navegador y luego pulsamos sobre el botón **phpMyAdmin** del menú principal:



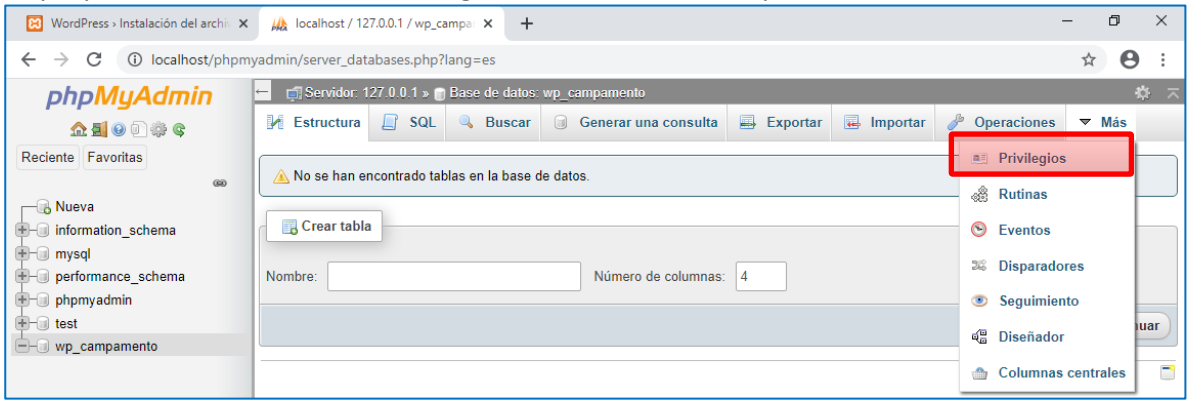
En cualquiera de los casos se nos abre el navegador en la página **http://localhost/phpmyadmin/**
Pulsamos en la pestaña Base de datos:



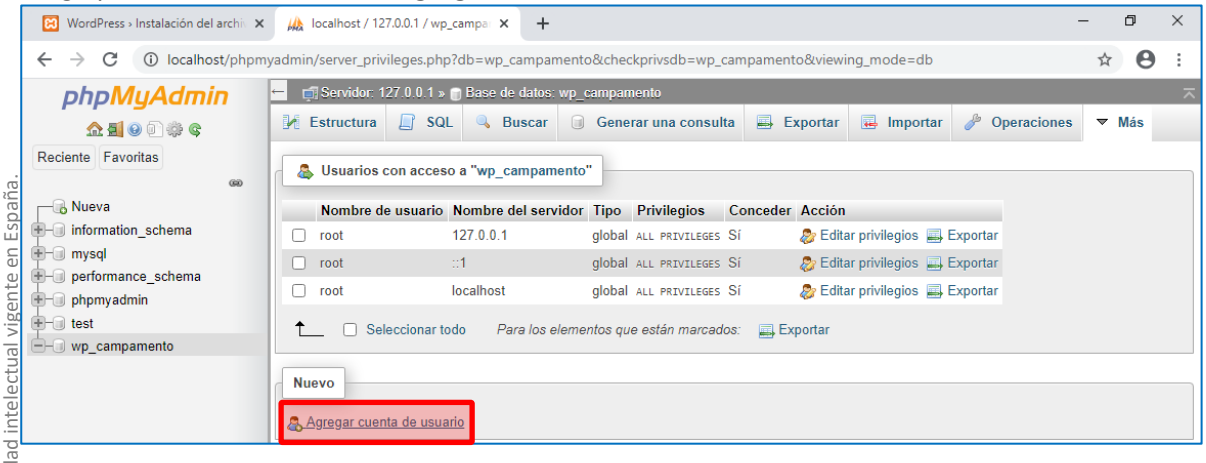
Escribimos el nombre de la nueva Base de datos: **wp_campamento** y pulsamos sobre **crear**:



Con la base de datos creada, el siguiente paso es crear el **usuario** y la contraseña de acceso a la misma, para lo que pulsamos sobre el botón **Privilegios**, si no lo vemos en la pantalla estará dentro del menú Más:



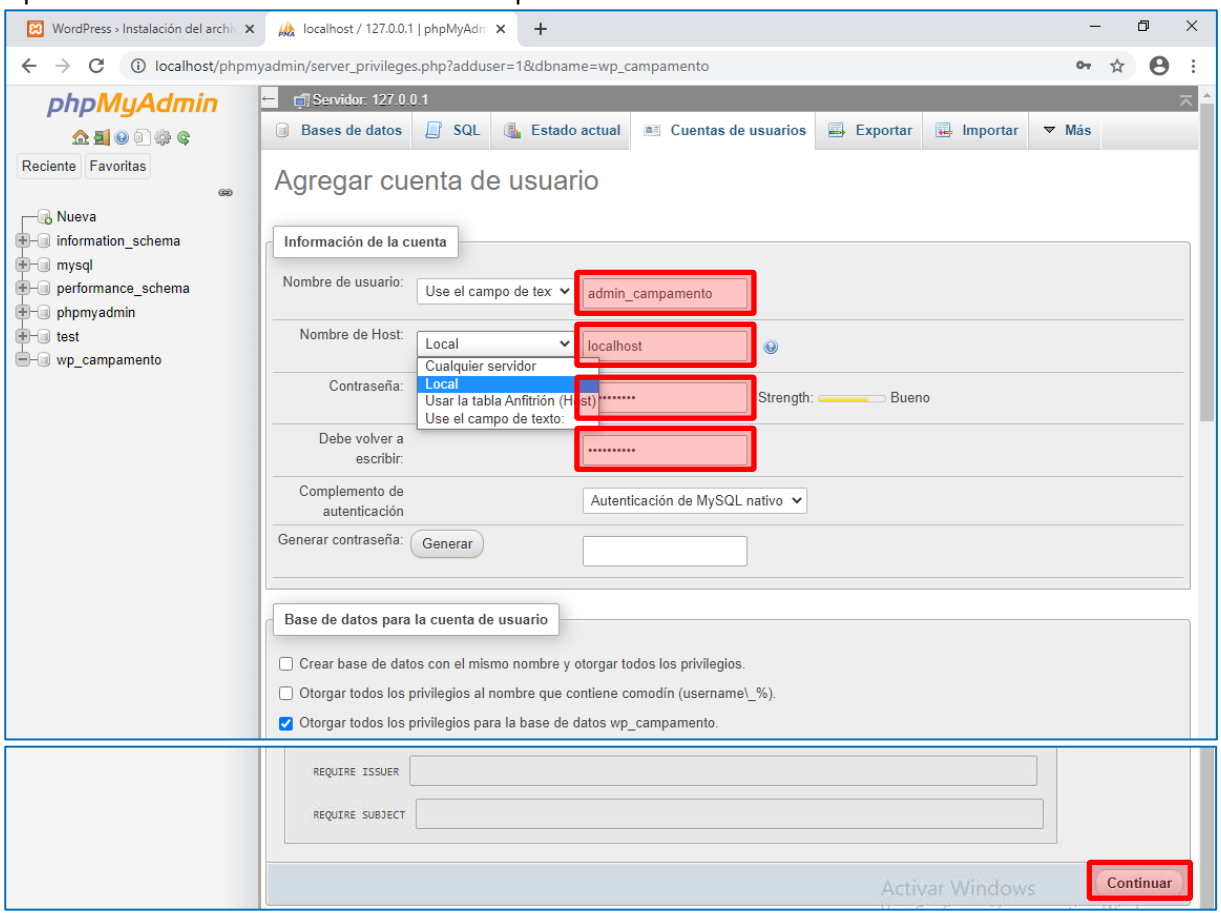
Luego pulsamos sobre el botón **Agregar cuenta de usuario**:



Y le indicamos los datos de:

- Nombre de Usuario: **admin_campamento**
- Nombre del Host-Servidor: **locahost** (lo seleccionamos de la lista)
- Contraseña: **123456** y la volvemos a escribir dónde nos pone **Debe volver a escribir**

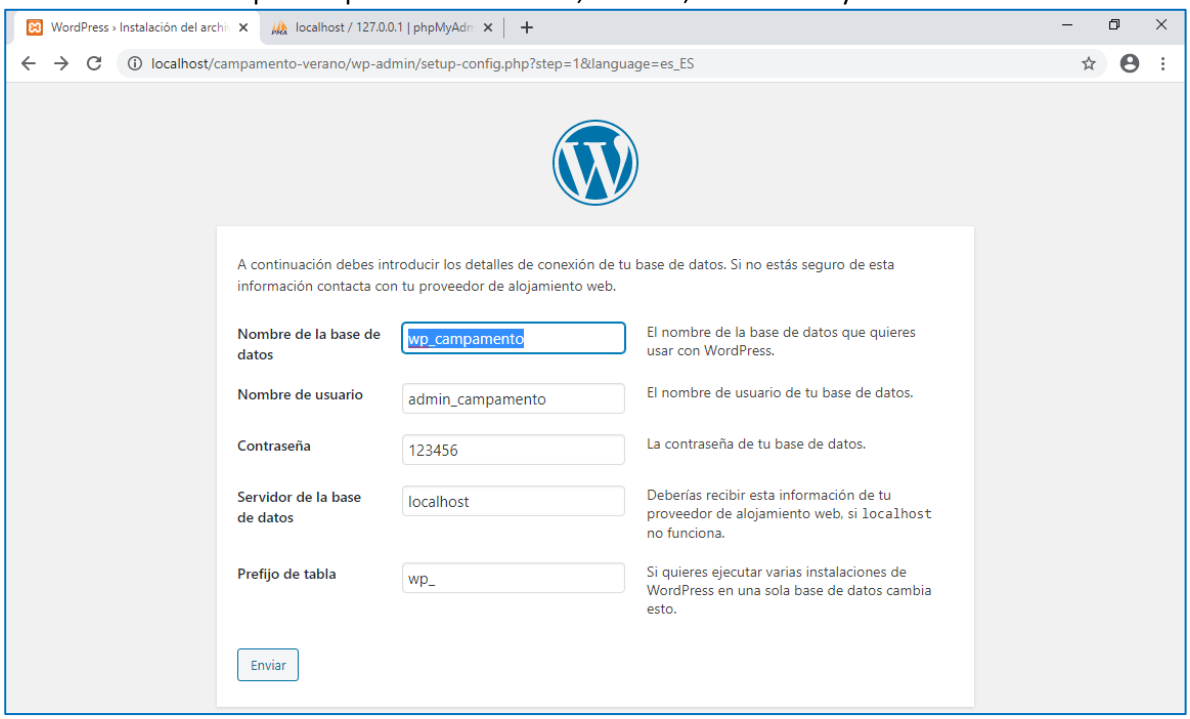
Y pulsamos sobre el botón **Continuar** de la parte inferior:



Con todo esto ya está creada la base de datos, así que ya podemos pulsar sobre el botón **¡Vamos a ello!** de la página de WordPress:

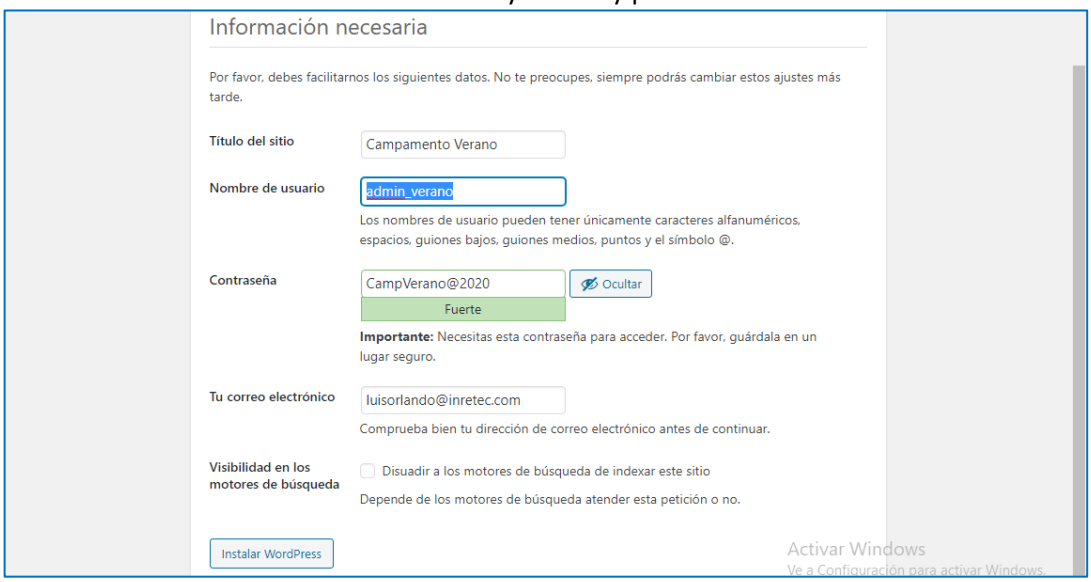
Construcción del sitio WordPress

Indicamos los datos que nos pide: Base de datos, Usuario, Contraseña y Servidor

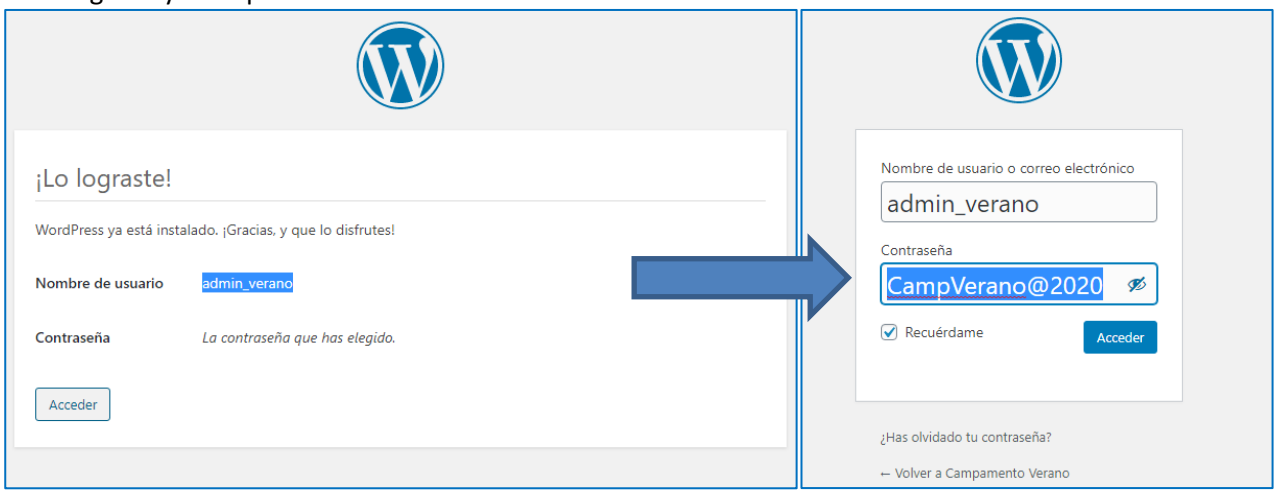


Y pulsamos sobre **Ejecutar la instalación**

E indicamos el Titulo del sitio, el nombre de usuario de WordPress: **OJO!!!** no confundir con el usuario de la Base de datos, el usuario de WordPress es el que daremos a nuestro cliente para que maneje la Web. También indicaremos la Contraseña de WordPress y el mail y pulsamos sobre **Instalar wordPress**:

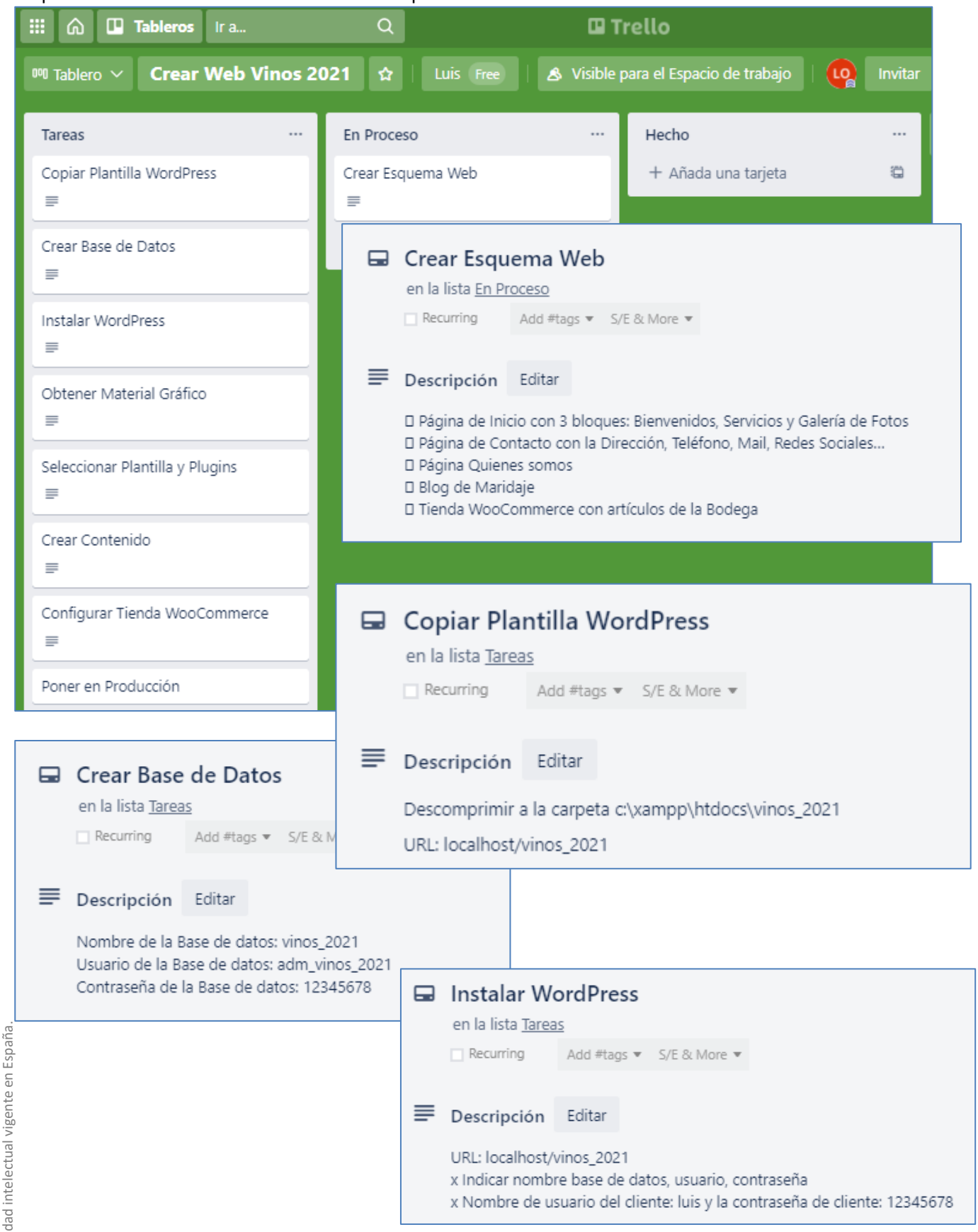


Acto seguido ya nos permite acceder a WordPress:



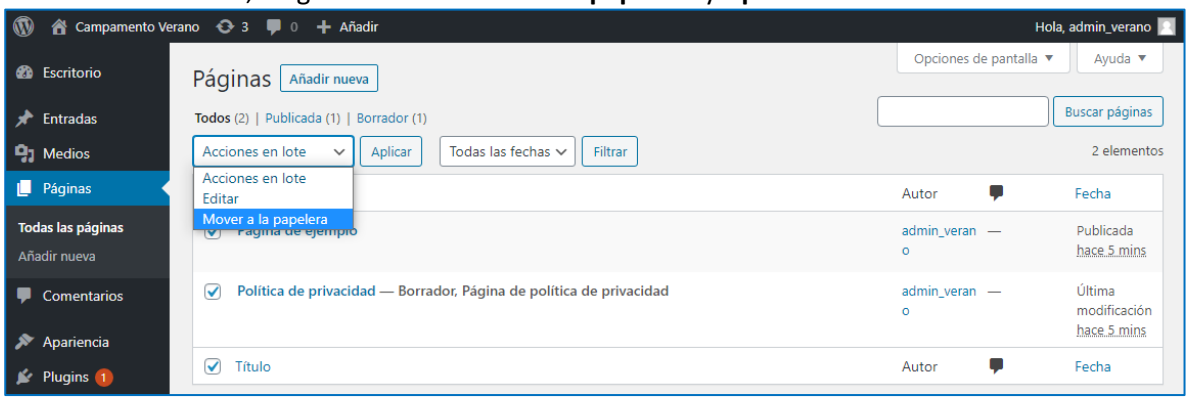
Creamos Nuevo sitio Vinos_2021

Preparamos un tablero en Trello con las tareas para la creación de este nuevo sitio web:

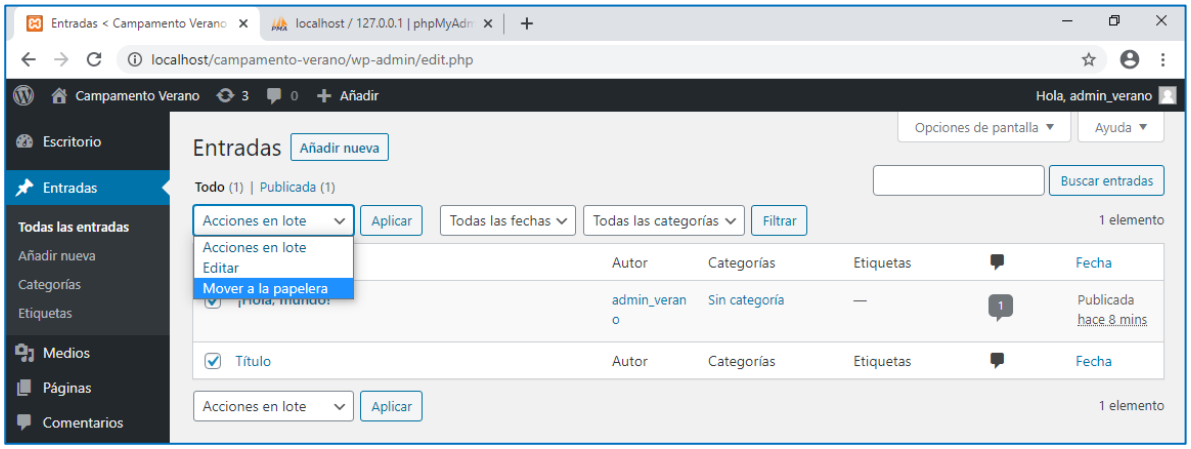


Instalación de la Plantilla y los Plugins

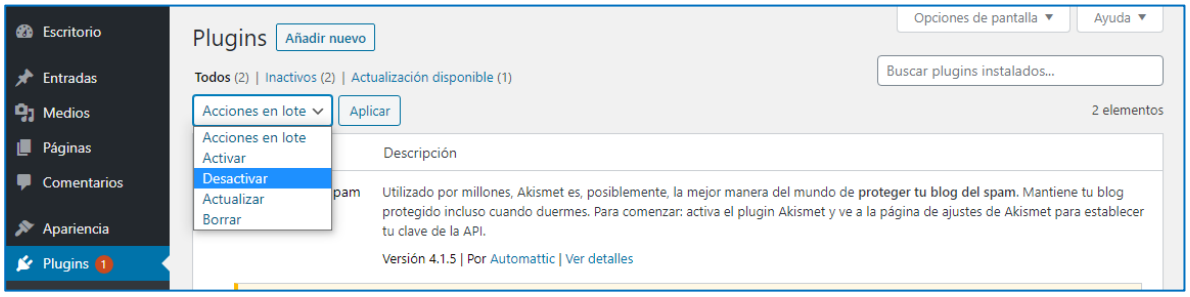
Limpiamos el contenido por defecto que nos aparece en WordPress, en la pestaña de **Páginas**, **Seleccionamos todo**, luego Acciones: **Mover a la papelera** y **Aplicar**:



Hacemos lo mismo en **Entradas**

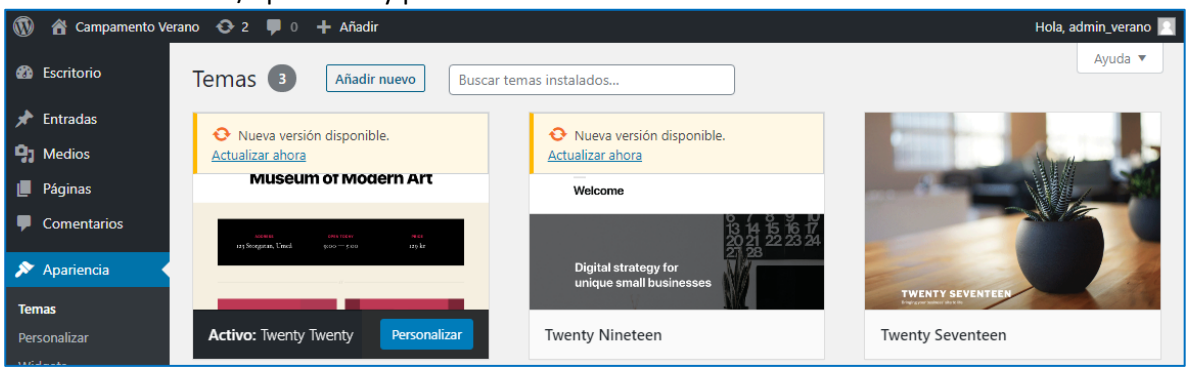


Y lo mismo con Plugins, pero para poder borrarlos primero hay que desactivarlos:

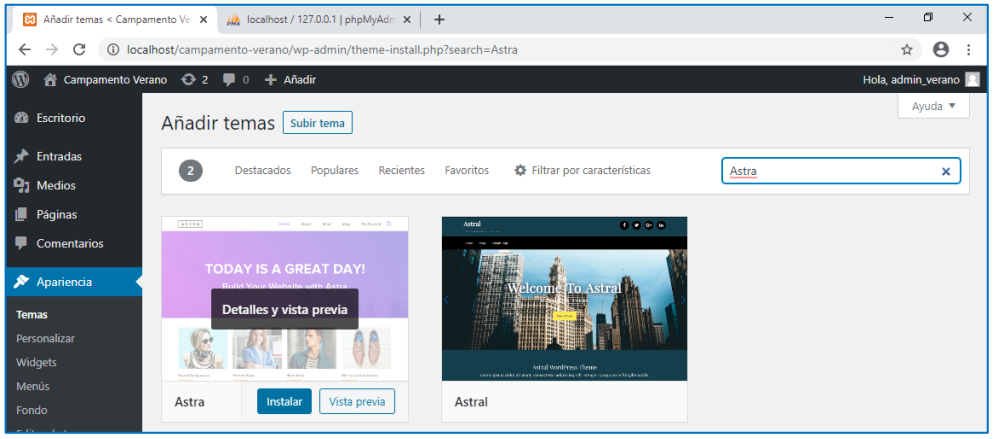


Y luego los borramos:

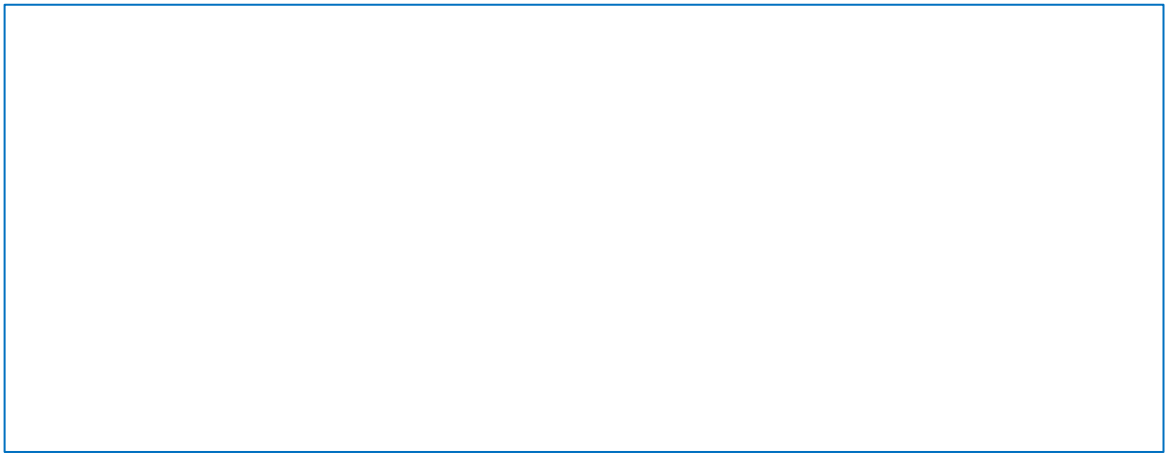
Creamos la plantilla: Diseños Pre-Creados para la página web.
Nos vamos a Temas/Apariencia y pulsamos sobre el botón **Añadir nuevo**



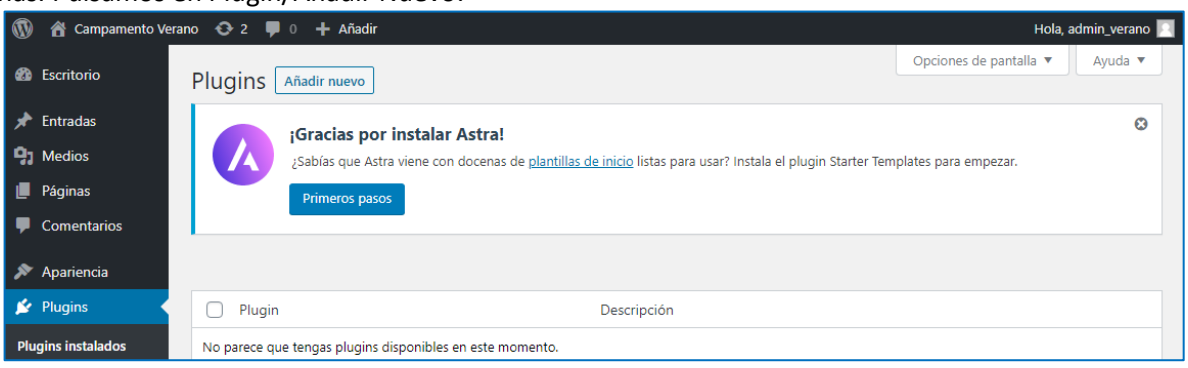
Buscamos **Astra** y le damos a **Instalar**



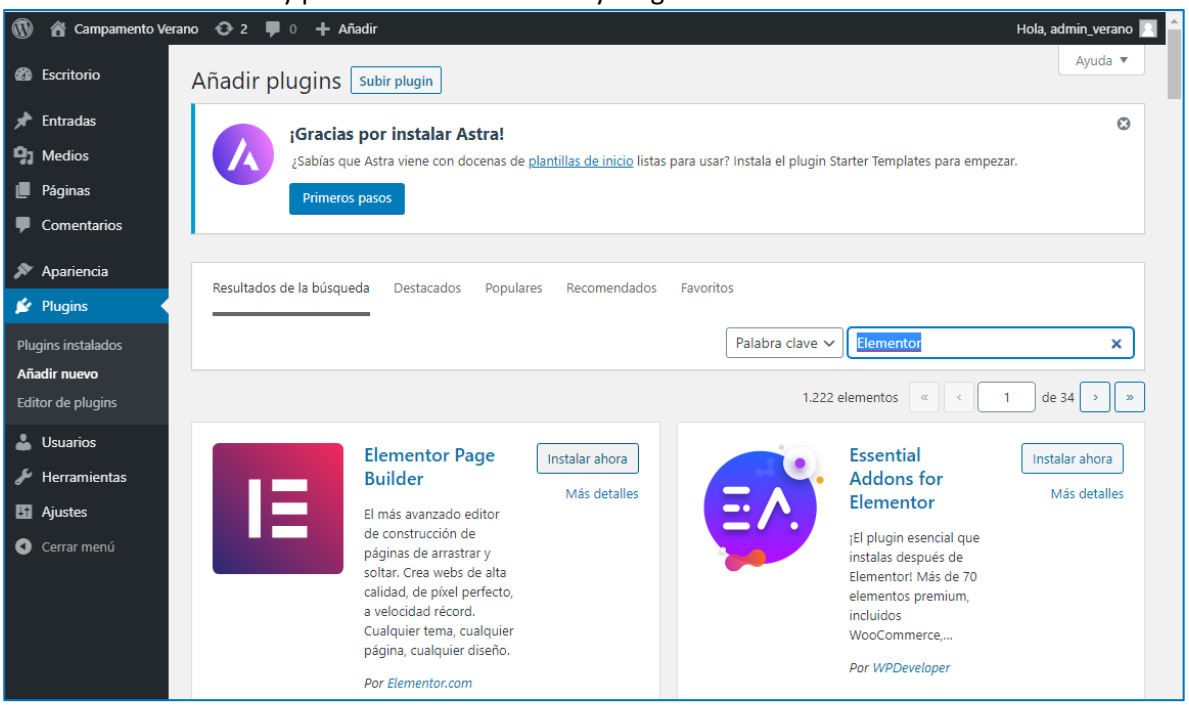
Y luego en **Activar**



Y por último instalamos el plugin **Elementor** para poder añadir contenido de forma sencilla a nuestras páginas. Pulsamos en Plugin/Añadir Nuevo:

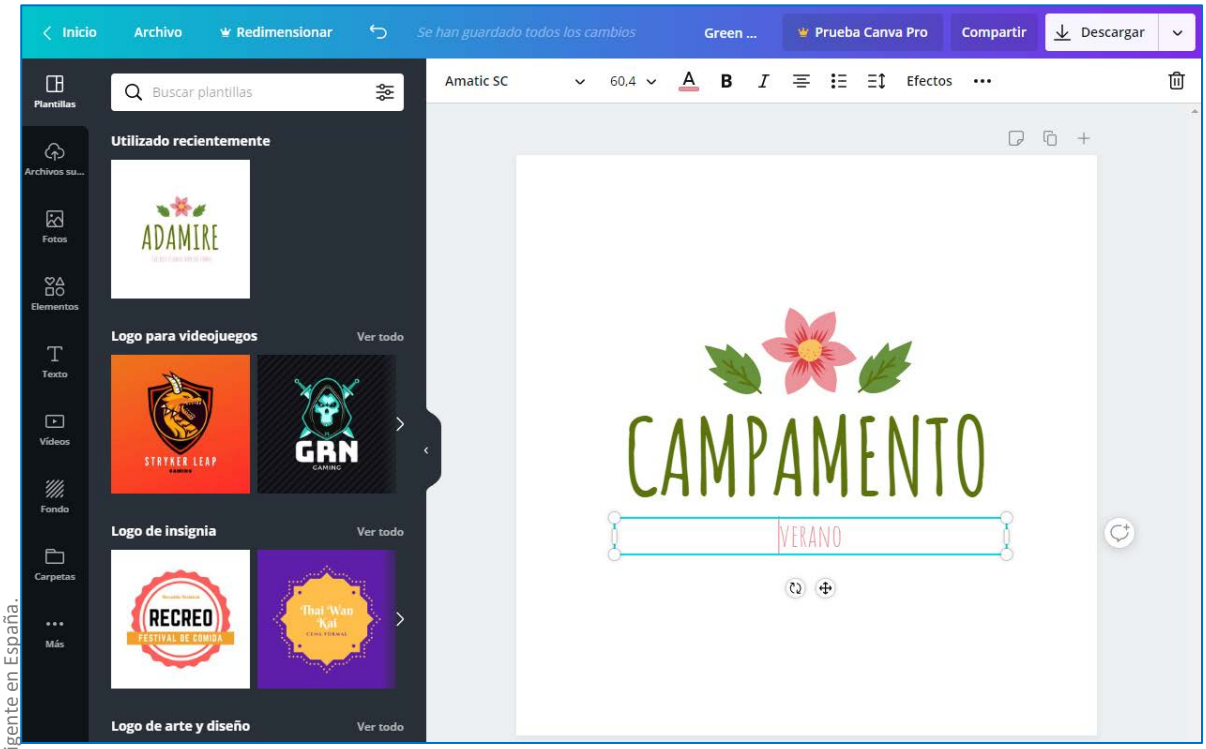


Y buscamos **Elementor** y pulsamos sobre **Instalar** y luego sobre **Activar**:



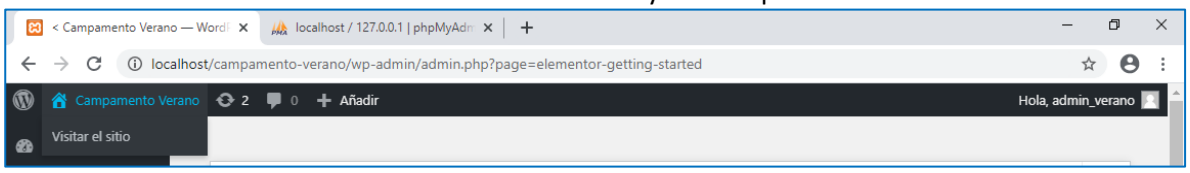
Creación del contenido del sitio Web

Ya tenemos creado el sitio web, ahora vamos a personalizarlo y meterle contenido. Empezamos por meter el Logotipo. Lo creamos en Canva, para la que abrimos una nueva pestaña en el navegador y vamos hasta https://www.canva.com buscamos una plantilla escribiendo el texto Logotipo y seleccionamos una:

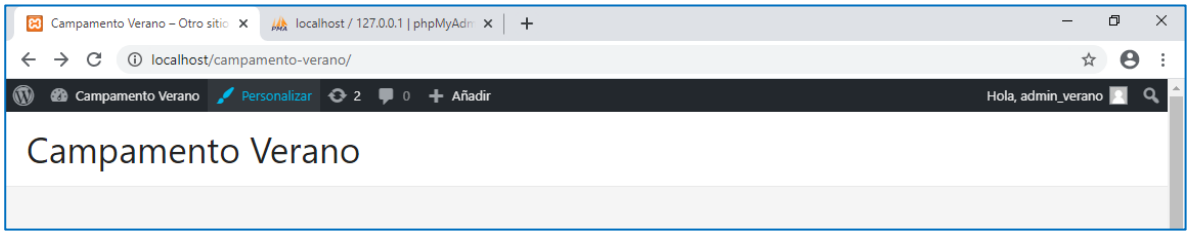


Diseñamos el logotipo modificando aquellos aspectos que nos interesen y finalmente lo descargamos como imagen PNG.

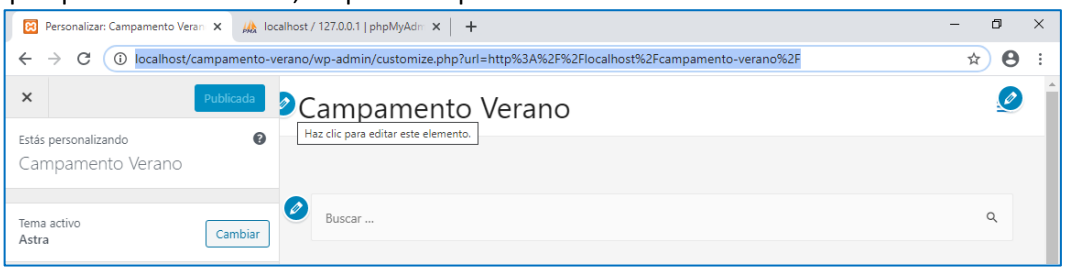
Nos volvemos a WordPress a la dirección **localhost/campamento-verano**. Pulsamos sobre el Icono con el símbolo de una casa - Campamento Verano para ver cómo queda el sitio. Ese primer botón nos sirve para cambiar entre el entorno de administración **back-end** y la web que ven los clientes **front-end**:



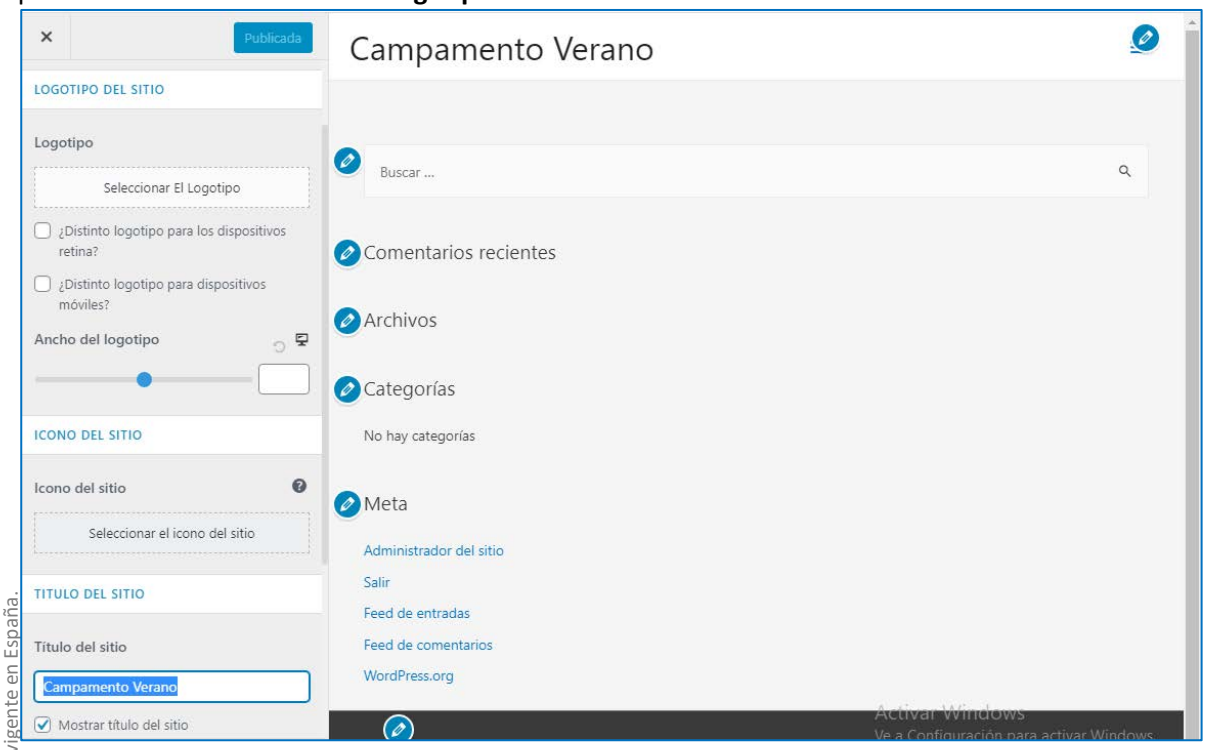
Después de ver como es elaspecto del sitio, luego pulsamos sobre **Personalizar**

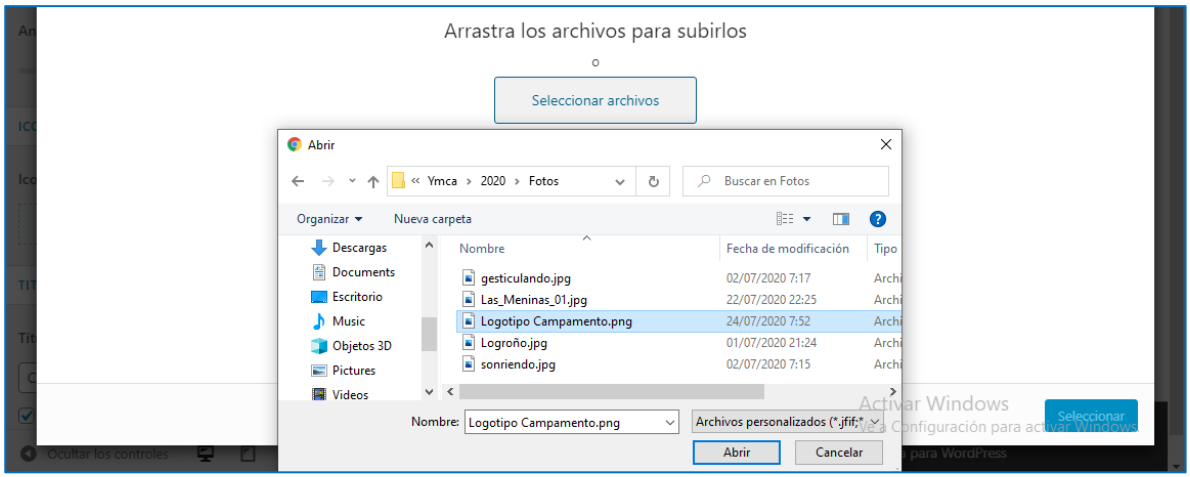


Desde aquí podemos modificar los elementos de la página web pulsando sobre el símbolito del Lápiz en el apartado que queremos modificar, empezamos por el Título:



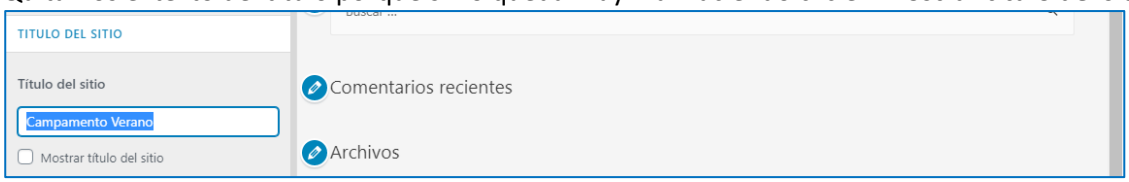
Y tenemos 2 opciones o meter el texto (que ya lo tenemos) o meter una imagen con el Logo, en este caso pulsamos sobre **Seleccionar El Logotipo**:





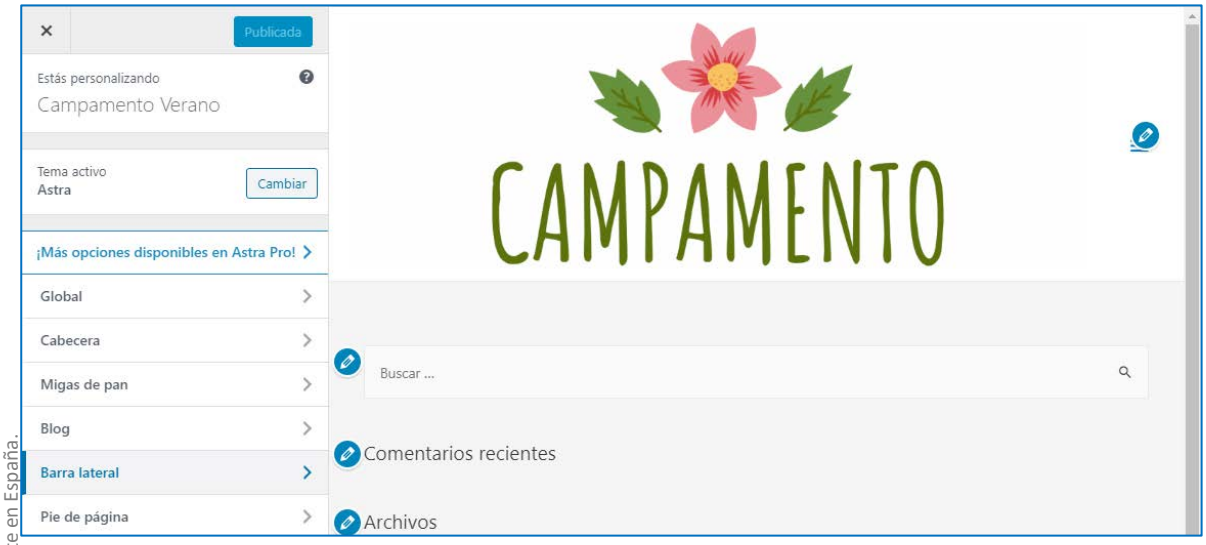
Luego en Seleccionar y Recortamos el Logo y pulsamos sobre **Recortar Imagen**:

Quitamos el texto del título porque si no queda muy mal haciendo clic en **Mostrar título del sitio**:

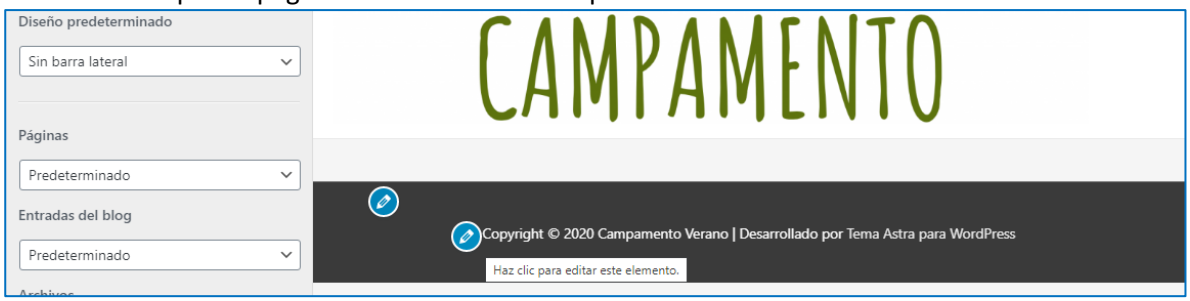


Y pulsamos sobre el botón **Publicar** de la parte superior, esto lo haremos con cada cambio para ir viendo cómo queda el sitio.

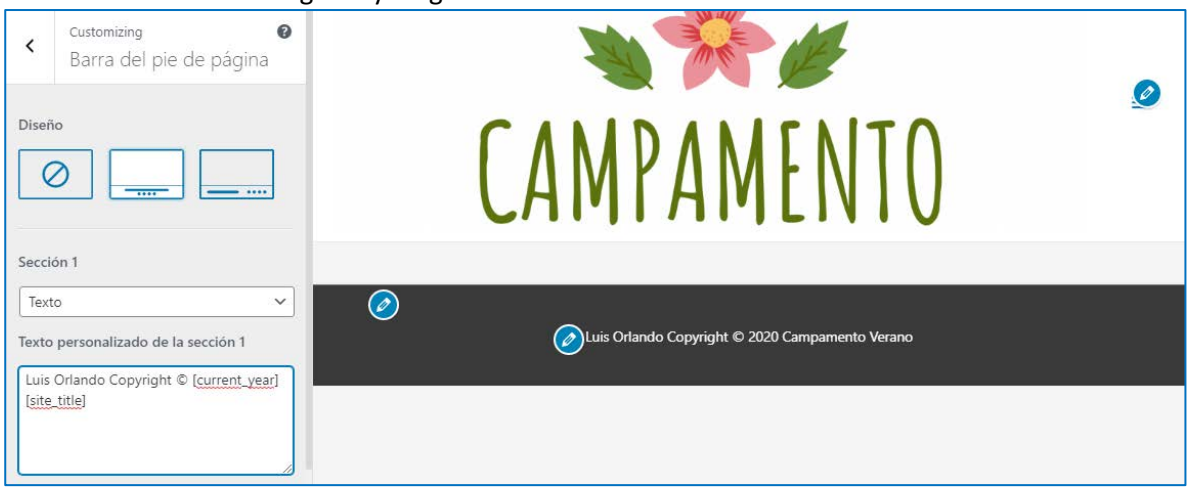
Quitamos la barra lateral que queda muy mal. Nos vamos hacia atrás con la flecha < 2 veces y pulsamos sobre **Barra Lateral/Sin Barra Lateral** y luego en **Publicar**:



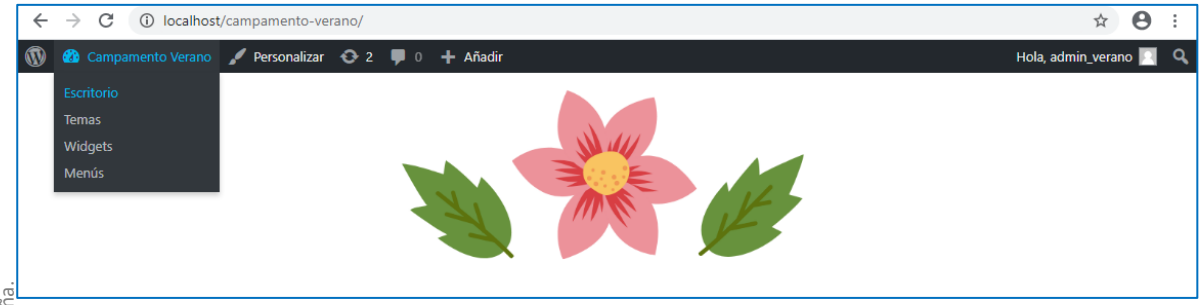
Cambiamos el pie de página haciendo clic en el lápiz azul:



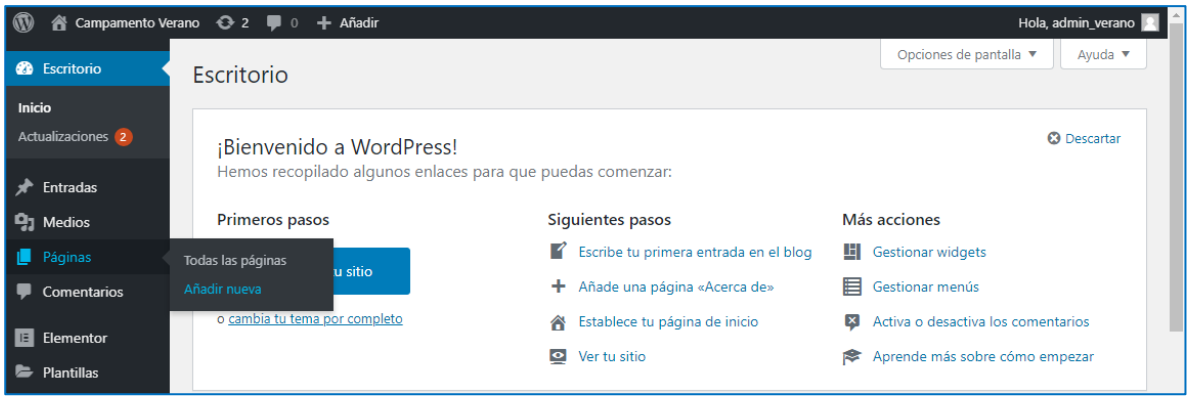
Lo cambiamos a nuestro gusto y luego le damos a **Publicar**



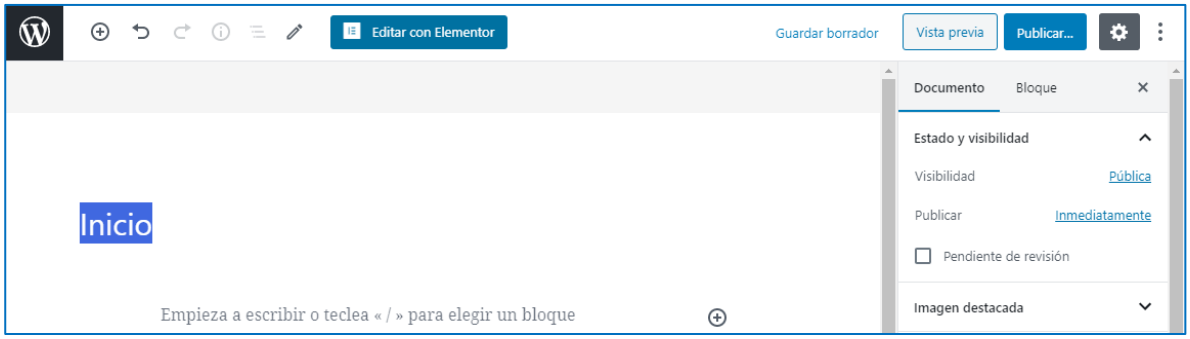
El siguiente paso es meter contenido en la página, para lo cual pulsamos sobre la X de la parte Superior Izquierda y luego pulsamos sobre **Campamento Verano/Escritorio**



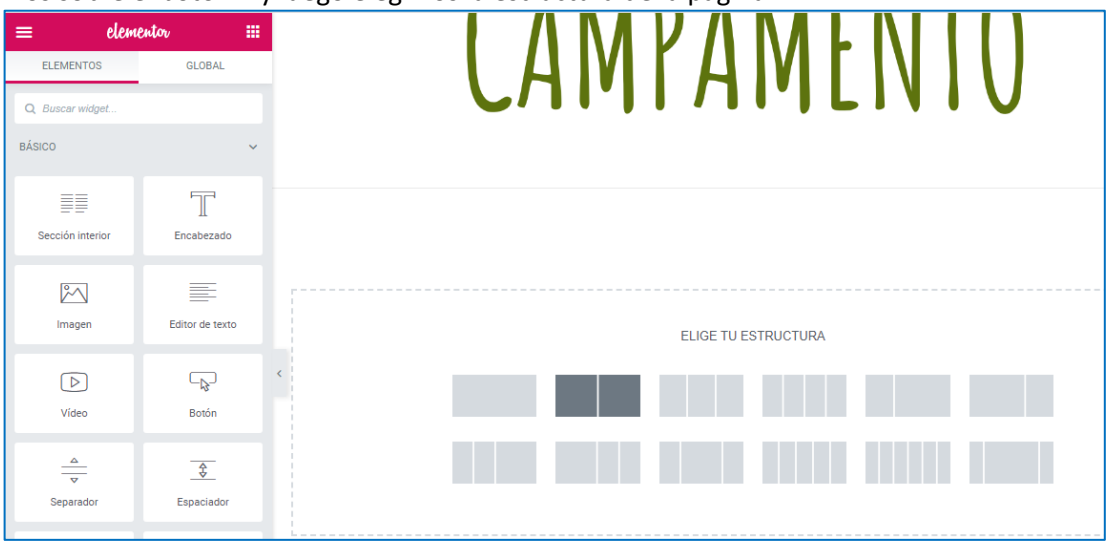
Luego nos vamos al menú **Páginas/Añadir Nueva**

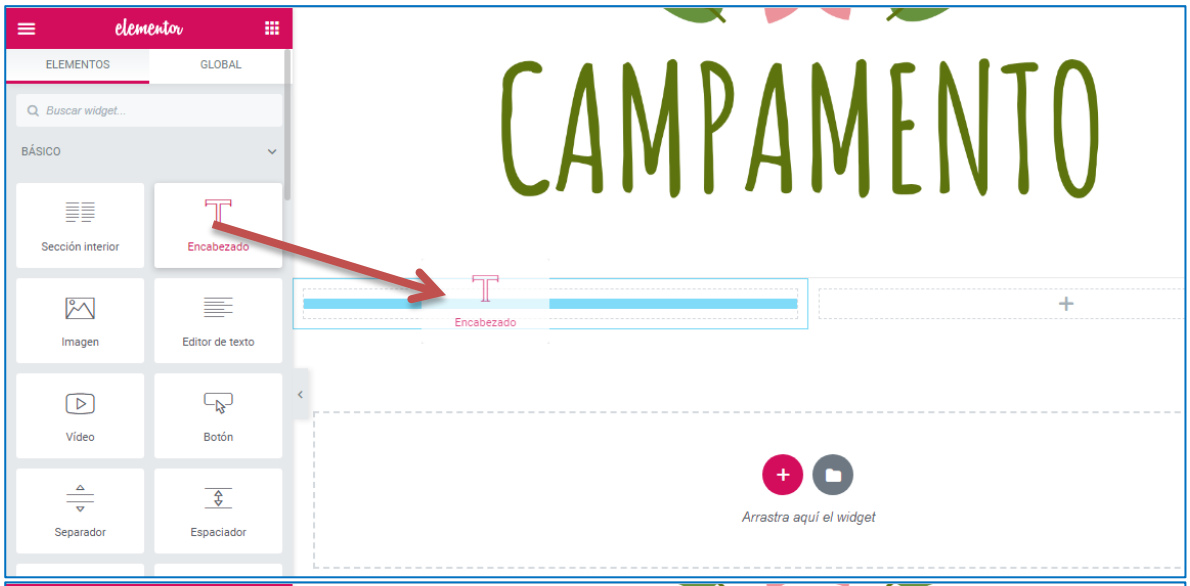


Le ponemos un Título, por ejemplo **Inicio** porque será la página principal y luego pulsamos sobre el botón **Editar con Elementor**:

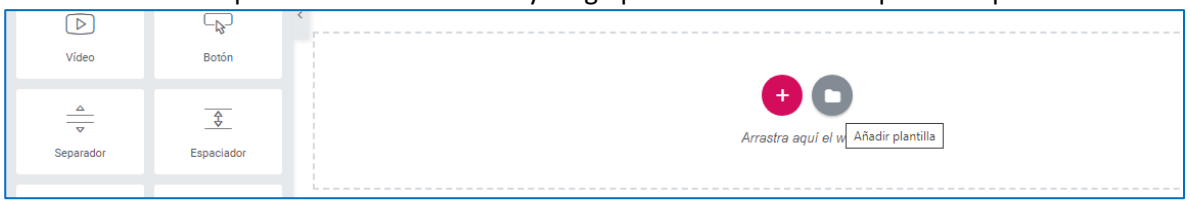


Desde este editor podemos arrastrar elementos como Textos, Imágenes… para hacerlo de forma manual pulsaríamos sobre el botón + y luego elegimos la estructura de la página:

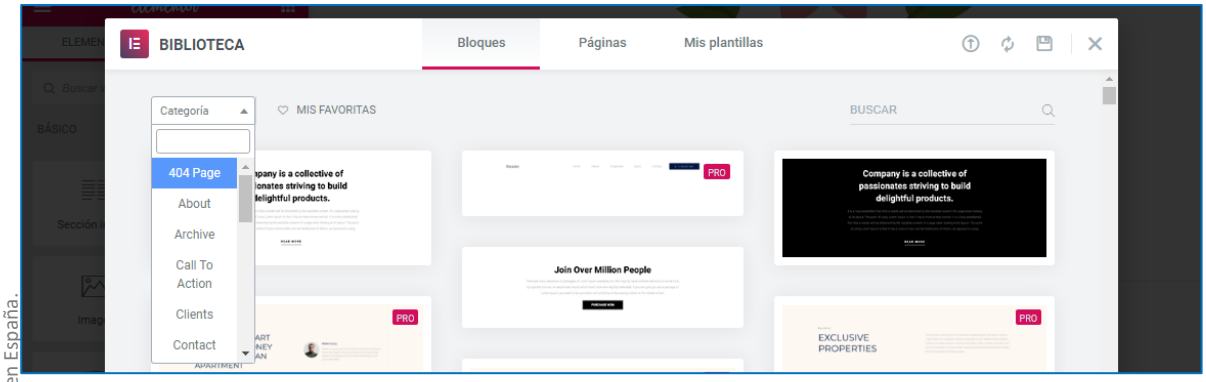




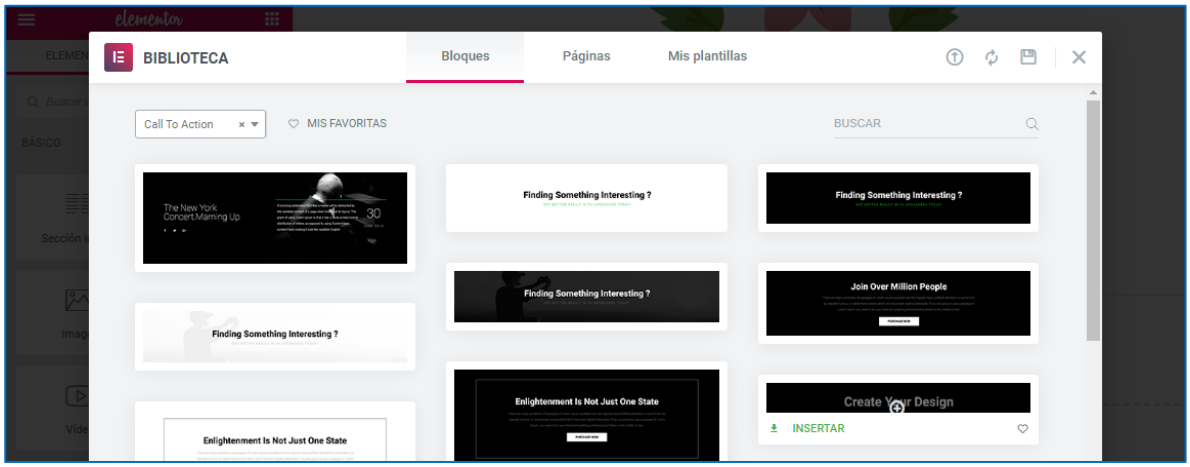
Pero nosotros lo vamos a hacer usando Bloques o Páginas ya prediseñados. Borramos la sección que acabamos de crear pulsando sobre la X azul y luego pulsamos sobre la carpeta Gris para añadir el bloque:



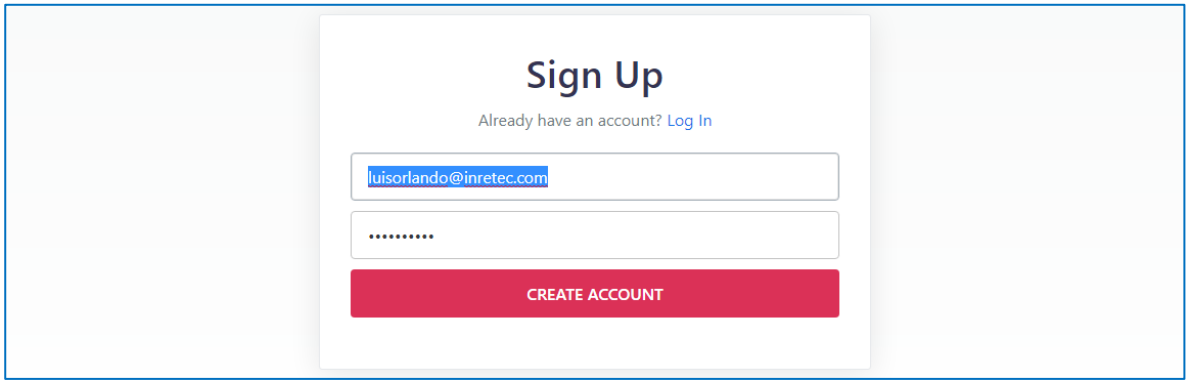
Podemos añadir páginas y bloques, nosotros vamos a añadir Bloques que están agrupados por categorías:



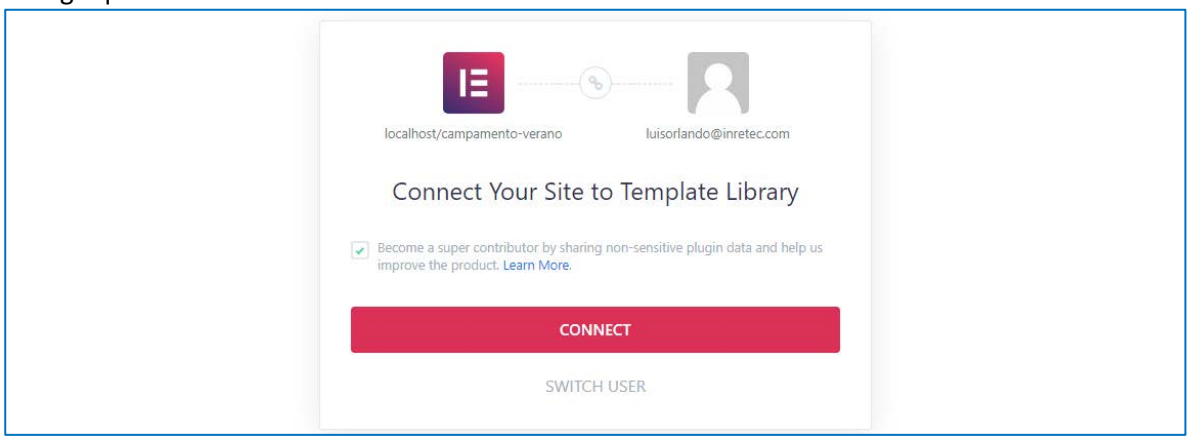
Y vamos a añadir el que nos interesa, tenemos algunos gratuitos y otros de pago (PRO) en este caso vamos a seleccionar **Call to Action**:



Si es la primera vez nos pedirá que creemos una cuenta gratuita:

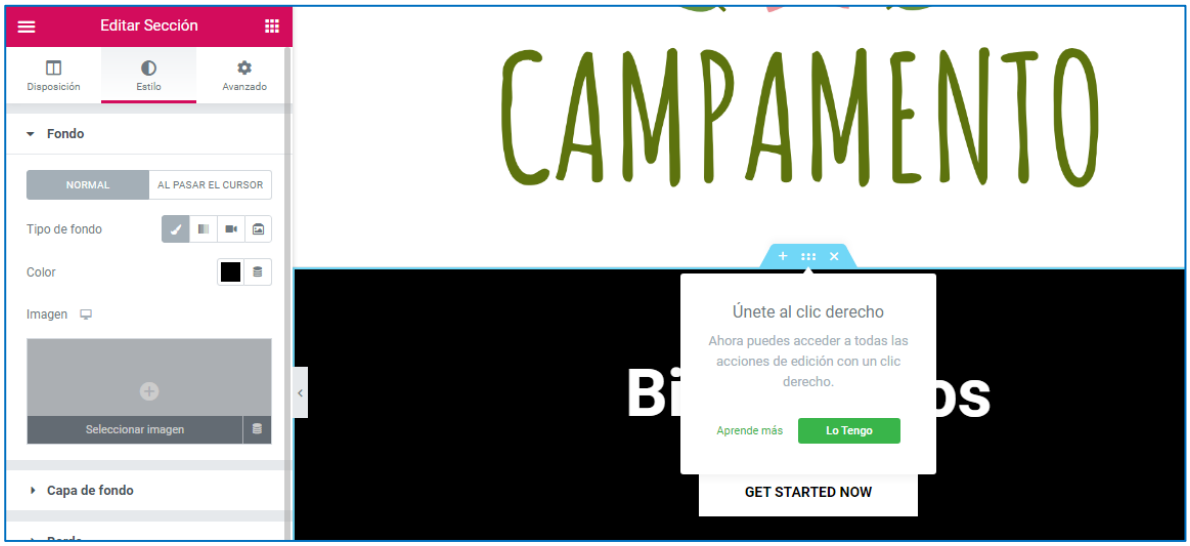


Y luego que la conecte a nuestro sitio:



Y ya podemos usar cualquier bloque o plantilla que no sea PRO:

Si hacemos clic en el botón central del bloque podemos cambiar por ejemplo los Estilos/Imagen de Fondo/Colores de fondo…



Podemos buscar imagen de fondo en cualquier repositorio de los que vimos o en **Unsplash.com**

Para insertar una imagen de presentación en nuestra página de inicio:

1. Pulsamos sobre el botón el + de la sección **Imagen** que vemos en la figura anterior
2. Como es una imagen nueva y no estará en la **Biblioteca de Medios**, pulsamos sobre **Subir archivos/Seleccionar archivos**, y después sobre el botón **Insertar medio**
3. Si la imagen es muy grande, para cambiar le tamaño, elegimos **Tamaño/Abarcar**
4. Para hacer la sección más grande, pulsamos sobre **Avanzado** Relleno arriba y abajo 200
5. Si el texto que tenemos encima no se lee muy bien pulsamos en sobre **Capa de Fondo** (que está debajo del botón anterior de imagen), luego en **Estilo/Tipo de Fondo** seleccionamos un Color
6. Una vez que queda como deseamos pulsamos sobre **Publicar**

Si queremos añadir un texto debajo de Bienvenidos:

1. Pulsamos en la parte superior sobre las 3 *rallitas* de Editar Sección
2. Luego sobre la **flecha** que ha aparecido en este mismo lugar
3. Y luego arrastramos la sección T Encabezado, debajo de Bienvenidos, y ponemos un mensaje de Bienvenida
4. Luego desde **Estilo** podemos cambiar la Tipografía, Tamaño del texto…

Si queremos modificar el botón, hacemos clic encima del botón y pulsamos sobre **Contenido** y desde esta opción podemos cambiar el Tipo, Texto e incluso el enlace.

Luego meteremos la sección de Servicios (Services)

Pulsamos sobre la carpeta de la siguiente sección

Bloques/Categorías/Services

Seleccionamos la que nos gusta

Para borrar un elemento que no nos interesa, pulsamos sobre el botón de la parte superior derecha de esa sección con el botón derecho y pulsamos sobre **Borrar**

Para cambiar el texto, lo seleccionamos y desde Contenido/Título y descripción…

Podemos cambiar los iconos, pulsando sobre la imagen del mismo

E incluso podemos cambiarlos por imágenes:

1. Pulsando sobre la papelera que aparece en la parte superior de la imagen
2. Luego vamos hacia a tras pulsando sobre las 3 rallitas, luego flecha, nos aparecen todos los elementos que podemos añadir y seleccionamos imagen y la arrastramos

La sección de Sobre Nosotros (About con video)

Pulsamos sobre la carpeta de la siguiente sección

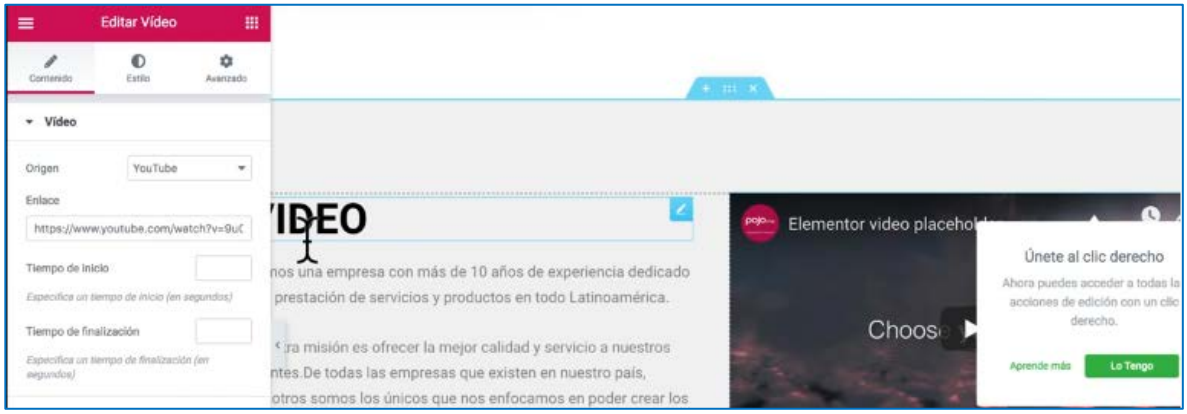
Bloques/Categorías/About

Si queremos cambiar el fondo de la sección:

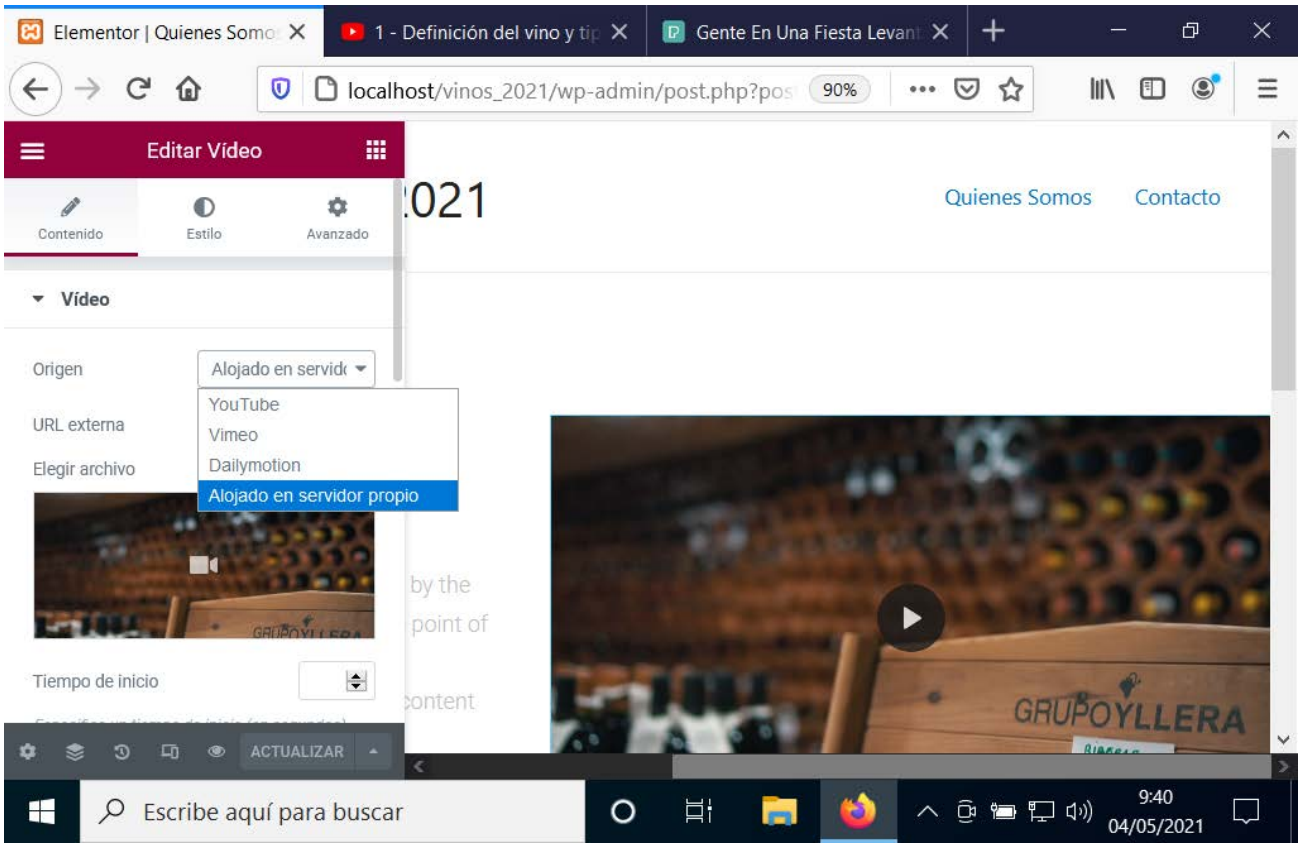
3. Pulsamos sobre los 6 puntitos de la sección
4. Y luego sobre Estilo

5. Luego sobre Tipo de Fondo y le damos al primer botón y elegimos un color gris

6. Y para cambiar el vídeo pulsamos sobre a esquina superior derecha del video y en el apartado Enlace podemos pegar una dirección de un vídeo de youtube:

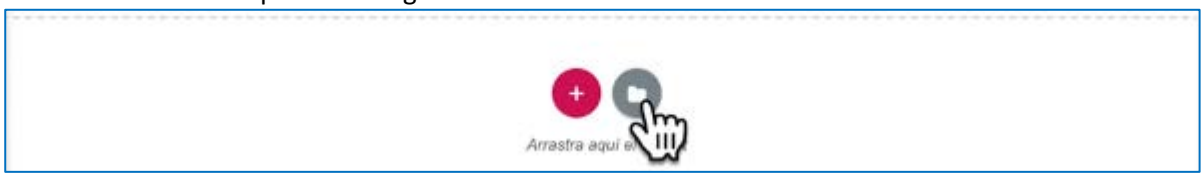


Y sino seleccionamos la opción de **Alojado en servidor propio**



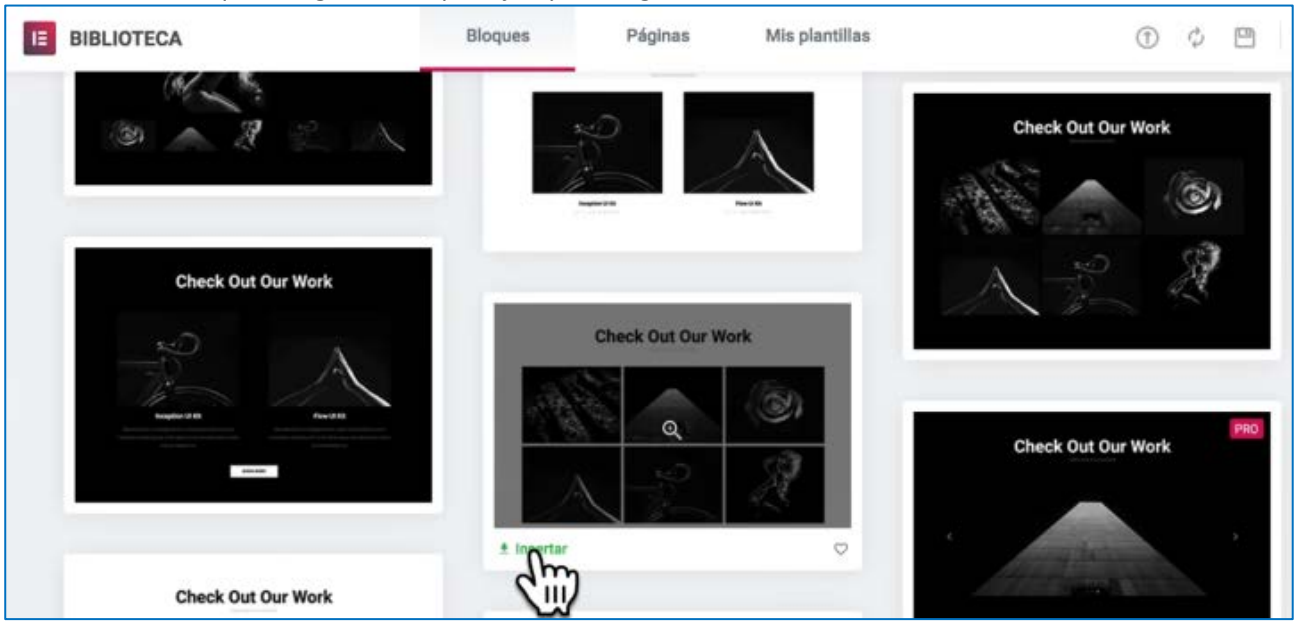
La sección de Galería de Fotos (Portfolio)

Pulsamos sobre la carpeta de la siguiente sección:

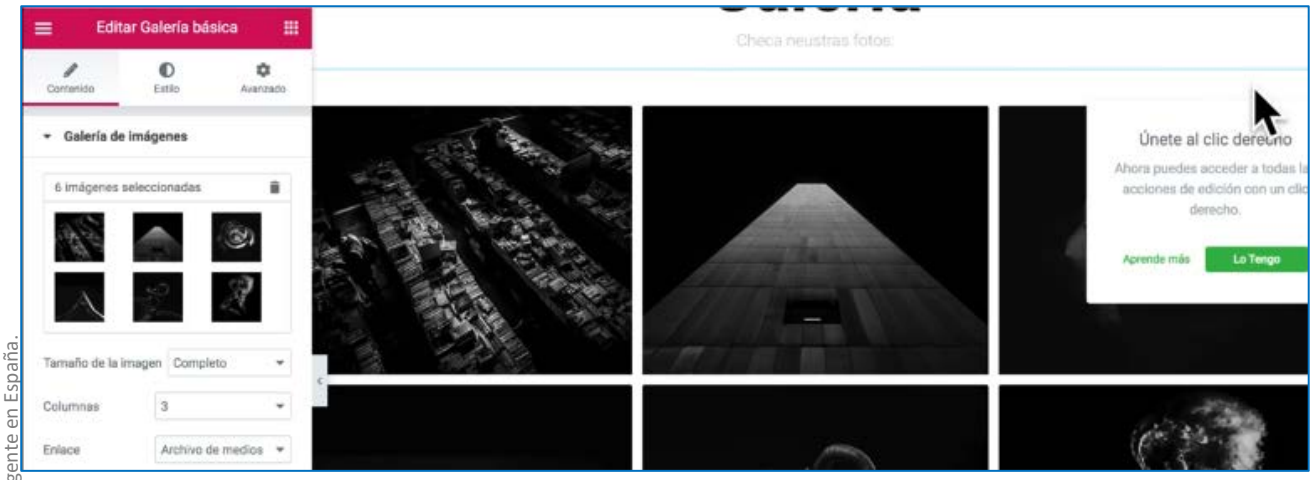


Bloques/Categorías/Portfolio

Seleccionamos la que nos guste más por ejemplo la siguiente:



Cambiamos el título y ponemos por ejemplo Galería y para cambiar las fotos pulsamos sobre el lápiz de la esquina superior derecha de las 6 fotos y luego clic en la parte derecha dónde pone 6 imágenes seleccionadas:

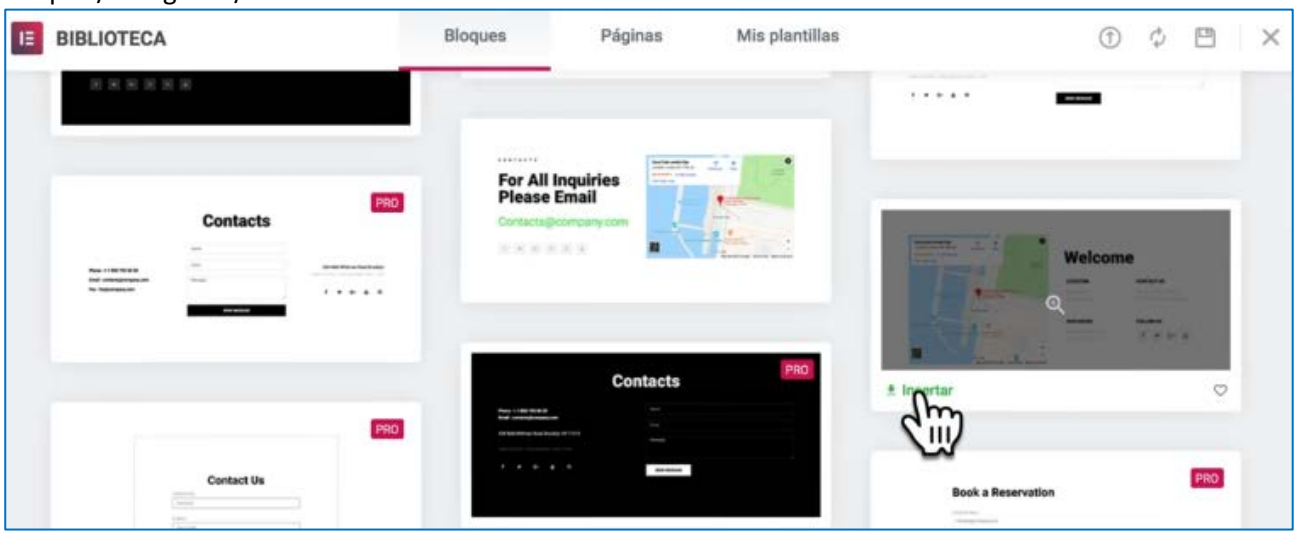


Luego pulsamos sobre **Seleccionar Archivos** y elegimos las fotos que queremos que nos aparezcan en nuestra galería.

La sección de Contacto (Contact)

Pulsamos sobre la carpeta de la siguiente sección

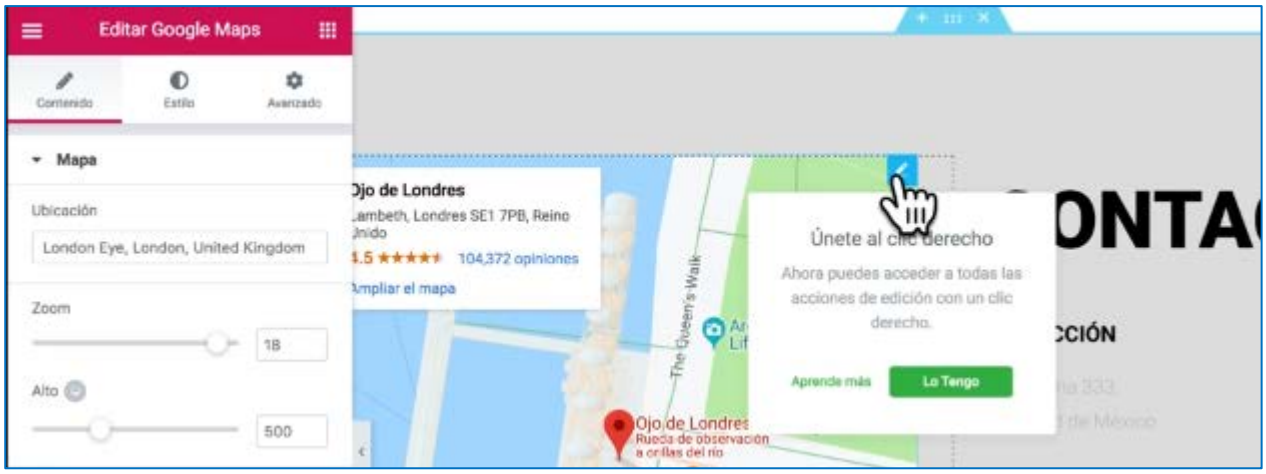
Bloques/Categorías/Contact



Cambiamos los datos de Localización (Dirección), Horario, Contáctanos

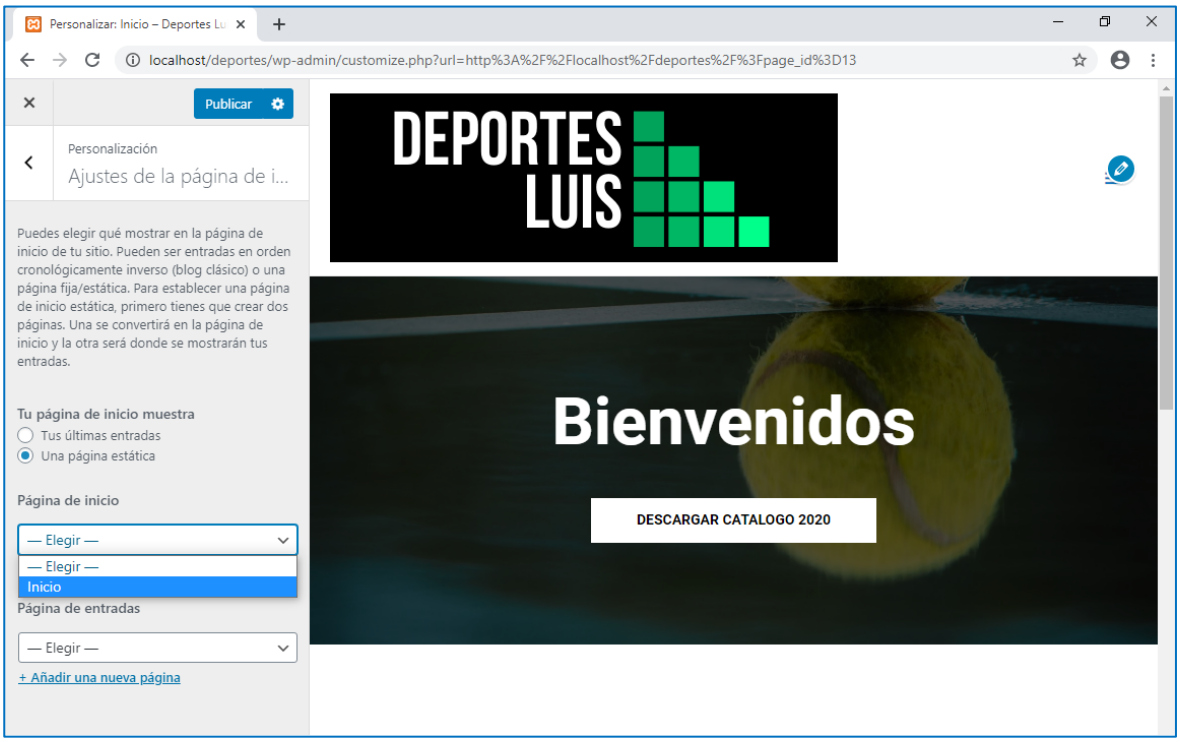
Igualmente podemos cambiar los Iconos de Redes sociales copiando los enlaces de nuestras redes sociales

Para cambiar la dirección del Google Maps, simplemente hacemos clic en el lapiz del mapa y en el apartado ubicación escribimos nuestra dirección.



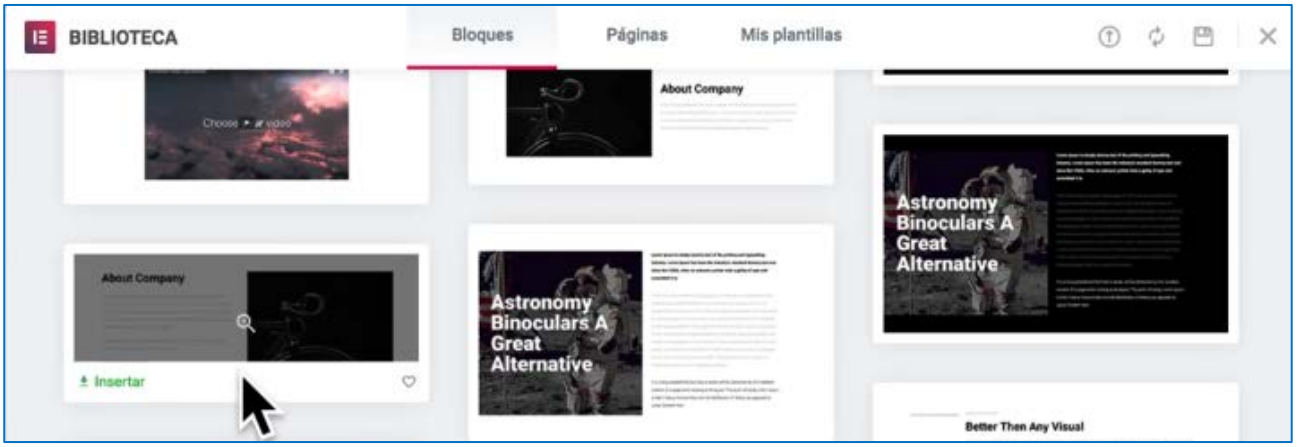
Para convertirla en página de Inicio, le damos a:

1. Personalizar
2. Ajustes de Página de Inicio -> Una página Estática
3. Página de Inicio -> Inicio



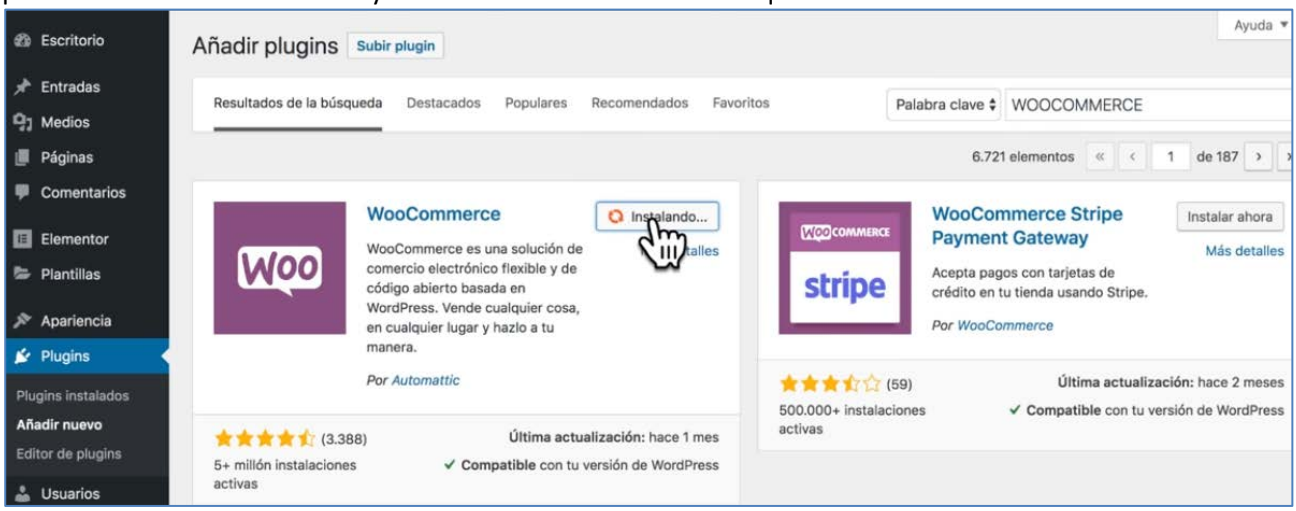
Y finalmente pulsamos sobre **Publicar**

Para añadir una nueva Página pulsamos sobre **Páginas/Añadir Nueva**
Por ejemplo la página de Quienes somos, le damos título y luego **Editar con Elementor**
Bloques/Categorías/About y elegimos **About Company**



Crear una Tienda Online en WordPress con Woocomerce

Lo primero que tenemos que hacer es Instalar el Plugin Woocomerce, con lo cual en el apartado de **Plugins** pulsamos sobre **Añadir Nuevo** y escribimos en el cuadro de Búsqueda **Woocomerce**

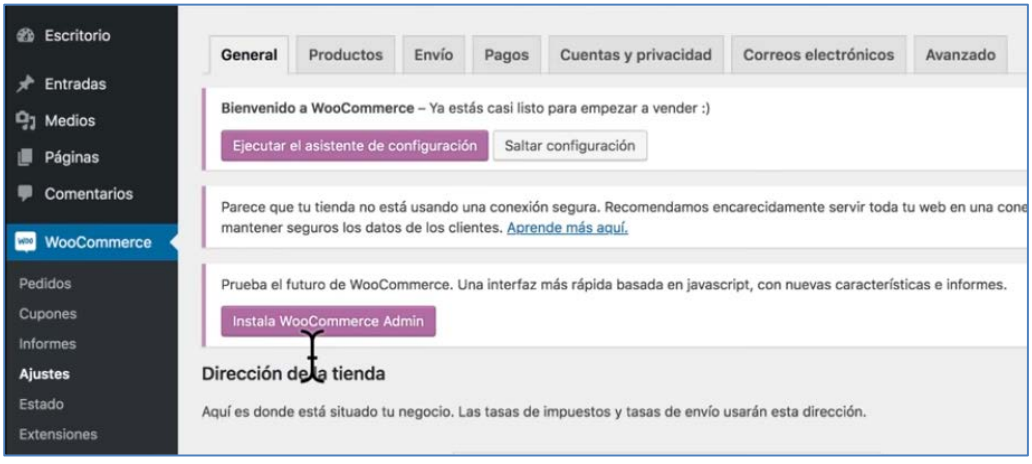


Luego en la primera ventana de Ajustes deberíamos indicar los datos sobre la tienda, dirección… en nuestro caso como vamos a ver simplemente como montar la tienda y ponerla rápidamente en funcionamiento no indicamos ningún dato y pulsamos sobre el botón de la parte inferior **Ahora No**.

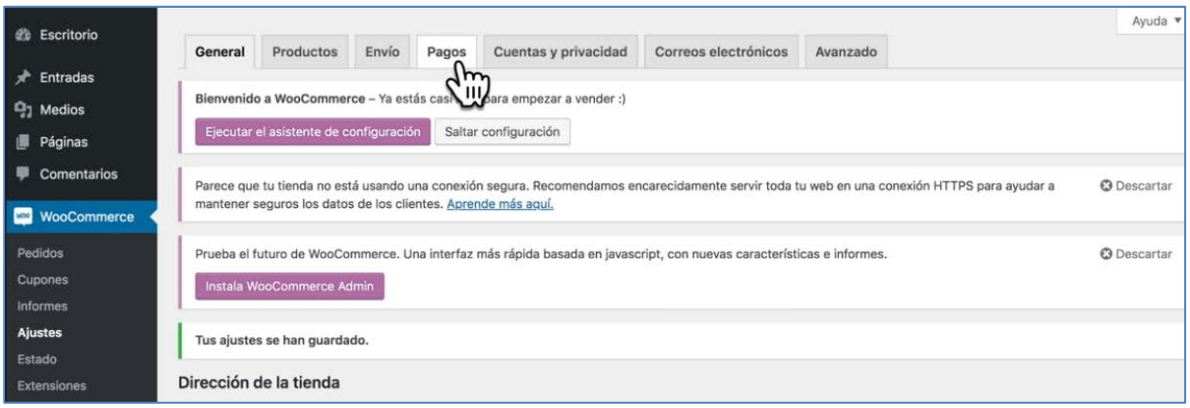
Si realmente quisiésemos montar una tienda online, Si que deberíamos perder un poco de tiempo y seguir los pasos que nos aparecen:

Para poner en marcha la tienda rápidamente simplemente tenemos que cambiar algunos valores prestablecidos y luego dar de alta los productos:

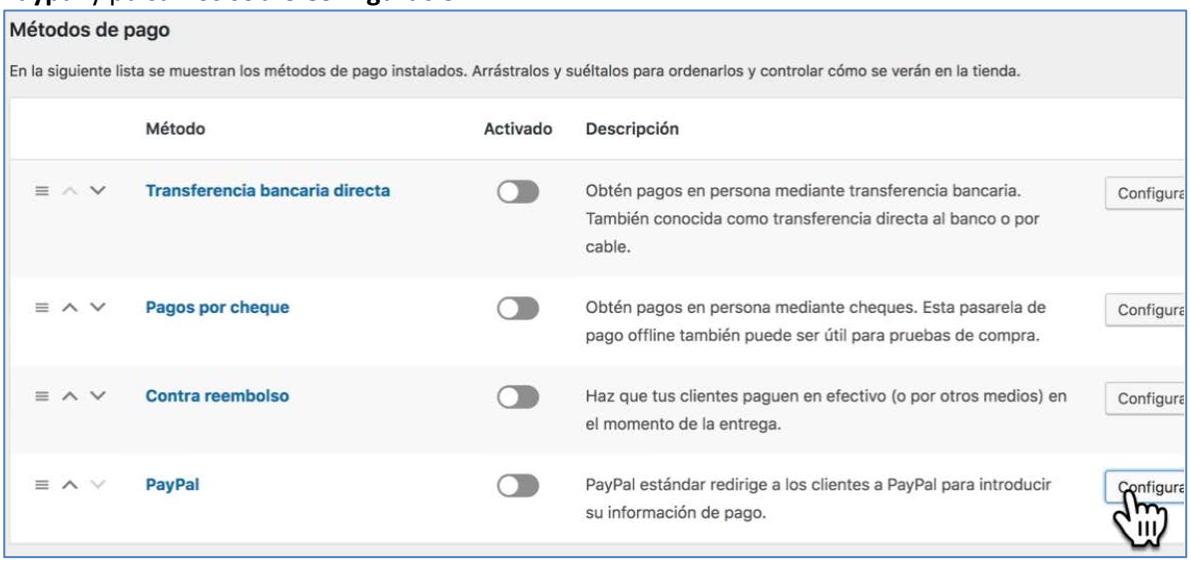
1. Como la aplicación viene por defecto con la moneda Libra esterlina y el formato para separador decimal y de miles anglosajón, el primer paso sería cambiarla a Euro (€), que coloque el símbolo del Euro a la derecha y que use la coma "," como separador de decimales y el punto "." Como separador de miles, y todo eso lo hacemos haciendo clic en **Woocomerce/Ajustes** y en la pestaña de **General** bajamos hasta **Moneda**, metemos los valores y pulsamos sobre **Guardar cambios**



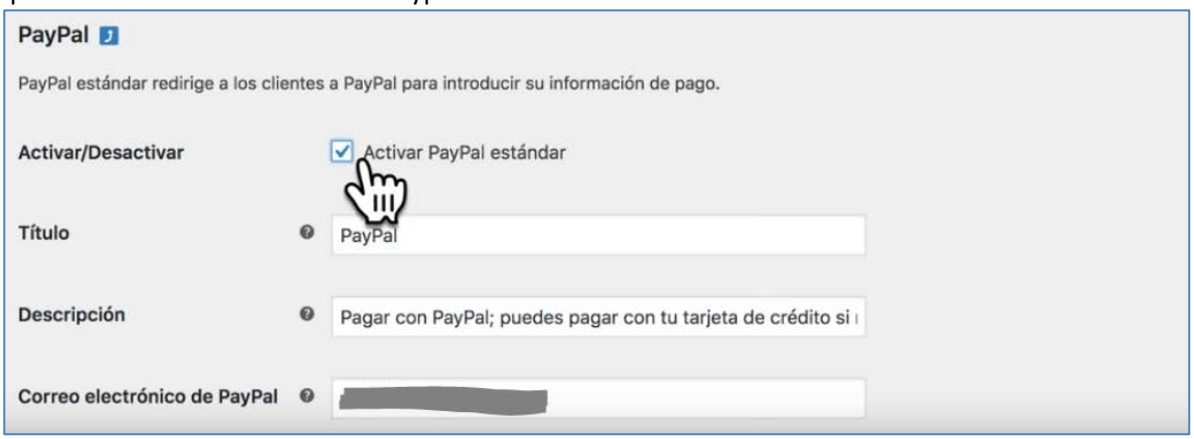
2. El siguiente paso es elegir el método de pago, para lo cual pulsamos sobre **Pagos** y activamos **Paypal**, previamente nos tendremos que haber dado de alta en Paypal para configurar que método queremos para recibir nuestros ingresos: abono en tarjeta, en cuenta corriente…



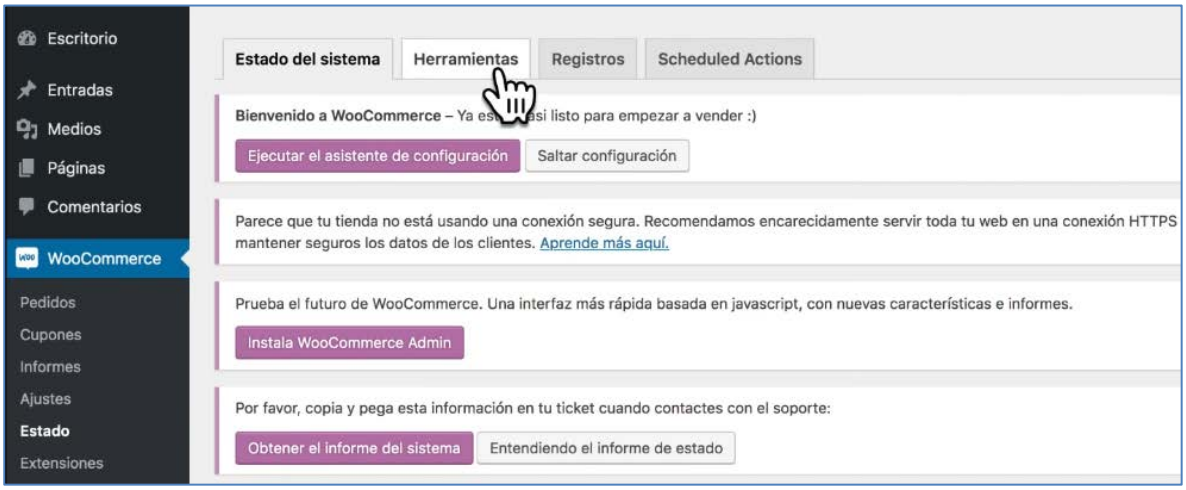
Bajamos hasta dónde pone **Métodos de Pago** y podemos ver muchos, nosotros en el apartado **Paypal** y pulsamos sobre **Configuración**



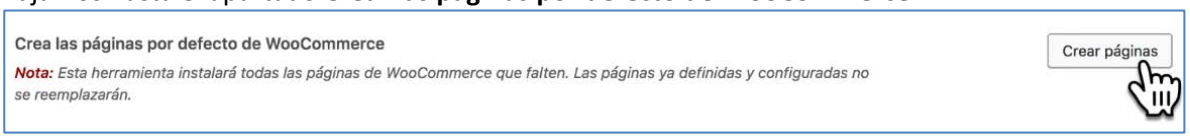
Y Luego sobre **Activar Paypal estándar** tendremos que indicar 2 veces la dirección de correo con la que nos hemos dado de alta en Paypal:



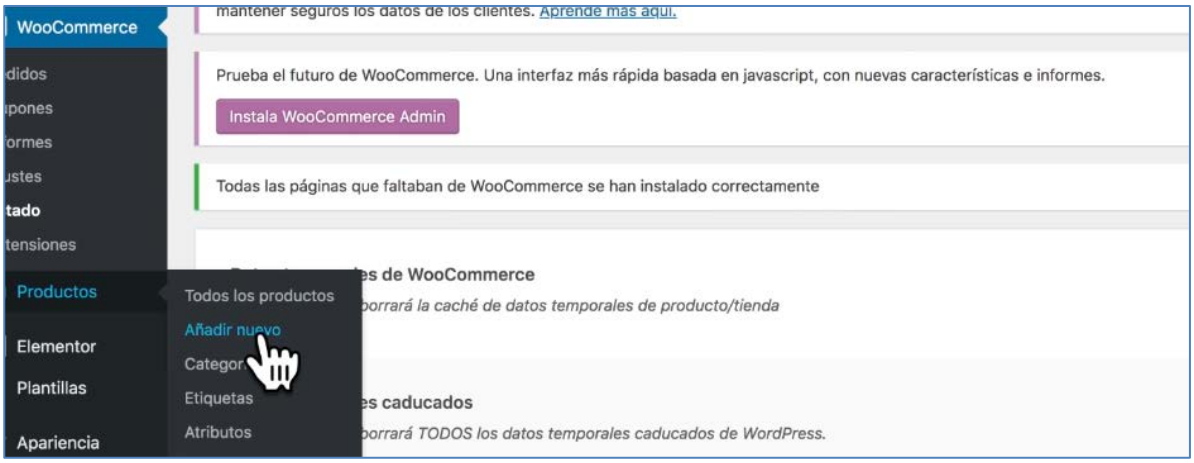
3. Luego creamos las páginas por defecto, para hacerlo pulsamos sobre **Woocomerce/Estado/Herramientas**



Bajamos hasta el apartado **Crear las páginas por defecto de WooCommerce**



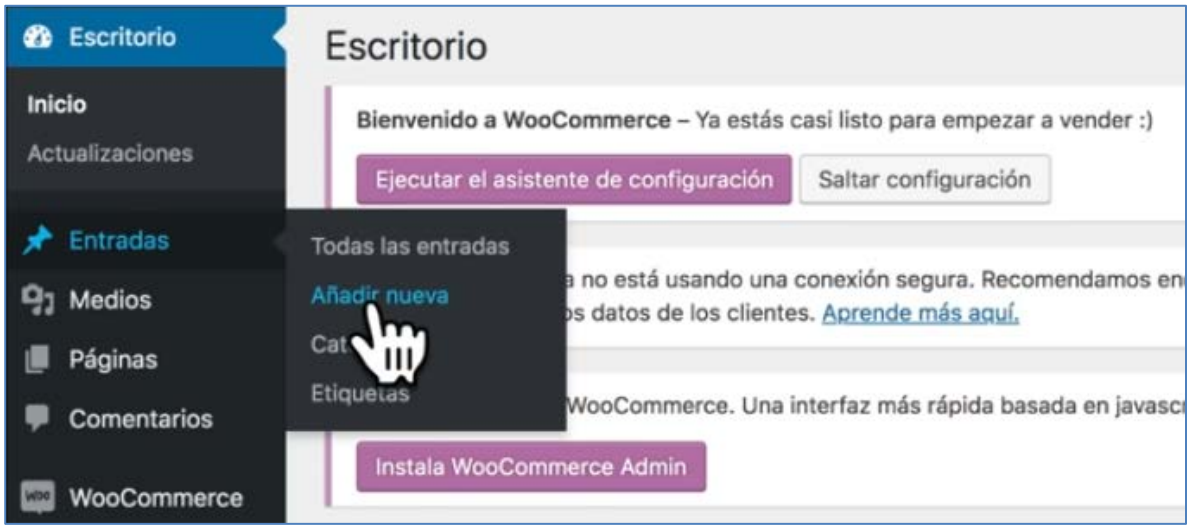
4. Y listo, ya solo queda Agregar nuestros productos para hacerlo simplemente vamos a Productos/Añadir nuevo



Dentro le daremos un: **Nombre, Descripción, Precio, Establecer Imagen de Producto Guardamos Cambios** y podemos ver como queda, incluso comprarlo en **Vista Previa del Producto**

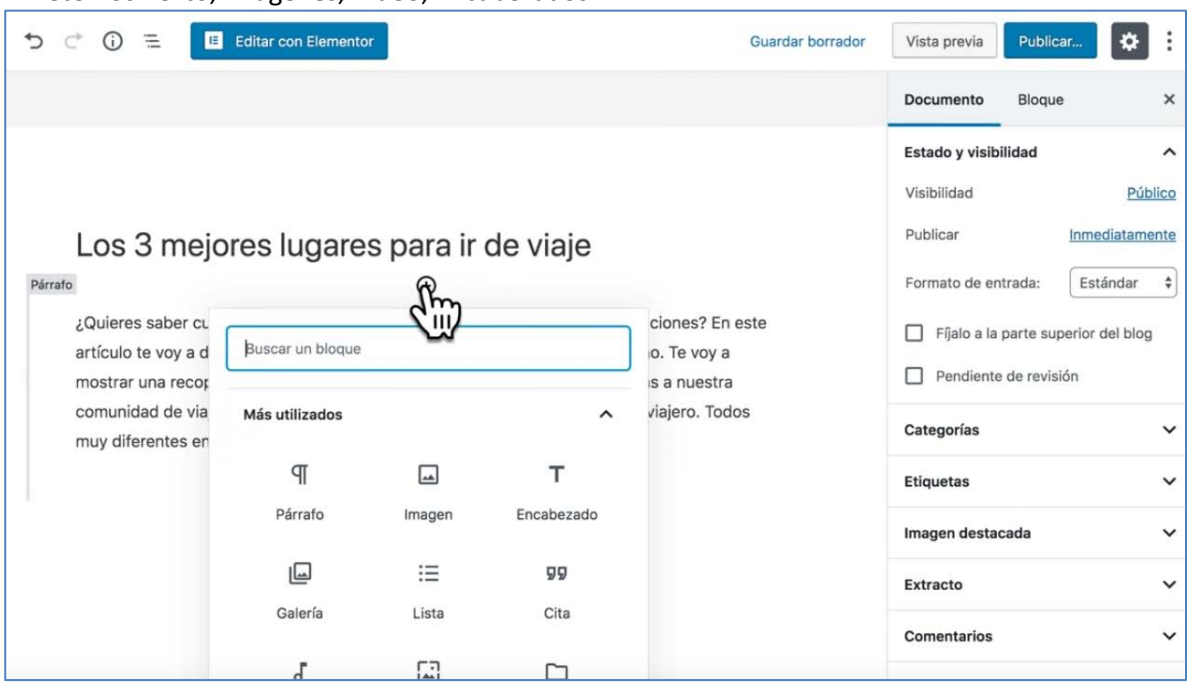
Crear un Blog

Entradas/Añadir Nueva

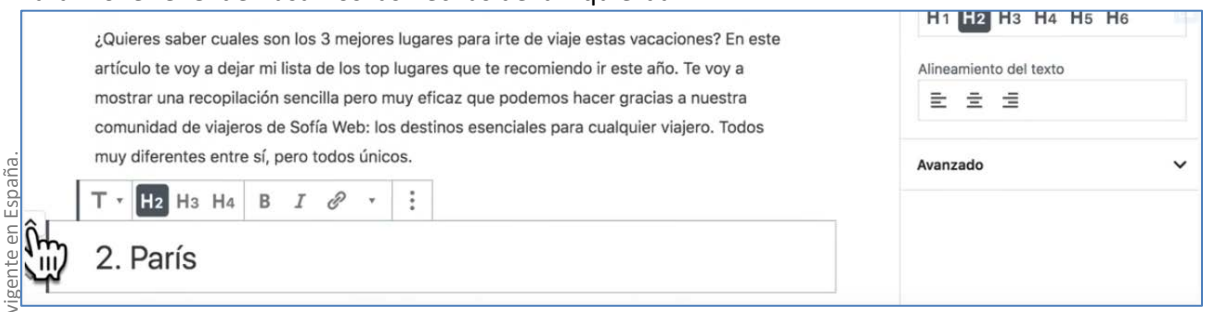


Ponemos un título atractivo

Y metemos Texto, Imágenes, Vídeo, Encabezados…



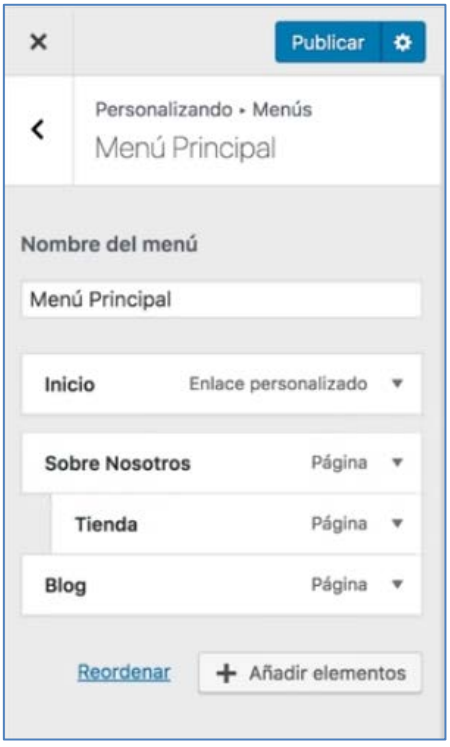
Para mover el Orden usamos las flechas de la izquierda:



Y para publicar el blog, porque lo que acabamos de crear es un artículo.
Viendo la vista previa del artículo Nos vamos a personalizar: **Ajustes de ´Página de Inicio** y luego en **Página de Entradas/Añadir Página Nueva** le damos un Nombre por ejemplo Blog y luego **Añadir** luego Publicamos

Para crear el menú:

1. Personalizar
2. Menus
3. Nuevo Menu
4. Le damos Nombre y Luego marcamos Menu Principal, luego Siguiente
5. Y en Elementos los vamos añadiendo: Inicio, Tienda, Carrito, Sobre Nosotros…
   Si queremos crear submenú simplemente arrastramos a la derecha un poco:



Ejercicio Individual – Crear Sitio Web Propio

Vais a realizar un ejercicio individual, el cual consiste en crear un sitio web propio que contenga una Página de Inicio, un par de páginas sobre la empresa, un blog y una tienda online realizada con WooCommerce.
Si no se os ocurre una Web propia, os propongo hacer una web sobre artículos de cocina.
Los pasos en general serán:

1 – Creamos un esquema de cómo queremos que sea nuestro sitio web:
- ⇨ Página de Inicio con 3 bloques: Bienvenidos, Servicios y Galería de Fotos
- ⇨ Página de Contacto con la Dirección, Teléfono, Mail, Redes Sociales…
- ⇨ Página Quienes somos
- ⇨ Blog de recetas de cocina
- ⇨ Tienda WooCommerce con artículos de cocina

2 – Obtenemos y Diseñamos todo el material gráfico
- ⇨ Nos metemos en **canva.com**, buscamos una plantilla logotipo y creamos el nuestro propio
- ⇨ Vamos a la página pexels.com/es-es y buscamos imágenes sobre cocina, necesitaremos varias:
  - o 1 imagen de fondo para la Bienvenidos
  - o Imágenes de cada uno de los servicios que ofrecemos: Cursos de Cocina, Venta de Artículos de Cocina, Servicio de Catering
  - o 6 Fotos para la Galería
  - o 1 Foto y 1 vídeo para quienes somos, que luego podemos retocar y montan con canva.com
  - o Varias fotos de recetas de cocina para el Blog
  - o Como vamos a vender artículos de cocina, al menos 2, 4 fotos de cada artículo que vendemos de cocina

3 – Creamos el sitio Web:
- ⇨ Arrancamos XAMPP (si no está ya en funcionamiento)
- ⇨ Creamos la Base de datos: **webcocina** para lo cual pulsamos sobre el botón **Admin** del servicio MySQL de XAMPP, nos vamos al apartado Bases de datos y escribimos el nombre de la base de datos **webcocina** y pulsamos sobre **Crear** luego nos vamos a privilegios y creamos el usuario **admin_cocina** el host **Local** y la contraseña **123456**
- ⇨ Copiamos la carpeta con la plantilla de wordpress a la carpeta de **htdocs** (si no sabemos llegar a c:\xampp\htdocs, buscamos htdocs en nuestro ordenador) y le cambiamos el nombre **webcocina**
- ⇨ Nos vamos en el navegador a **localhost/webcocina** e iniciamos el proceso de creación e instalación de wordpress 1º la Base de datos y luego el sitio y el usuario "cliente" en el cual ponemos, por ejemplo, nuestro nombre

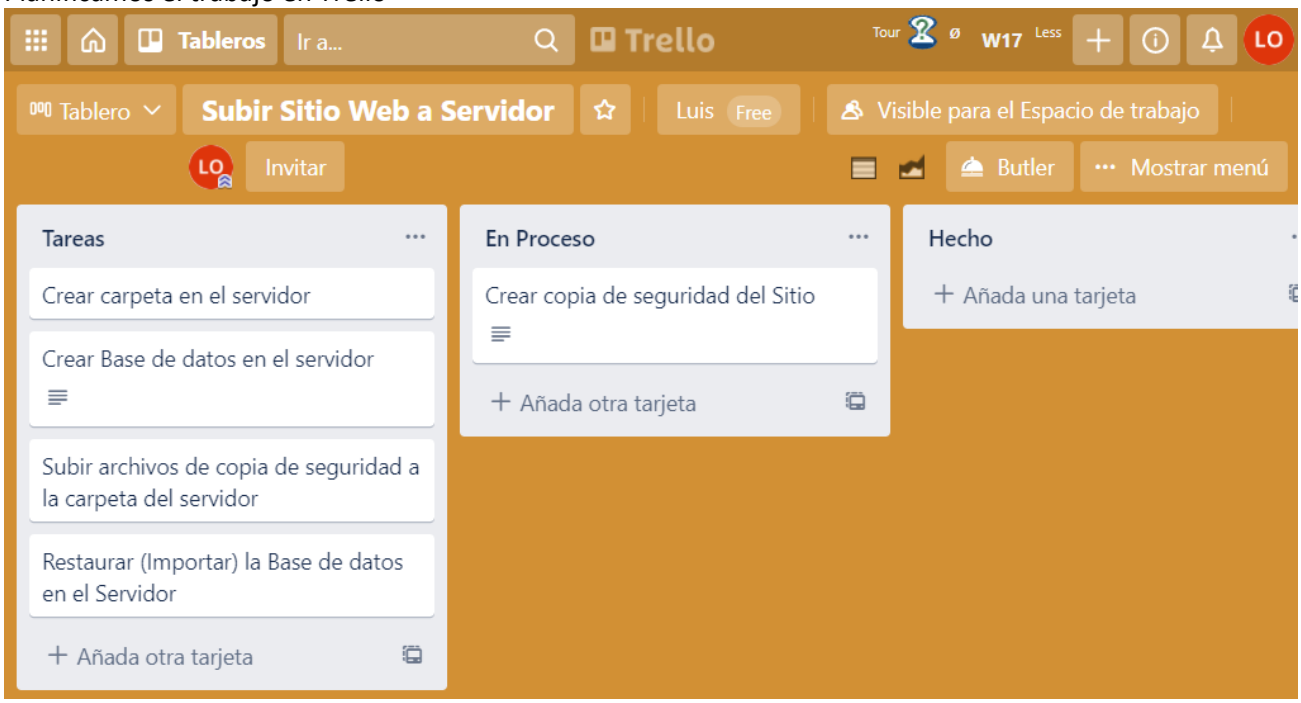
4 – Seleccionamos la plantilla y los plugins del sitio Web:
- ⇨ Borramos el contenido que aparece por defecto tanto de Páginas, Entradas como de Plugins
- ⇨ Seleccionamos la plantilla que vamos a usar, en este caso **Astra**
- ⇨ Instalamos el plugin **Elementor**

5 – Creamos el contenido de la página:
- ⇨ Vamos a **localhost/webcocina** cambiamos a la vista pública: frontend (botón casita), pulsamos sobre **Personalizar** y definimos el **encabezado** (Logotipo) y el **pie** (copyright)
- ⇨ Volvemos al entorno de administración backend (botón casita) y creamos una nueva Página desde **Página/Añadir Nueva** llamada **Inicio** la cual editamos con **Elementor** y añadimos los bloques deseados con las 3 secciones que hemos establecido antes: Bienvenidos, Servicios y Galería de Fotos
- ⇨ Cambiamos al frontend (botón casita) y pulsamos sobre el botón personalizar para establecer la página de inicio desde **Ajustes de Portada/Página de Inicio**
- ⇨ Volvemos al backend (botón casita) y creamos otras 2 páginas desde **Página/Añadir Nueva** llamadas Contacto y Quienes somo las cuales Editamos también con Elementor
- ⇨ Creamos las entradas del blog, desde **Entradas/Añadir Nueva**
- ⇨ Pulsamos sobre la casita para ir al frontend y en Ajuste de **Portada/Página de Entradas/Añadir Página Nueva** le damos nombre: Blog y luego Añadir

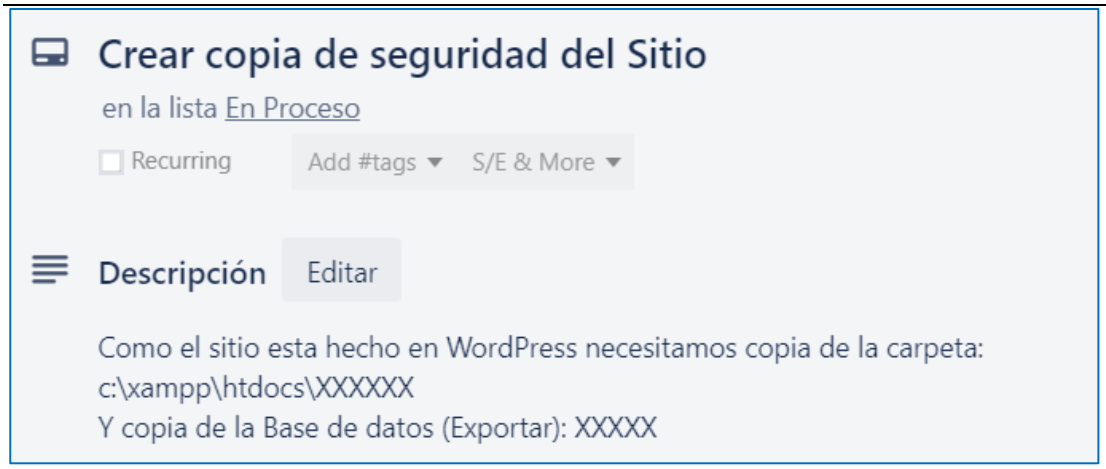
- ⇨ Volvemos al backend y vamos al apartado de pulgins para Añadir Nuevo y buscamos Woo para localizar el plugin WooCommerce, lo instalamos, podemos saltarnos los procesos de creación de la tienda física, ya lo haremos más adelante
- ⇨ Para empezar a funcionar con WooCommerce simplemente configuramos la moneda desde Woocomerce/Ajustes, pestaña de General bajamos hasta **Moneda**, luego pulsamos sobre **Pagos** y activamos Paypal y por último creamos las páginas por defecto, para hacerlo pulsamos sobre Woocomerce/Estado/Herramientas **Crear las páginas por defecto de WooCommerce**
- ⇨ Añadimos 2 productos nuevos desde **Productos/Añadir nuevo**
- ⇨ Y por último organizamos los menús desde el frontend, pulsamos sobre Personalizar, Menus
- ⇨ Nuevo Menu, le damos Nombre, marcamos Menu Principal, y añadimos los diferentes elementos

Subir Página Web a servidor:

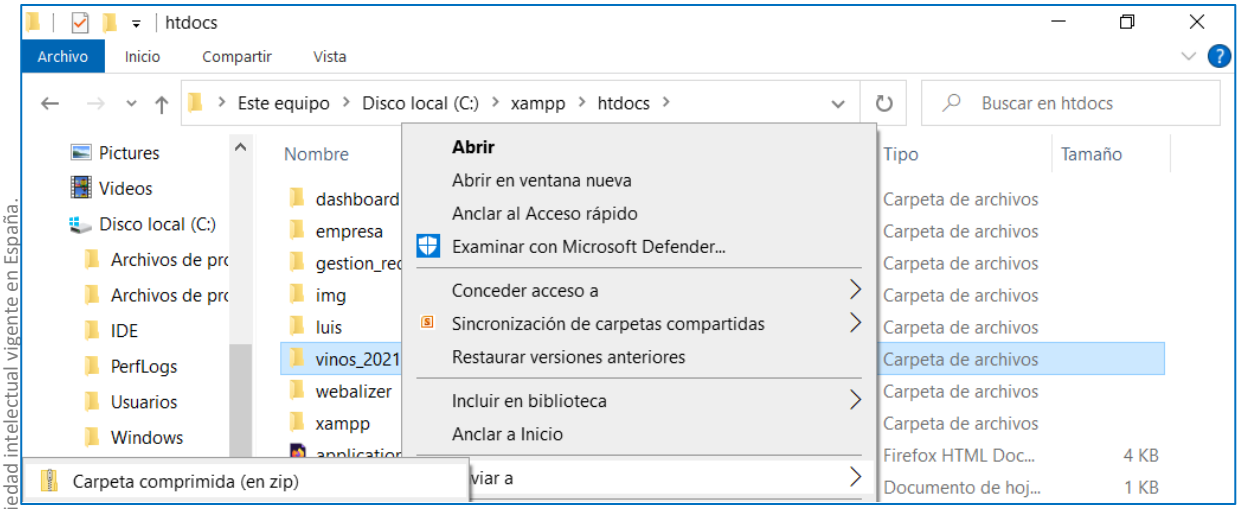
Planificamos el trabajo en Trello



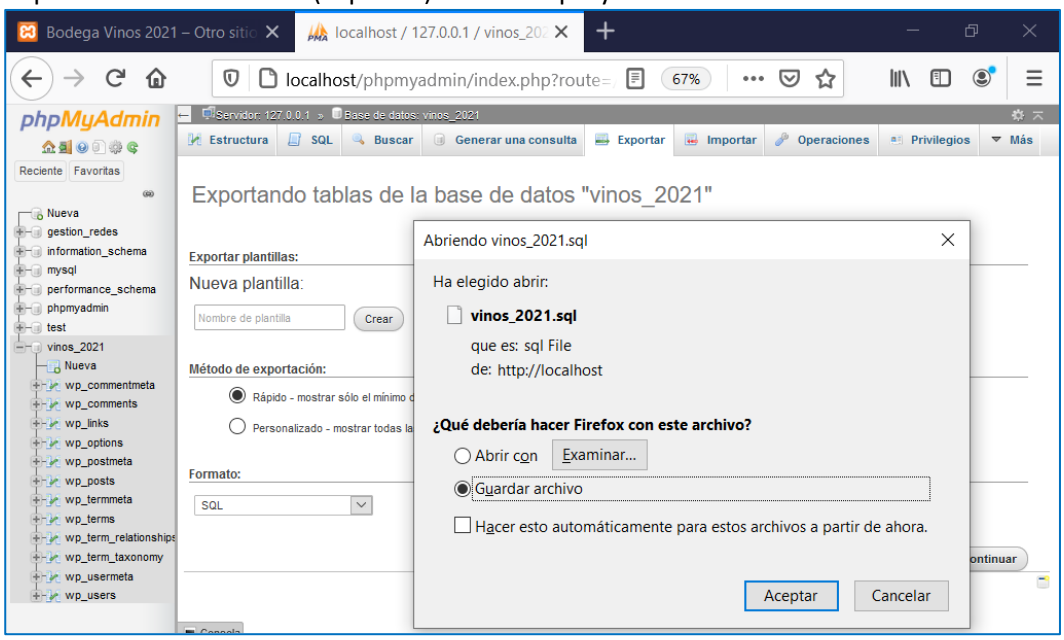
Tarea 1: Crear copia de seguridad del Sitio: archivos y base de datos



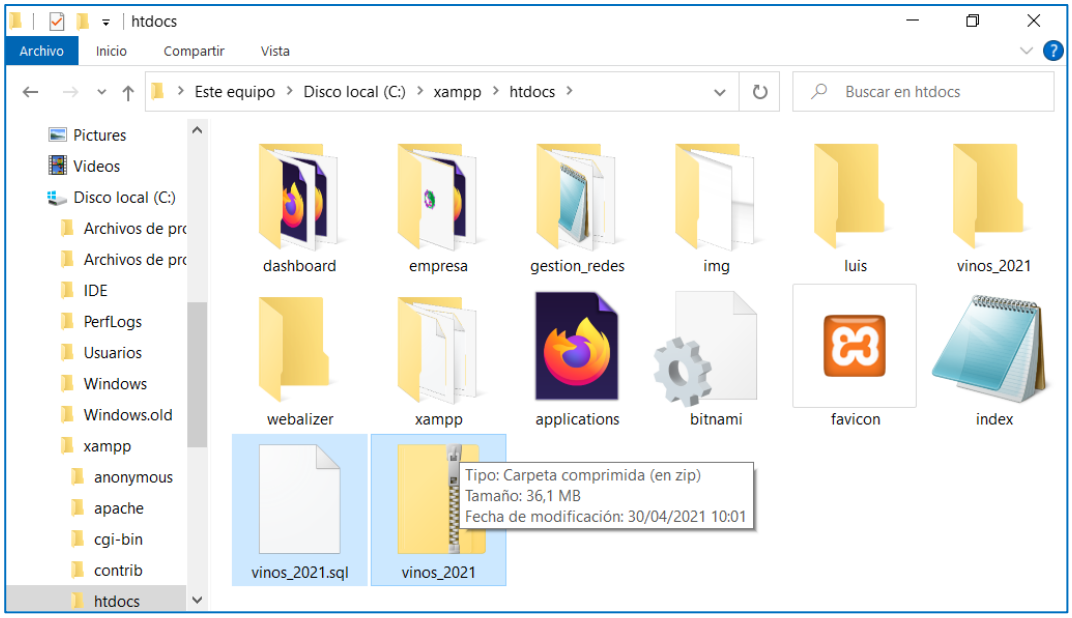
Copiar archivos, en c:\xampp\htdocs\XXXX con el botón derecho pulsamos sobre crear archivo comprimido



Copia de la Base de datos (exportar): Desde PhpMyAdmin

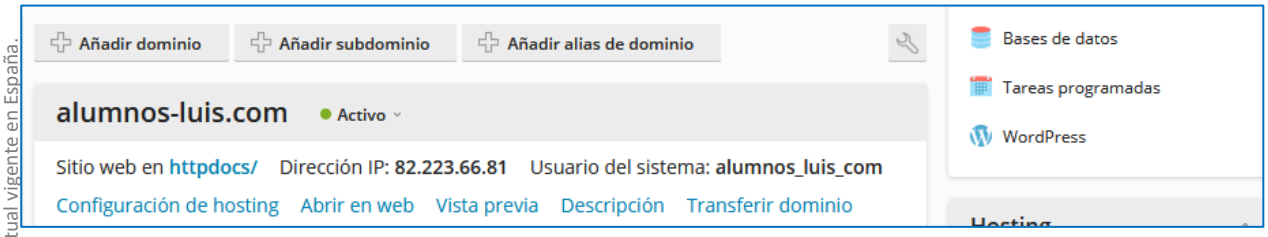


Ya podemos ver los archivos de la copia de seguridad:

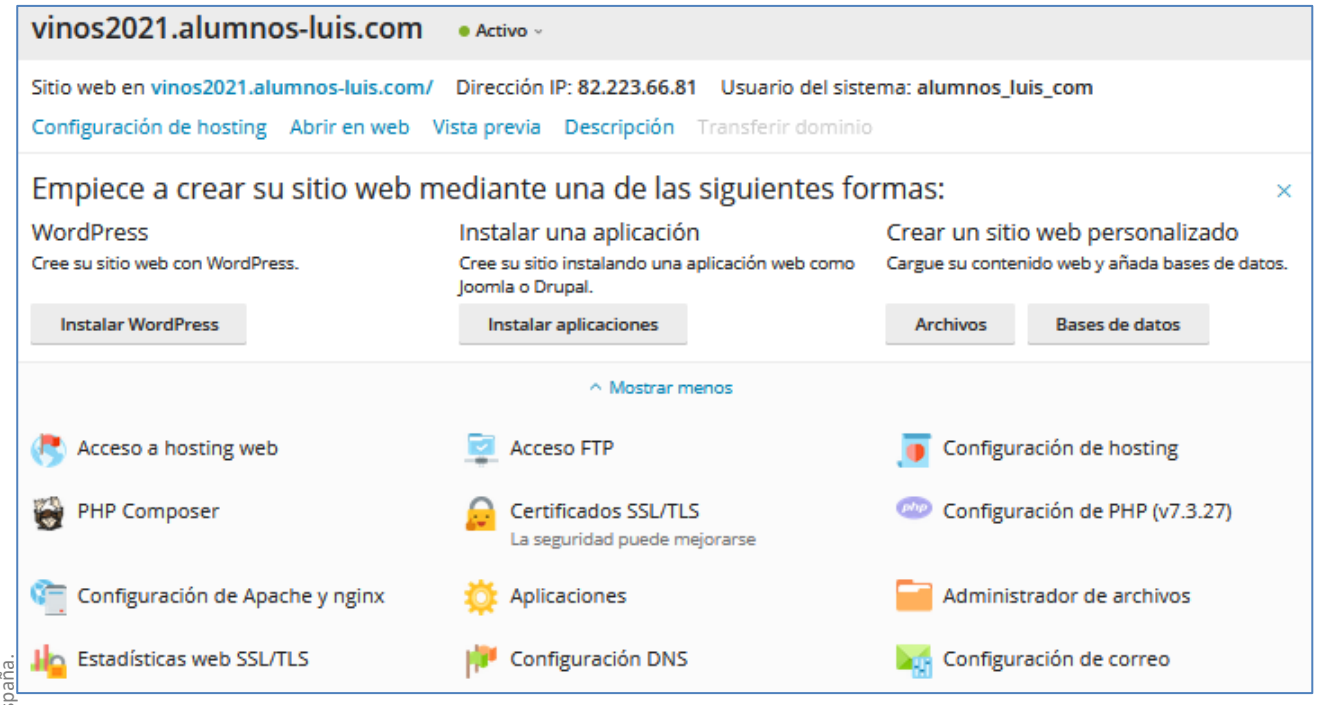


Tarea 2. Creamos la carpeta del Sitio

En este caso vamos a crear un sub-dominio del dominio principal alumnos.luis.com usando una consola de gestión llamada Plesk (existen otras muchas en el mercado CPanel algunas incluso opensource como ISPConfig)

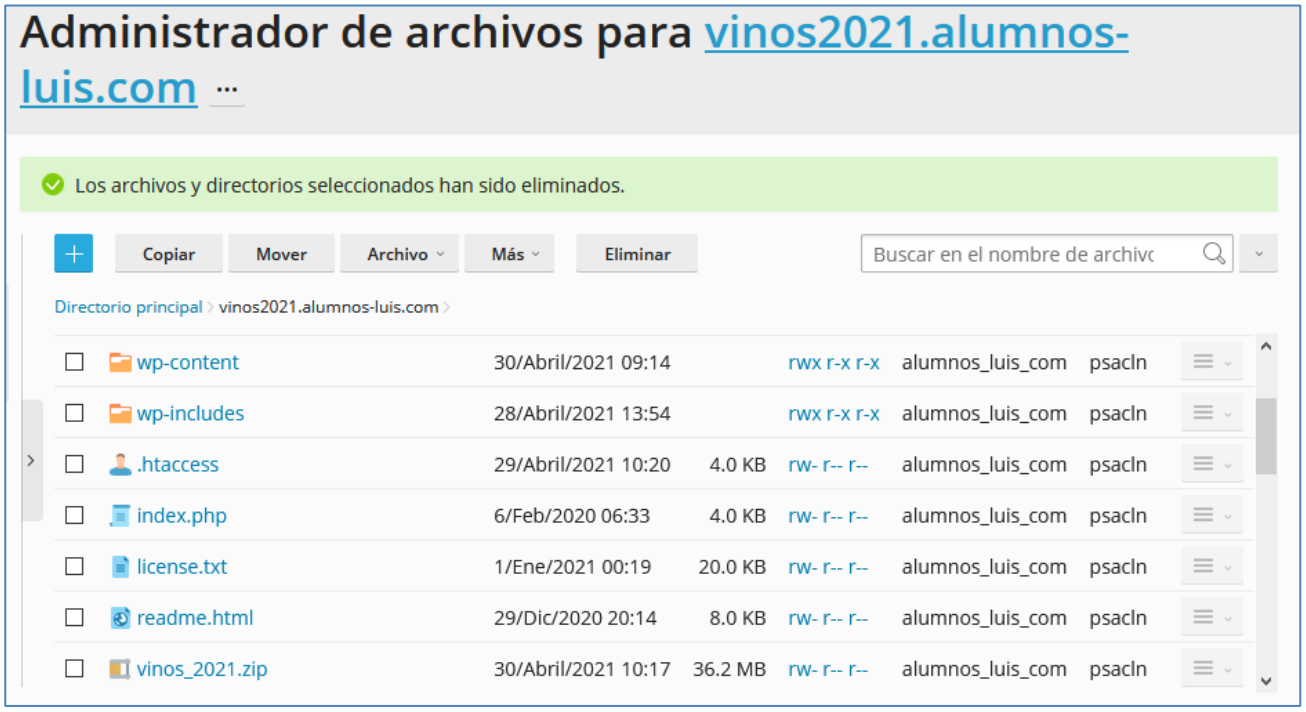


Para subir los archivos que antes hemos copiado (la carpeta comprimida) pulsamos sobre **Administrador de archivos**

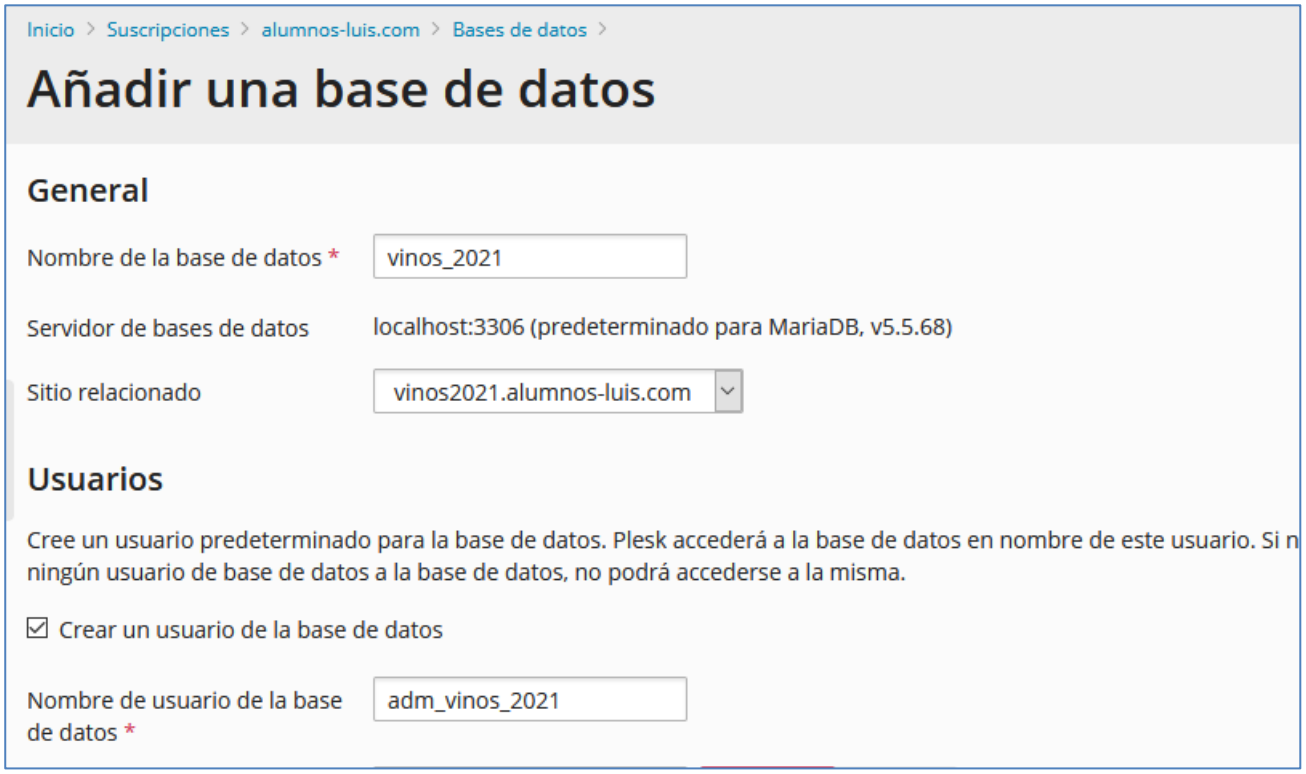


Pulsamos sobre el **+** y luego sobre **Cargar archivos**

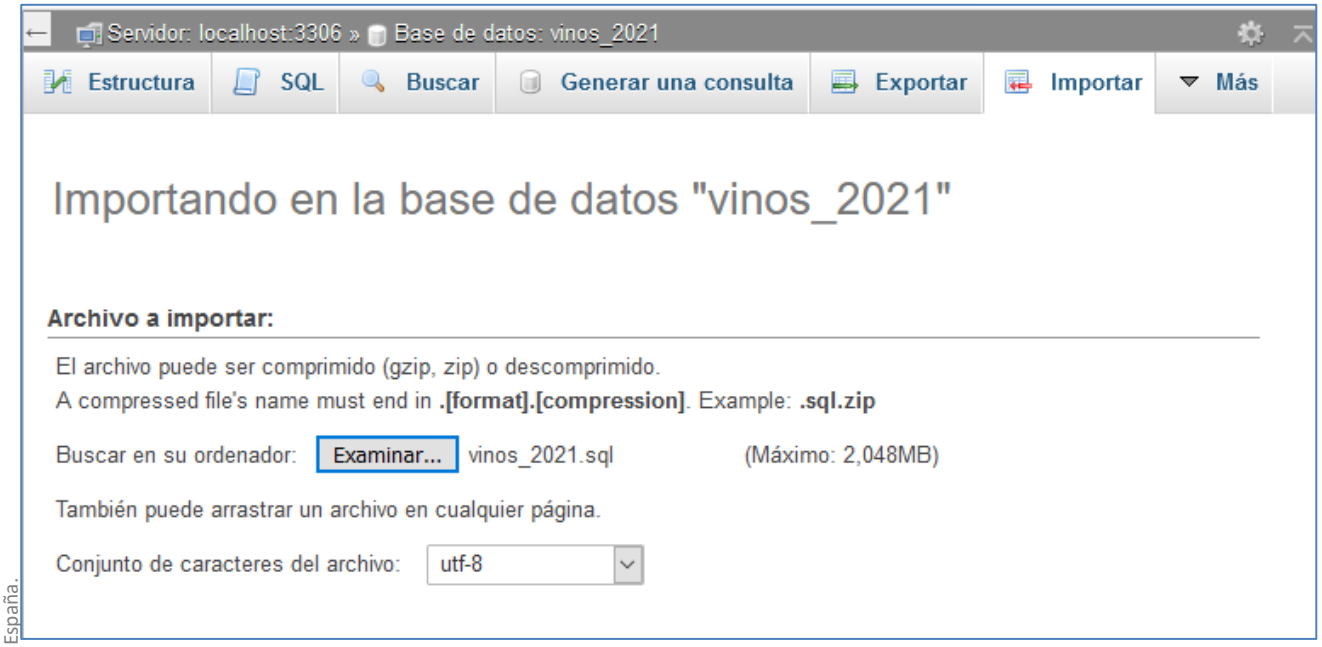
Y finalmente descomprimimos el archivo, pulsando sobre **Archivo/Descomprimir**



Volvemos amla pantalla principal del dominio y pulsamos sobre **Bases de datos** y seleccionamos crear nueva base de datos **Añadir una base de datos**:



Y una vez creada pulsamos sobre **PhpMyAdmin** y solo nos quedaría **Importarla** buscando el archivo SQL que hemos exportado en los pasos anteriores.



1. Continuación

1.3.2. Funciones de los protocolos

Cada protocolo tiene claramente definidas una serie de funciones dependiendo del nivel al que corresponda y del sistema de comunicaciones al que pertenezca.
Pero todas ellas tienen una serie de funciones genéricas que son las siguientes:

- Permitir localizar un equipo u ordenador de forma inequívoca.
- Permitir realizar las conexiones entre equipos u ordenadores.
- Permitir que la comunicación sea segura y fiable e independiente de la arquitectura de los equipos que se conecten (PC sobremesa o portátil, Mac, etc.), es decir permitir la interoperabilidad de equipos.
- Abstraer a los usuarios de los enlaces utilizados (red telefónica, radioenlaces, satélite, etc.) para el intercambio de información.
- Permitir liberar la conexión de forma ordenada.

1.3.3. El modelo de referencia OSI. Funciones y servicios

El modelo OSI (Open System Interconnection) es un estándar europeo que permite que diferentes dispositivos con arquitectura distinta puedan interactuar y comunicarse entre sí.
Es por tanto un estándar abierto que permite la 'interoperabilidad' de los dispositivos, especialmente de comunicaciones.
Fue desarrollado por la International Organization for Standarization (ISO) en 1984.
Este modelo crea una arquitectura por niveles para el diseño de sistemas de red. La creación de los niveles parte de la idea de 'dividir un problema en tareas o procesos más pequeños para su mejor diseño y operatividad'.
Este modelo está basado en siete niveles o capas:

1. Nivel físico.
2. Nivel de enlace.
3. Nivel de red.
4. Nivel de transporte.
5. Nivel de sesión
6. Nivel de presentación.
7. Nivel de aplicación.

Casi todas las aplicaciones suelen 'correr' en la capa de aplicación. Cuando se quiere conectar a otro equipo o dispositivo se debe conectar con la misma aplicación en el nivel de aplicación del otro equipo. Para ello la información a enviar debe 'pasar' por la torre de capas de cada uno de los equipos o dispositivos.
La capa de PRESENTACIÓN pasa sus datos a la capa de SESIÓN, CAPA 5, y así sucesivamente, hacia abajo, hasta llegar a la capa FÍSICA, CAPA 1.
Para llegar a B el proceso es al contrario.

Los siete niveles se pueden agrupar en **tres subgrupos**.
Los niveles **1, 2 y 3** (físico, de enlace y de red) son los **niveles de soporte de red** (son los más importantes por el operador de telecomunicaciones ya que son tratados por éste). Su funcionalidad está relacionada con los aspectos físicos de la transmisión de los datos de un dispositivo a otro.
El **nivel 4** (de transporte) es el encargado de la **transmisión fiable de la información de un extremo a otro**.
Y por último, los niveles siguientes **5, 6 y 7** (de sesión, presentación y aplicación) proporcionan **servicios de soporte de usuario** y permiten la interoperabilidad entre sistemas **software**.

Los **niveles superiores** se implementan casi siempre mediante **software** siendo **los niveles más bajos una combinación entre software y hardware**. **El último nivel** -nivel físico-, se implementa casi en su totalidad mediante **hardware**.
A continuación vamos a ver con detalle las funciones y tareas que realiza cada capa o nivel en el proceso de transmisión de la información.

La capa física

Corresponde a la capa de nivel 1 del modelo OSI y describe las reglas para poner y extraer los bits del medio de transmisión empleado en la red, es decir, se encarga de la transmisión del flujo de bits.
En esta capa o nivel se define:

- El medio de transmisión empleado: coaxial, fibra, wifi, PLC, etc.
- Sus características o interfaces físicos: voltajes, amperaje, conectores, etc.
- Los dispositivos físicos empleados en la red.
- La tasa de transmisión (en bits por segundos).
- La representación de los bits: en señales eléctricas, ópticas, etc.
- La topología física de cómo están conectados los dispositivos.
- El modo de transmisión: simplex, semi-dúplex, full-dúplex. Es por tanto el nivel más 'hardware' de toda la comunicación IP.

La capa de enlace

Corresponde a la capa de nivel 2 del modelo OSI y es la encargada de la transmisión fiable de la comunicación nodo a nodo. Es decir, toda la comunicación realizada entre nodos adyacentes es correcta y libre de errores. Todo ello se consigue en un **control de los paquetes enviados**.
Son funciones de esta capa las siguientes tareas:

- **Agrupar** el flujo de bits en unidades de datos (**tramas**) con una longitud específica de bits. Ahora se manejan tramas y no bits.
- **Direccionar** físicamente las tramas, es decir, enviar las tramas a sus destinos correctos añadiendo en la trama una cabecera (**cabecera de trama**) que indica el nodo destino al que va dirigido (también se incluye la dirección del nodo emisor).
- Realizar el **control de flujo**, es decir, adaptar la velocidad de transmisión a la velocidad que acepta la red o que puede soportar el receptor evitando así colapsos o desbordamiento de la red o del receptor respectivamente.
- Realizar el primer **control de errores**, es decir, se añaden bits de redundancia o de paridad para asegurar que la trama recibida es correcta y no ha sido alterada en la transmisión.

Esta capa de enlace a su vez se divide en dos subcapas: capa MAC y capa LLC (Control de enlace lógico), siendo la primera más 'hardware' al estar más vinculada a la capa física.
Funcionamiento de Ethernet

La capa de red

Corresponde a la capa de nivel 3 del modelo OSI y es la encargada de la entrega de paquetes IP desde el emisor hasta el receptor a través de toda las redes subredes que existan en la transmisión. Asegura que el paquete llega al destino correcto.
Son funciones de esta capa las siguientes tareas:

- Realizar el direccionamiento lógico, es decir, añade una cabecera (cabecera de red) al paquete donde se añade la dirección lógica (no física) del emisor y del receptor para que el paquete llegue al destino deseado (las direcciones físicas van cambiando cuando se 'traspasan' diversas redes).
- Realizar el encaminamiento, es decir, para interconectar diferentes redes se utilizan dispositivos como router o pasarelas las cuales requieren 'enrutar' el paquete a la red de destino correcto.

La capa de transporte

Corresponde a la capa de nivel 4 del modelo OSI y es la encargada de la entrega extremo a extremos de paquetes IP asegurando una transmisión correcta y libre de errores. Esto se consigue con la creación de un 'túnel' lógico entre emisor y receptor que se libera con la finalización de la transmisión.

Para asegurar la transmisión fiable y libre de errores, en esta capa se realiza un control de errores y control de flujo de los paquetes enviados.
Es responsable de esta capa:

- Realizar el direccionamiento del punto de servicio, es decir, añade una cabecera (cabecera de transporte) al paquete donde se añade el proceso al que va dirigido los paquetes, es decir, se añade el puerto (tanto en origen como en destino).
- Realizar el encaminamiento: para interconectar diferentes redes se utilizan dispositivos como router o pasarelas las cuales requieren 'enrutar' el paquete a la red de destino correcto.
- Realizar la segmentación y reensamblado, es decir, los mensajes se dividen en segmentos, que son la unidad que se transmite y se la asigna un número de secuencia para luego poder ordenarlos en recepción y conseguir así la transmisión correcta y en orden.
- Realizar el control de conexión, es decir, dado que en este nivel se debe crear un conexión o 'túnel' virtual entre emisor y receptor, se debe gestionar el establecimiento de la conexión, la transferencia de datos y la liberación de la conexión.
- Realizar el control de flujo extremo a extremo.
- Realizar el control de errores extremo a extremo. En este caso cuando un segmento ha llegado con error, se corrige con retransmisiones del paquete o segmento erróneo.
- UDP y TCP.

Capa de Sesión

Corresponde a la capa de nivel 5 del modelo OSI y se encarga de establecer, mantener y sincronizar la interacción en una sesión de comunicación entre dos equipos.
Es responsabilidad de esta capa:

- El control de diálogo, es decir, se establece qué tipo de comunicación se va a dar entre los dos equipos: simplex, semi-dúplex o full-dúplex.
- La sincronización: se añaden puntos de prueba en una transmisión para asegurar que las transmisiones anteriores han llegado correctamente y no se realizan nuevas transmisiones hasta haberse asegurado la recepción correcta de los paquetes anteriores. Ello se consigue insertando 'checkpoints' en diversos puntos de la transmisión.

La capa de presentación

Corresponde a la capa de nivel 6 del modelo OSI y se encarga de la sintaxis y la semántica de la información intercambiada entre los dos equipos intercomunicados.
Para lograr lo anterior se realiza:

- La traducción, en ella cada máquina o equipo puede manejar la información en distintos formatos o codificación, y en esta capa se traduce dicha información en un formato de flujo de bits para que pueda ser transmitida y luego en el receptor 'descifrarla' y presentarla en el formato adecuado que pueda entenderlo el receptor o como espera recibirlo. Por ejemplo en esta capa se realiza la compresión de video en formatos MPEG-2, MPEG-4 o formatos como JPEG, MP3, etc.
- El cifrado: para asegurar una transmisión segura y privada libre de posible ataques exteriores, en esta capa se realiza el cifrado de la información transmitida. Esta es una tarea cada vez más importante en todas las transmisiones IP dado que la información se transmite por canales inseguros como Internet.

La capa de aplicación

Corresponde a la capa de nivel 7 y última del modelo OSI y es la que proporciona el interfaz con el usuario y toda su gestión y soporte.
En esta capa o nivel es donde se encuentran los diversos servicios o protocolos que se emplean en las comunicaciones:

- Servicio de http: es el servicio de hipertexto o navegación por internet.
- Servicio de ftp: es el servicio de transferencia de archivos a través de una red.
- Servicio de smtp: es el servicio de correo electrónico.

- Servicio de telnet: es el servicio de acceso remoto a máquinas o equipos a través de una red.
- Servicio de directorio: es el servicio del Active Directory o acceso a bases de datos distribuidas.

1.3.4. La arquitectura de protocolos TCP/IP. Funciones y servicios

El modelo TCP/IP es un estándar americano que permite que diferentes dispositivos con arquitectura distinta puedan interactuar y comunicarse entre sí.
Es el equivalente al modelo OSI y ha sido el estándar utilizado por Internet por lo que es el modelo más ampliamente utilizado.
Fue desarrollado durante la época de los años 60 por el Departamento de Defensa de los EE.UU. En plena época de la Guerra Fría se usó como medida de defensa en las comunicaciones militares. Más tarde se hizo popular entre las universidades y empresas, y en los años 90 se extendió al público en general.
Este modelo se basa al igual que el modelo OSI en una arquitectura por capas o niveles.
Su arquitectura consta de cinco niveles, que aunque no coincide 'exactamente' con el modelo OSI, en su conjunto realiza las mismas funciones:

- Nivel de acceso a la red.
- Nivel de red.
- Nivel de transporte.
- Nivel de aplicación.

Al igual que en el modelo OSI, los datos descienden por la pila de protocolos en el sistema emisor y escalan en el extremo receptor. Cada capa de la pila añade datos a la capa inferior, información de control para que el envío sea correcto.
Esta información de control se denomina cabecera, pues se coloca precediendo a los datos. A la adición de esta información en cada capa se le denomina encapsulación.
Cuando los datos se reciben, tiene lugar el proceso inverso, es decir, según los datos ascienden por la pila, se van eliminando las cabeceras correspondientes.
Cada capa de la pila tiene su propia forma de entender los datos y, normalmente, una denominación específica. Sin embargo, todos son datos a transmitir, y los términos sólo nos indican la interpretación que cada capa hace de dichos datos.

Nivel de acceso a la red

Este nivel recibe muchos nombres en función de la bibliografía consultada. En todos los casos se refiere al nivel más hardware del modelo TCP/IP y es la que se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico y posteriormente otro.
Realiza las funciones equivalentes al nivel físico y de enlace del modelo OSI, por lo que en algunas bibliografías la capa se divide en estos dos niveles.

Nivel de red

También denominada "capa de Internet", tiene como misión principal la de enviar paquetes origen desde cualquier punto de la red y que lleguen a su destino independientemente de la ruta y de las redes que hayan recorrido para llegar hasta allí.
El protocolo específico que rige esta capa se denomina Protocolo Internet (IP). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes. Esto se puede comparar con el sistema postal, ya que cuando se envía una carta por correo, no se sabe cómo llega a su destino (existen varias rutas posibles); lo que interesa es que la carta llegue.

Nivel de Transporte

El nivel o capa de transporte se responsabiliza de los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores.
Uno de sus protocolos, el protocolo para el control de la transmisión (TCP), ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo.
TCP es un protocolo orientado a la conexión.
Mantiene un diálogo entre el origen y el destino mientras empaqueta la información de la capa de aplicación en unidades denominadas segmentos. Que esté orientado a la conexión no significa que el

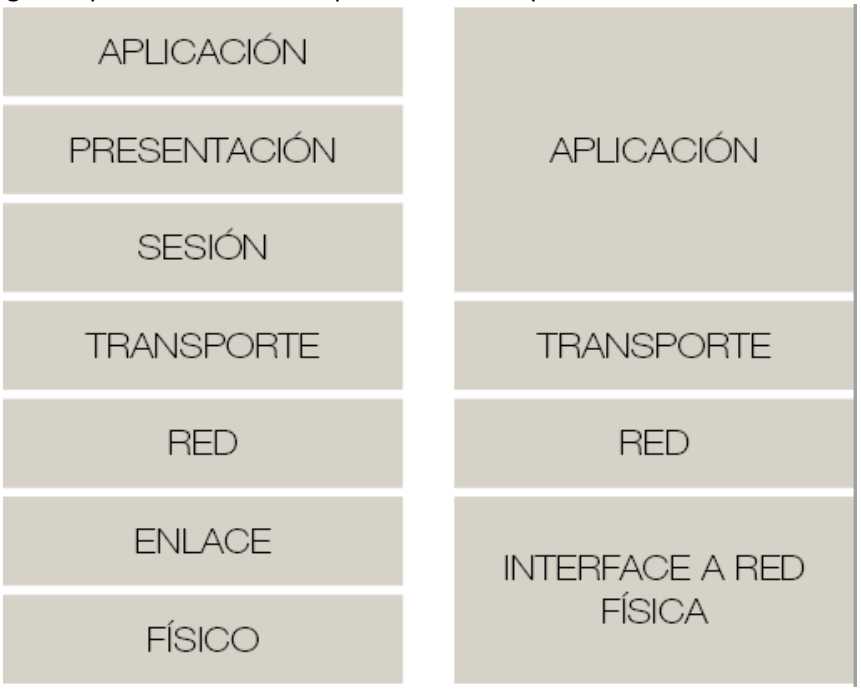
circuito exista entre los ordenadores que se están comunicando (esto sería una conmutación de circuito), esto significa que los segmentos de Capa 4 viajan de un lado a otro entre dos hosts para comprobar que la conexión existe lógicamente para un determinado período. Esto se conoce como conmutación de paquetes.

Nivel de Aplicación

En el modelo TCP/IP, los niveles de sesión, presentación y aplicación se integran en un único nivel: nivel de aplicación. Con esto se pretende que una capa de aplicación maneje protocolos de alto nivel, aspectos de representación, codificación y control de diálogo.
El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y garantiza que estos datos estén correctamente empaquetados para la siguiente capa.

1.3.5. Correspondencia entre TCP/IP y OSI

En la siguiente imagen se puede observar la equivalencia de capas entre ambos niveles: OSI y TCP/IP.



Comparación entre el modelo OSI y el modelo TCP/IP

Similitudes:

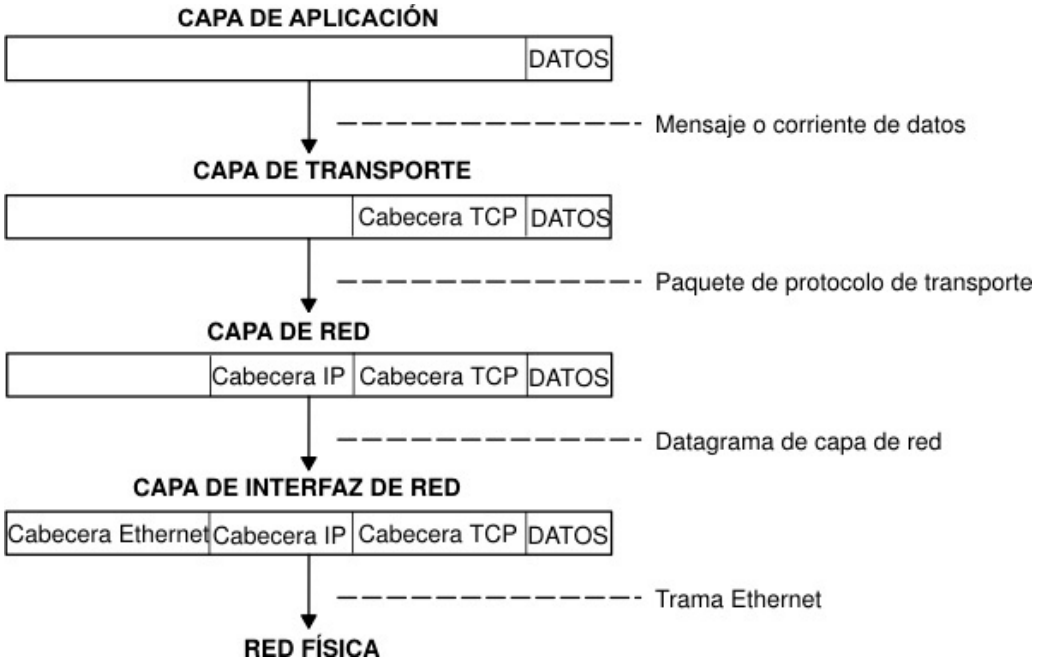
- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.
- Se supone que la tecnología es de conmutación por paquetes (no de conmutación por circuito).
- Los profesionales de redes deben conocer ambos.

Diferencias:

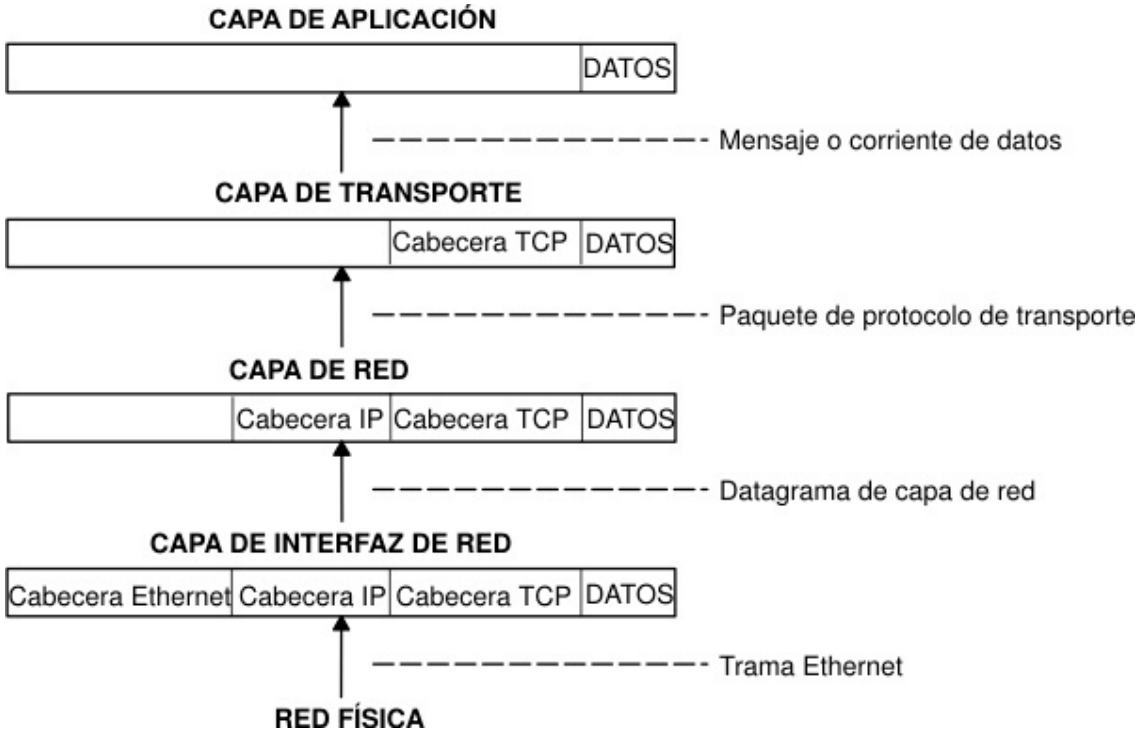
- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.
- TCP/IP combina las capas de enlace de datos y la capa física del modelo OSI en una sola capa.
- TCP/IP parece ser más simple porque tiene menos capas.
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, las redes típicas no se desarrollan normalmente a partir del protocolo OSI, aunque el modelo OSI se usa como guía.

TCP/IP define cuidadosamente cómo se mueve la información desde el remitente hasta el destinatario. En primer lugar, los programas de aplicación envían mensajes o corrientes de datos a uno de los protocolos de la capa de transporte de Internet, UDP (User Datagram Protocol) o TCP (Transmission Control Protocolo). Estos protocolos reciben los datos de la aplicación, los dividen en partes más pequeñas llamadas paquetes,

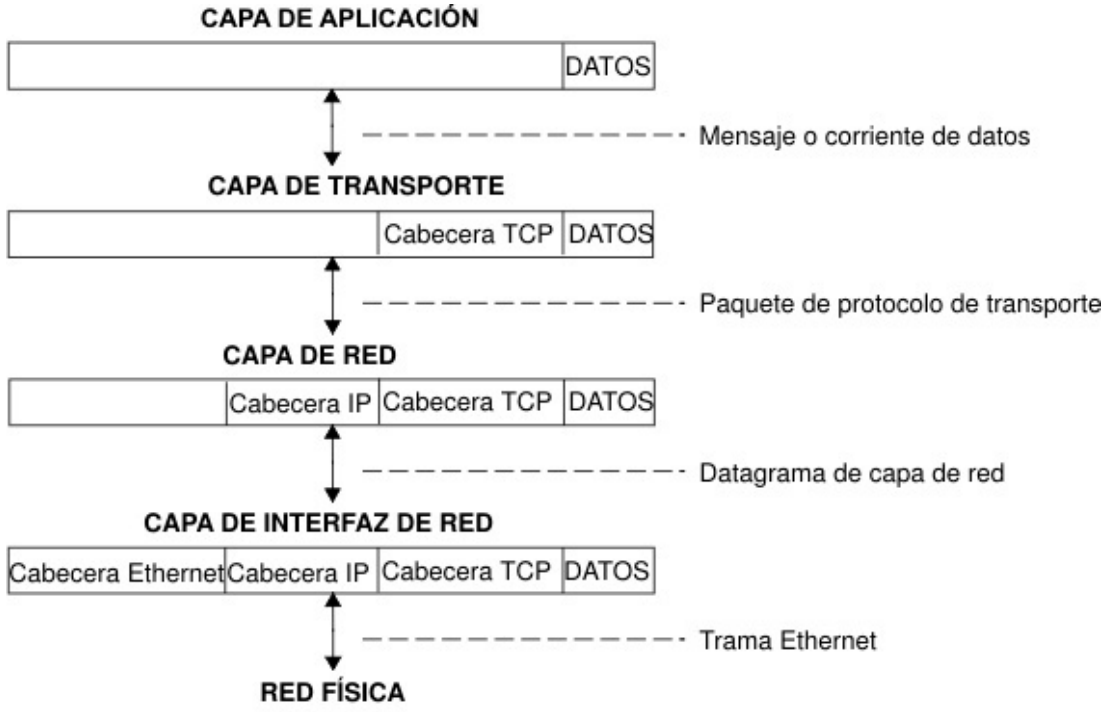
añaden una dirección de destino y, a continuación, pasan los paquetes a la siguiente capa de protocolo, la capa de red de Internet.
La capa de red de Internet pone el paquete en un datagrama de IP (Internet Protocol), pone la cabecera y la cola de datagrama, decide dónde enviar el datagrama (directamente a un destino o a una pasarela) y pasa el datagrama a la capa de interfaz de red.
La capa de interfaz de red acepta los datagramas IP y los transmite como tramas a través de un hardware de red específico, por ejemplo redes Ethernet o de Red en anillo.



Esta figura muestra el flujo de información de las capas de protocolo TCP/IP del remitente al host.
Las tramas recibidas por un sistema principal pasan a través de las capas de protocolo en sentido inverso. Cada capa quita la información de cabecera correspondiente, hasta que los datos regresan a la capa de aplicación.



Esta figura muestra el flujo de información de las capas de protocolo TCP/IP desde el sistema principal al remitente.
La capa de interfaz de red (en este caso, un adaptador Ethernet) recibe las tramas. La capa de interfaz de red quita la cabecera Ethernet y envía el datagrama hacia arriba hasta la capa de red. En la capa de red, Protocolo Internet quita la cabecera IP y envía el paquete hacia arriba hasta la capa de transporte. En la capa de transporte, TCP (en este caso) quita la cabecera TCP y envía los datos hacia arriba hasta la capa de aplicación.
Los sistemas principales de una red envían y reciben información simultáneamente. Esta imagen representa de forma más precisa un sistema principal mientras se comunica.



Nota: las cabeceras se añaden y separan en cada capa de protocolo a medida que los host transmiten y reciben datos.

1.4. Reglamentación y Organismos de Estandarización. IETF. ISO. ITU. ICT

Como ya se ha mencionado antes, los protocolos OSI y TCP/IP han sido diseñados y gestionados por una serie de organizaciones internaciones gubernamentales. Son los encargados de la estandarización de las reglas, protocolos y normativas que permiten la interoperabilidad de todos los elementos en un sistema de telecomunicación.
Entre estos organismos internaciones destacan principalmente los siguientes:

- IETF (Internet Engineering Task Force):
  Es una organización sin ánimo de lucro de normalización de protocolos y elementos de la red Internet.
  Es el organismo que regula y publica las RFC, que son las propuestas y estándares de Internet y donde se describen todos los protocolos y arquitectura de la red.
  Su ámbito es mundial y está abierta a que cada usuario o profesional pueda realizar sus propuestas.
- ISO (International Standard Organization):
  Es una organización internacional de estandarización que promueve el desarrollo de normativas internacionales en muchas disciplinas de fabricación, ingeniería y desarrollo de productos y servicios.

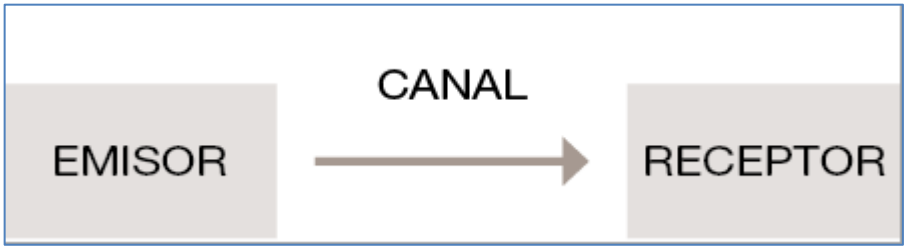
Su objetivo no es otro que buscar la estandarización de productos en base a la seguridad de los mismos.
Está formada por instituciones de numerosos países del mundo. Tiene su sede principal en Ginebra y aunque sus publicaciones o recomendaciones no son de obligado cumplimiento, es seguida por fabricantes y organizaciones.

- ITU (Internacional Telecommunications Union):
  Es un organismo dependiente de la ONU encargado de la regulación de las telecomunicaciones de organizaciones, empresas, operadoras e instituciones a nivel mundial.
  Publica periódicamente recomendaciones donde se recogen normas y procedimientos a seguir para la normalización de los estándares de las comunicaciones.
  Tiene su sede en Ginebra y es una de las organizaciones más antiguas en telecomunicaciones.
- ICT:
  Es una reglamentación nacional de España en la que se regula el acceso y distribución de los servicios de telecomunicaciones en el entorno residencial.
  Comprende un conjunto de normas que permite la distribución de los servicios de televisión, telefonía, datos y servicios de banda ancha para su acceso por parte de los usuarios.
  Es de obligatorio cumplimiento desde que entró en vigor en 1998.
  El 11 de Marzo del 2013 se publicó una actualización de dicho reglamento (R.D. 346/2011) en el que se introdujo la regulación de la fibra óptica y del par trenzado en el acceso de los servicios de telecomunicación dentro de la edificación.
  Además de los organismos anteriormente mencionados, existen numerosos otros de carácter nacional para cada uno de los países, aunque se sueñen ajustar a recomendaciones internacionales.
- Las redes de comunicaciones son un conjunto de infraestructuras y aplicaciones que permiten realizar trabajo en red entre equipos y personas.
- Las redes se clasifican en función de diferentes criterios destacando sobre todo el criterio del tamaño. Así se pueden clasificar las redes en LAN, MAN y WAN.
- La arquitectura de las redes se rige por unos modelos denominados OSI y TCP/IP.
- El modelo OSI establece que toda arquitectura en red se basa en un modelo jerárquico de 7 capas: capa física, de enlace, de red, de transporte, de sesión, de presentación y de aplicación.
- El modelo TCP/IP (modelo americano) establece que la arquitectura de redes se basan en un modelo jerárquico de 4 capas: capa de enlace de datos, de red, de transporte y de aplicación.
- Existe no obstante una correlación entre los modelos OSI y modelo TCP/IP.

2. Principios de transmisión de datos

2.1. Conceptos

El principio de la transmisión de datos comienza cuando una persona, equipo o agente denominado emisor quiere hacer llegar información a otra llamada receptor.
Para ello deberá utilizar un medio físico denominado **canal**, para hacer llegar esta información del **emisor** al **receptor**.
A continuación podemos ver el esquema de este principio de transmisión.



Se entiende por información un conjunto ordenado de datos que constituye un mensaje que envía un emisor a un receptor.
Por **dato** se entiende la unidad mínima de información o conocimiento y que forma parte de un mensaje.
El **canal** es el medio por donde viajará el mensaje desde el emisor hasta el receptor. Debe ser un medio físico y actuará como soporte de esta comunicación.
Como ejemplos de canales de comunicaciones podemos encontrar:

- El aire:
  Es el canal habitual para transmitir sonidos, por ejemplo, cuando hablamos.
- El agua:
  Es el canal habitual para transmitir ondas acuáticas y comunicaciones submarinas.
- El papel:
  Es el canal habitual para enviar una carta.
- Impulsos eléctricos.
  Es el canal que empleando medios telemáticos permite transmitir datos, mensajes o información de un punto a otro.

El canal que nosotros vamos a estudiar en profundidad es el de los impulsos eléctricos, que se emplea en las comunicaciones electrónicas y las redes de comunicaciones.
En primer lugar vamos a definir lo que se entiende por comunicación telemática.
Una comunicación telemática es la transmisión de datos o información entre un equipo emisor y un equipo receptor empleando sistemas informáticos y electrónicos.
Por tanto es la comunicación empleada en las redes de comunicaciones y redes de ordenadores.
En una comunicación telemática encontramos que:

- El emisor y receptor no son personas sino equipos u ordenadores.
- El canal de transmisión empleado puede ser guiado (un cable de transmisión) o inalámbrico (aire) pero en cualquier caso empleamos impulsos eléctricos, ópticos u ondas de radio.
- La información que se transmite generalmente va 'tratada' en forma de cadenas de bits o impulsos analógicos que luego el receptor deberá de decodificar para leer la información.

En los últimos tiempos cada vez está tomando más fuerza la opción de cifrar la información con objeto de que la información (al viajar por medios inseguros o compartidos como es el caso de Internet) no pueda ser manipulada o alterada por terceros no deseados. De ello se encarga la seguridad informática.
Uno de los aspectos más estudiados en una comunicación telemática es el canal.
El canal, por regla general, suele distorsionar, alterar o introducir ruido en el mensaje original que emite el emisor, por lo que el sistema de transmisión deberá adoptar las medidas detectoras y correctoras necesarias para el mensaje llegue al receptor para su correcta lectura.

Los canales más empleados en una comunicación telemática son:

- Medios guiados:
  Cuando se emplean cables para la transmisión de los datos como por ejemplo el par trenzado, la fibra óptica o el cable coaxial.
- Medios no guiados:
  Cuando se emplea el aire para la transmisión de datos en forma de ondas de radio, infrarrojos, etc.

Cada uno de ellos tienen sus ventajas e inconvenientes que lo hacen apropiados para transmitir un tipo u otro servicio de telecomunicación (voz, televisión, radio, etc).
En todos los casos, el canal introduce distorsión y ruido en los mensajes, por lo que en todos existen mecanismos correctores para la correcta transmisión del mensaje.

2.1.1. Flujo de datos: símplex, semi-dúplex y dúplex

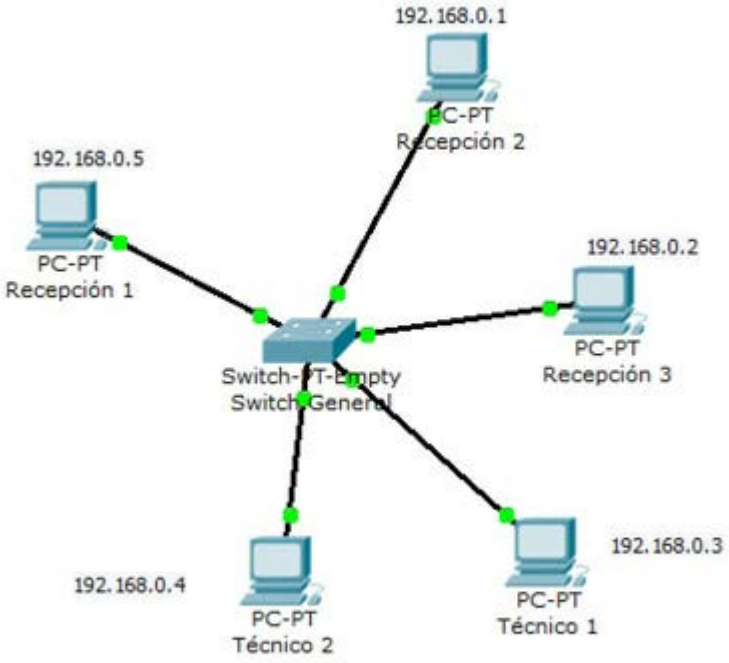
En el esquema de transmisión de datos anteriormente descrito (emisor, canal y receptor) la transmisión de los datos puede adquirir diferentes configuraciones.
Así el sistema puede estar configurado para que los equipos puedan actuar como emisor, receptor o como ambos.
En función de esto, la conexión de los datos que se intercambian puede realizarse de tres formas:

- Modo símplex:
  Es aquel en que la información se transmite sólo en un único sentido desde el emisor hasta el receptor, no pudiéndose transmitir de forma inversa.
  Ejemplo de ello son los sistemas de televisión, telemetría y/o de control.
- Modo semi-dúplex:
  Es aquella en que la información se puede transmitir en cualquiera de los dos sentidos, es decir, cada equipo puede actuar como emisor y como receptor. La salvedad es que no pueden transmitir y recibir a la vez. Este tipo de transmisión se adapta a las aplicaciones de pregunta/respuesta.
  El ejemplo más claro son las transmisiones de **walkie-talkie**.
- Modo full-dúplex:
  Es aquel en que la información puede cambiar en cualquier de los dos sentidos y de forma simultánea de forma que cada equipo puede actuar como emisor y receptor. Es un tipo de conexión donde se aprovecha al máximo el canal de comunicación (se obtiene eficiencia) ya que podemos enviar y recibir datos a la vez.
  La mayoría de las aplicaciones usan este tipo de modo de transmisión como por ejemplo la telefonía, redes de datos, etc.

En todos los casos existen los tres elementos del principio de transmisión de datos (emisor, receptor y canal) y lo único que varía es la configuración del mismo.
Esta configuración es independiente del canal empleado, es decir, pueden ser realizados sobre medios de transmisión guiados o medios de transmisión inalámbricos.

2.1.2. Direccionamiento

Las comunicaciones telemáticas son el medio de comunicación empleado por las redes de ordenadores.
Una red de ordenadores, como ya se ha descrito anteriormente, no es más que un conjunto de equipos interconectados entre sí para intercambiar datos.
Cuando varios equipos u ordenadores comparten el mismo canal de comunicación, surge el concepto de direccionamiento.
El direccionamiento es una técnica que permite asignar una dirección (generalmente una dirección IP) a cada elemento de la red para poderlos identificar de forma única.
Así cuando un equipo quiera enviar datos a otro equipo tan sólo deberá indicar antes del mensaje de datos a enviar, la dirección IP al equipo al que va dirigido.
Es la misma analogía para cuando queremos enviar una carta donde además del mensaje debemos indicar la dirección postal del receptor que queremos que reciba la carta.
Así por ejemplo, si tenemos el siguiente esquema de red de ordenadores, podemos observar que cada uno de ellos tiene una dirección IP.



Obviamente, cada dirección IP es única, sólo es empleada una vez en la red y únicamente se le asigna a un equipo.
Si el equipo con dirección IP 192.168.10.11 quiere enviar datos al equipo con dirección 192.168.10.192, tan sólo debe indicar al principio del mensaje esta dirección IP.
En dicho mensaje, no sólo va la dirección IP del destino, sino también del origen para que el receptor pueda identificar de quién parte el mensaje.
Ambas direcciones son imprescindibles para que los elementos de enrutado y de interconexión de redes puedan enrutar el mensaje desde emisor al receptor de forma adecuada.

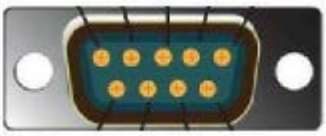
2.1.3. Modos de transmisión

En una comunicación de datos también podemos hablar del modo de transmisión.
El modo de transmisión indica de qué forma se transmiten los bits en una sistema de comunicación. Pueden ser de dos tipos:

- Modo serie:
  En este modo de transmisión los bits se transmiten de forma secuencial, es decir, se emite un bit, a continuación otro, a continuación otro, y así sucesivamente hasta la finalización de la trama o mensaje.
- Modo paralelo:
  En este modo de transmisión el canal empleado permite transmitir varios bits a la vez, es decir, simultáneamente (generalmente 8 bits) por el mismo cable.

Este modo de transmisión es más rápido que el de serie (enviamos en cada transmisión 8 bits y no uno).
El modo de transmisión paralelo es el modo más usado, ya que aprovecha que los equipos son capaces de procesar en paralelo y con ello se consigue más eficiencia en el sistema.
El modo de transmisión (serie o paralelo) es independiente del medio de transmisión empleado (cableado o inalámbrico), aunque como se ha comentado anteriormente, la mayoría de las transmisiones suelen emplear el modo paralelo.
El modo serie ha sido usado antiguamente como medio de transmisión, aunque poco a poco va quedando en desuso.

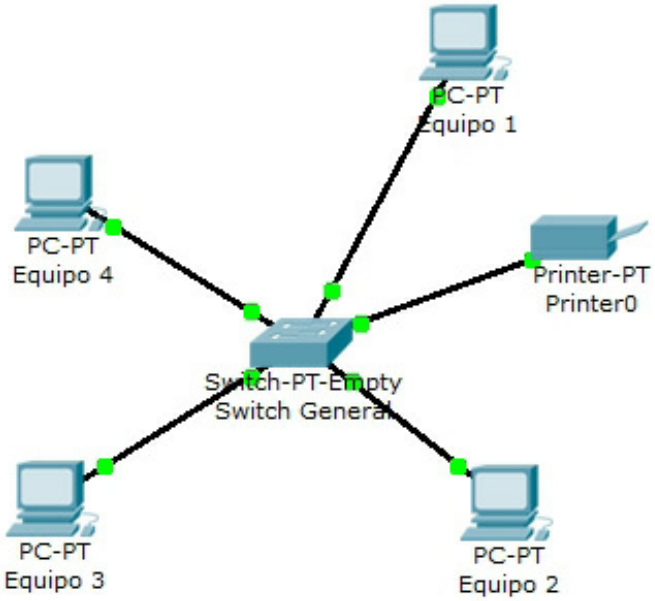
El ejemplo más claro de un interfaz serie es el interfaz RS-232 que incorporan aún muchos ordenadores (por compatibilidad con equipos antiguos).



También hay que destacar que existen dispositivos capaces de transformar transmisiones de serie a paralelo y de paralelo a serie con objeto de adecuar la transmisión al canal empleado.
Estos dispositivos conversores tienen implementados un registro de desplazamiento de bits que les permite realizar estas transformaciones.

Veamos un **ejemplo**:

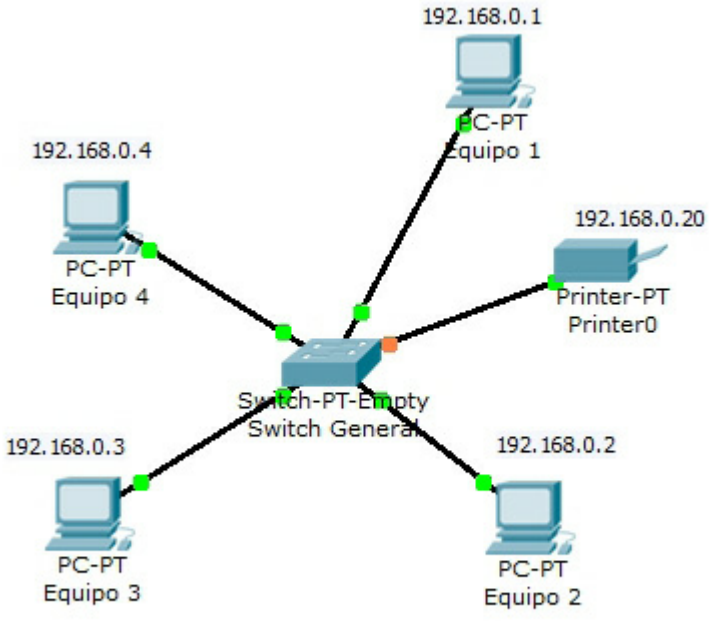
En la siguiente red de datos, especifica qué elementos actúan como emisores, receptores y canal. Indica también si el flujo de datos habitualmente utilizado y asigna direcciones a cada uno de ellos para configurar adecuadamente el sistema.



Solución:

En primer lugar, al tratarse de una red de ordenadores podemos establecer que todos los equipos pueden actuar como emisor y receptor (ya que envían datos y reciben datos como por ejemplo de la navegación web) a excepción de la impresora que sólo puede actuar como receptor.
El canal elegido para transmitir la información es el cableado (aunque también puede ser inalámbrico a través de una red Wifi).
El flujo de datos, a raíz de que todos los equipos pueden ser emisores y receptores a la vez, será un flujo de datos dúplex (ya que pueden enviar y recibir datos a la vez).
Mención especial será la impresora, que sólo puede recibir datos, luego el flujo será símplex (si por ejemplo fuera una multifunción con posibilidad de escáner sería también emisor y receptor y con flujo de datos dúplex).

Como todo equipo, una red debe tener dirección física (dirección IP) para que pueda ser identificado.
Asignamos las siguientes direcciones IP (que deben ser únicas para cada dispositivo).



Observamos que la impresora también debe tener su dirección IP.
Uno de los problemas cuando se transmite la información en serie o en paralelo es saber cada cuánto tiempo va a llegar un dato o bit.
Es decir, el receptor no sabe cuándo le va a llegar un dato por parte del emisor. Para solucionar este problema se emplean **técnicas de sincronización**.
En base a la técnica empleada podemos hablar de dos tipos de transmisión:

- Transmisión asíncrona:
  En este tipo de transmisión los datos se envían de forma irregular, es decir, no existen determinados tiempos para transmitir sino que el emisor envía los datos cuando tiene para enviar.
  Para que el receptor sepa o atienda el envío de datos que inicia el emisor, este último antes de enviar los datos, envía un bit de inicio que indica al receptor que comienza la transmisión de datos.
  Cuando finaliza la transmisión el emisor envía un bit de parada al receptor indicando que el proceso de transmisión de datos ha finalizado.
  De esta forma con los bits de inicio y parada se pueden comunicar el emisor y receptor.
- Transmisión síncrona:
  En este tipo de transmisión el emisor y receptor están sincronizados mediante un reloj (idéntico en frecuencia para ambos) de forma que el receptor recibe los datos en el mismo tiempo tal como el emisor lo está enviando.
  Para este tipo de transmisión emisor y receptor deben estar perfectamente sincronizados. Esto implica que existen determinados bits dentro de las tramas enviadas que resincronizan los relojes de ambos con objeto de evitar la desincronización.

Tanto un modo de transmisión asíncrona o síncrona tiene sus ventajas e inconvenientes.
Así en la transmisión asíncrona el principal problema es que cuando no hay datos a enviar la línea está desocupada. En la transmisión síncrona se da el problema de introducir códigos de sincronización en las tramas enviadas (para evitar la desincronización) o de tener que tener otro canal para enviar las señales de sincronismo.

Veamos un **ejemplo**:
Consideremos la transmisión entre un ordenador y un módem donde se envía un bit de arranque, seis de bits de información y un bit de parada.
Indica qué tipo de transmisión (asíncrona o síncrona) se emplea en esta transmisión, así como la velocidad sabiendo que toda la trama se envía en 1 mseg.
Solución:
Si existen bits de inicio y de parada en la transmisión está indicando que se trata de una transmisión asíncrona.
Por otro lado, considerando que la velocidad de transmisión ha sido 8 bits en 1 mseg, se trata de calcular la tasa binaria de transferencia, es decir:
(8 bits / 1 mseg) x 1000 mseg = 8.000 bits/seg = 8 Kbps.

Ejemplo:
En el ejemplo anterior se ha considerado en la tasa binaria los bits que se emplean como bits de control, es decir, bits de arranque y de parada. Pero la información que se transmite es de sólo 6 bits.
Si se considera como tasa binaria de transferencia sólo los bits de información efectiva enviado, calcule de nuevo la tasa binaria de transferencia del ejemplo anterior.
Solución:
En este caso si descontamos de la trama de transmisión los bits de arranque y de fin (bits de control), sólo se envían 6 bits de información, pero el tiempo de la trama de información sigue siendo 1 mseg, por lo que la tasa binaria de transferencia será ahora de:
(6 bits / 1 mseg) x 1000 mseg = 6.000 bits/seg = 6 Kbps.
Es decir, la tasa binaria efectiva es menor, ya que representa información de datos efectivamente enviados no incluyendo los bits de control.

2.2. Transmisión analógica y digital

El objetivo de toda red de comunicaciones es la transmisión de datos de un punto a otro.
Puede ser una transmisión de un elemento a otro y es lo que se denominaría transmisión punto a punto, o una transmisión de un punto a muchos y en este último caso se denomina transmisión punto a multipunto.
En cualquiera de los casos hay una transferencia de información que puede transmitirse a través de un cable o por medios inalámbricos.
También se debe tener en cuenta el **formato** en el que se va a transferir dicha información, ya que puede ser **analógico o digital**.

2.2.1. Definición datos, señales y transmisión

En cualquier comunicación de datos se habla siempre de tres conceptos: datos, señales y transmisión.
¿Pero qué significa cada uno de ellos? Empecemos por definirlos.

- Se entiende por **dato** como la unidad mínima de conocimiento y que forma parte de una información mayor y que generalmente suele transmitirse de un agente a otro.
  Los datos generalmente pueden ser representados de numerosas formas: en escritura, en binario, en ondas, etc.
- Se entiende por **señal** a la variación de una magnitud física en el tiempo.
  Por ejemplo la variación del voltaje dentro de una cable o conductor metálico genera una señal eléctrica.
- Se entiende por **transmisión** a la propagación de un dato o señal de un punto a otro o varios puntos empleando para ello un canal o medio físico de comunicación.

Un ejemplo muy claro es la transmisión de datos en una red de ordenadores empleando como medio de transmisión el cable de red de par trenzados.

2.2.2. Espectro acústico

El sonido es una sensación detectada por nuestros oídos y que se produce por un movimiento ondulatorio que usa el aire como medio de transmisión y es originado por un movimiento vibratorio.

Por tanto para que exista sonido deben darse dos situaciones:

- Que haya un movimiento mecánico y vibratorio.
- Que exista un medio de transmisión elástico que propague dichas ondas acústicas generadas.

De lo anterior se deduce que si no hay vibración mecánica no hay sonido, y si por ejemplo no hay medio de transmisión (como el vacío) no hay tampoco sonido.
El tímpano del oído no es más que un receptor de ondas acústicas que es capaz de vibrar a la frecuencia de la onda recibida y traducirla a impulsos nerviosos que llega a procesar el cerebro.
Como todo movimiento ondulatorio estas ondas tienen frecuencia y se denominan ondas acústicas porque su frecuencia está comprendida dentro del espectro denominado espectro acústico que corresponde a las frecuencias desde los 20 Hz hasta lo 20Khz y que son las frecuencias que el ser humano es capaz de 'escuchar'.
No obstante, el espectro acústico indicado es para una persona normal, ya que existen ciertas personas cuyo espectro puede llegar hasta los 24 Khz y este margen dependerá de cada individuo.
Todas las frecuencias por debajo de los 20 Hz se denominan infrasonidos (no son audibles) y por encima de los 20 Khz se denominan ultrasonidos (tampoco son audibles).
Veremos a continuación con más detalles estas frecuencias.

Infrasonidos:

Son aquellas ondas acústicas que están por debajo de los 20 Hz y se caracterizan por tener una forma de onda esférica y alcanzar grandes distancias.
Determinados animales como el elefante son capaces de escuchar y emitir en estas frecuencias y las utilizan para comunicarse a largas distancias.
En esta banda se emplean dispositivos de detección de sonidos para fondos marinos o para movimientos sísmicos.

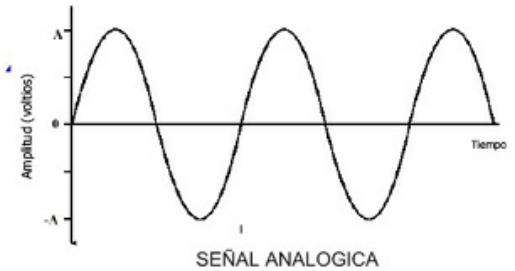
Ultrasonidos:

Son aquellas ondas acústicas que están por encima de los 20 KHz y se caracterizan por tener un alcance corto ya que su longitud de onda es pequeña (del orden de cm).
Determinados animales como el murciélago son capaces de escuchar y emitir en estas frecuencias y lo utilizan para comunicarse.
En esta banda se emplean dispositivos de telemedicina como por ejemplo las ecografías.

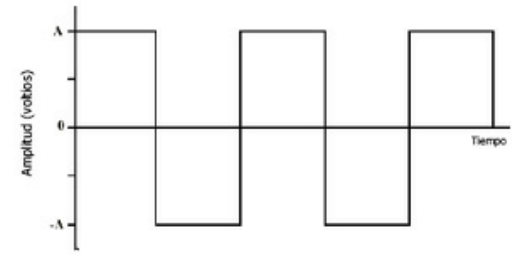
2.2.3. Señales analógicas y digitales. Ventajas e inconvenientes

Como ya se ha definido antes, una señal es la variación en el tiempo de una magnitud física.
En base a lo anterior, podemos realizar una primera clasificación de señales en:

- Señales **analógicas**:
  Son aquellas que pueden tomar valores infinitos en un rango dado.
- Señales **digitales**:
  Son aquellas que sólo pueden tomar valores discretos (un determinado finito de valores) en un rango dado.



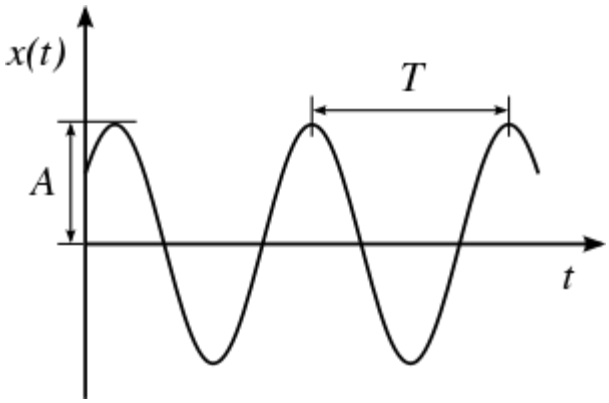
SEÑAL ANALOGICA



SEÑAL DIGITAL

En las siguientes imágenes podemos visualizar claramente la diferencia entre una señal analógica y otra digital.
En la señal analógica durante el intervalo de tiempo dado, la señal (su amplitud) puede adoptar cualquier valor posible, mientras que en la señal digital en ese mismo intervalo de tiempo sólo puede adoptar un valor de los posibles dados.

Todas las señales (tanto analógicas como digitales) quedan definidas por tres parámetros fundamentales:



- Su **amplitud** (A):

Es el valor que toma la señal en cada instante de tiempo. En el caso de señales analógicas puede ser cualquier valor y en el caso de señales digitales sólo un número finito de valores.

- Su **frecuencia**:

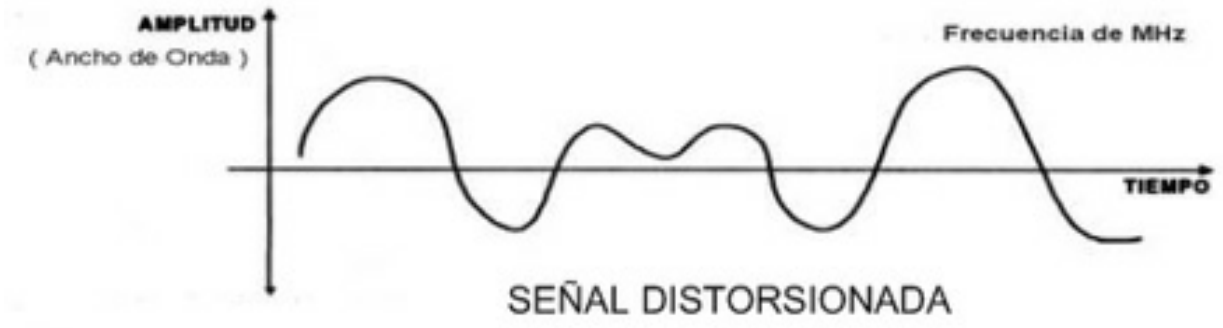
Es la magnitud que mide el número de veces que se repite la señal por unidad de tiempo. Se mide en Hz.
Es una magnitud inversa al periodo de la señal.
Siendo T el periodo de la señal medido en segundos.

$$f = \frac{1}{T}$$

- Su **fase**:
  Es una magnitud que indica la situación instantánea de un señal en un ciclo. Representa una fracción del periodo transcurrido con respecto a un estado de la señal tomado como referencia.

Todas las señales sufren tres problemas cuando se transmiten:

- **Atenuación**:
  Es la disminución de su valor en amplitud o de pico con respecto a la señal original emitida cuando se propaga por un medio de transmisión.
  Con objeto de que la señal pueda ser recibida por el receptor, se necesitan elementos repetidores que en definitiva lo que realizan es regenerar o amplificar de nuevo la señal emitida.
- **Distorsión**:
  Se define como la deformación que sufre la señal original emitida con respecto a la recibida tras su propagación por medio de transmisión.
  Como el medio de transmisión tiene atenuaciones variables con la frecuencia, esto provoca que la señal se 'deforme' permitiendo el patrón con que se emitió.
  Lo vemos en la siguiente figura:



- **Ruido**:
  El ruido se define como el conjunto de señales presentes en medio de transmisión diferentes a la señal emitida y que se 'acopla' de forma positiva (suma) o negativa (resta) a la señal emitida, provocando que no llegue al receptor y puede ser procesada.
  El ruido es un elemento siempre presente en un medio de transmisión y no puede ser eliminado, solo se pueden atenuar sus consecuencias.
  Lo vemos en la siguiente figura:

Aunque los tres problemas anteriores descritos (atenuación, distorsión y ruido) afectan por igual a señales analógicas y digitales, las señales digitales presentan grandes ventajas para con respecto a las analógicas en su tratamiento.
Así por ejemplo, en la atenuación, en el momento de regeneración de una señal digital, es mucho más sencillo en una transmisión digital ya que sólo debe detectar la presencia o no de señal (número discreto de valores), mientras que en las señales analógicas además deben regenerar la amplitud de la señal.
Además, hoy en día casi todos los equipos procesan en binario con lo cual si la transmisión ya se realiza en binario (digital), no es preciso realizar las conversiones analógicos-digitales, que en definitiva introduce retardos y posibles fallos.
Cualquier señal o fenómeno analógico (voz por ejemplo) puede ser tratada, procesada y transmitida como señales digitales gracias a la digitalización de la señal.

2.2.4. Datos y señales

Como ya se ha descrito anteriormente, los datos son unidades mínimas de información y susceptibles de ser transmitidas.
En cambio las señales son variaciones de una magnitud física con el tiempo.
Ambos están relacionados, ya que cuando queremos transmitir datos realmente los transformamos en señales para poder ser transmitidos.
Luego existe una correlación entre datos y señales usando entre ellos numerosas técnicas de comunicaciones.
Para transmitir estos datos podemos emplear dos tipos:

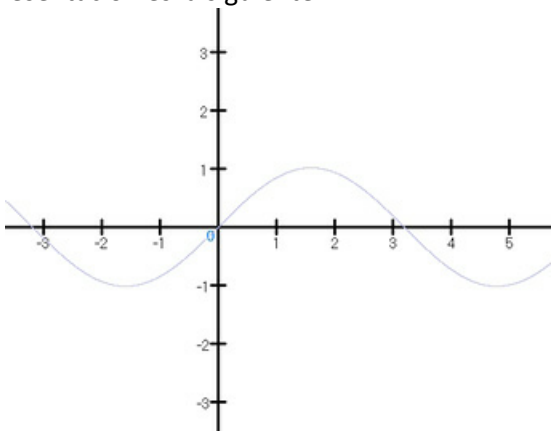
- Transmisión analógica: es aquella que transmite señales analógicas.
- Transmisión digital: es aquella que transmite señales digitales.

Cada una de ellas tiene sus ventajas e inconvenientes las cuales las veremos a continuación con más detalle.

2.2.5. Características de la transmisión analógica y digital

Transmisión analógica

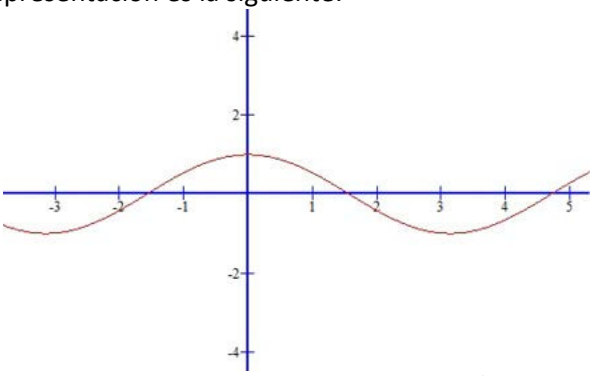
Una transmisión analógica se caracteriza por transmitir señales analógicas.
Dentro de las señales analógicas cobran especial importancia las señales sinusoidales ya que son las más ampliamente utilizadas.
Una sinusoide es una señal cuya forma se corresponde con la función matemática del seno. Su principal característica es que se trata de una señal periódica, es decir, tiene un ciclo que se repite constantemente hasta el infinito.
Su expresión matemática y representación es la siguiente:



$S(t) = A \times \text{seno}(2 \times \pi \times f \times t + Ø)$

Siendo:
A: el valor de amplitud de la señal.
f: la frecuencia de la señal medido en Hz.
t: la variable tiempo.
Ø: la fase de la señal medida en radianes.

También se emplea con frecuencia en la transmisión analógica la función del coseno.
Esta función coseno, al igual que la sinusoide, es una señal periódica y que presenta los mismos parámetros básicos que la función seno vista anteriormente.
Su expresión matemática y representación es la siguiente:



$S(t) = A \times \text{coseno}\ (2 \times \pi \times f \times t + Ø)$

Siendo:
A: el valor de amplitud de la señal.
f: la frecuencia de la señal medida en Hz.
t: la variable tiempo.
Ø: la fase de la señal medida en grados.

Se usan este tipo de señales en telecomunicaciones por los siguientes motivos:

- Las ondas electromagnéticas siguen el mismo comportamiento natural que las ondas sinusoidales.
- Estas señales son fáciles de procesar mediante dispositivos electrónicos y algoritmos de procesado de señales (DSP).
- Existen técnicas como las Series de Fourier, que establecen que cualquier señal se puede descomponer (o se puede construir) mediante combinaciones de señales sinusoidales.

Transmisión digital:

Una transmisión digital se caracteriza por transmitir señales digitales.
Las señales digitales se caracterizan por transmitir flujos de bits que en definitiva se corresponden con la presencia o ausencia de señal. Así, siguiendo este criterio podemos establecer la siguiente relación:

- ⇨ Hay señal es un 1
- ⇨ No hay señal es un 0

La relación anterior también se puede realizar a la inversa.
La transmisión digital se reduce en definitiva en enviar o no señal y así el receptor lo va interpretando como 0 y 1 para su decodificación.
Esta transmisión es mucho más sencilla ya que el procesado se basa en la detección o no de señal no siendo importante la amplitud o frecuencia como pueden ser en las transmisiones analógicas.
En la siguiente figura podemos ver cómo funciona una transmisión digital:

La relación anteriormente establecida de **enviar o no señal e interpretarlo como 0 o 1 se conoce como codificación** ya que establecemos un código (código binario) en función de presencia o ausencia de señal.

Pero esta codificación se puede realizar de varias formas:

- Presencia o ausencia de impulsos eléctricos (transmisión digital eléctrica).
- Presencia o ausencia de impulsos ópticas (transmisión digital óptica).
- Dos niveles de voltajes diferentes con respecto a la tierra (si enviamos 10 V es un 1 y si enviamos 5 v es un 0).
- Dos niveles de corriente diferentes (si enviamos 5 mA es un 1 y si enviamos 1 mA es un 0).
- Etc.

Es por ello que en la transmisión digital hay numerosas técnicas para su codificación.
Por último se ha de resaltar que los datos pueden ser analógicos o digitales.
Por ejemplo, la voz es un dato analógico y en cambio un archivo es un dato digital (son un listado de bits).
Las señales, como se ha visto antes, pueden ser analógicas o digitales.
Esto no significa que para datos analógicos se deban usar señales analógicas y para datos digitales se deban usar señales digitales. Puede darse cualquier combinación.
Es decir, los datos analógicos pueden transmitirse usando señales analógicas o digitales.
Los datos digitales pueden también transmitirse usando señales analógicas o digitales.
Esto se puede ver en los siguientes ejemplos:

- La señal de voz (dato analógico) puede digitalizarse y enviarse a través de un teléfono móvil usando transmisiones digitales.
- Un archivo (dato digital) podemos transmitirlo por una red Wifi empleando ondas electromagnéticas (transmisión analógica).

2.2.6. Ventajas de la transmisión digital

La transmisión digital representa hoy día grandes ventajas sobre la transmisión analógica y es por ello que se emplea en la mayoría de las transmisiones.
Entre las ventajas más significativas encontramos:

- Es un tipo de transmisión más inmune al ruido, ya que las señales analógicas son más vulnerables al ruido en su amplitud, frecuencia y fase.
- Prácticamente todos los equipos ya procesan en digital, por lo que es lógico que para evitar conversiones y retardos la transmisión de datos sea también en digital.
- La regeneración (en los repetidores) es más sencilla en una transmisión digital que en una analógica, ya que sólo detecta la presencia de señal o no y generan otra señal digital nueva y sin ruido. En cambio en la transmisión analógica no se puede regenerar completamente la señal.
- Existen técnicas mucho más eficaces para detectar y corregir transmisiones digitales que las transmisiones analógicas.

2.2.7. Perturbaciones en la transmisión

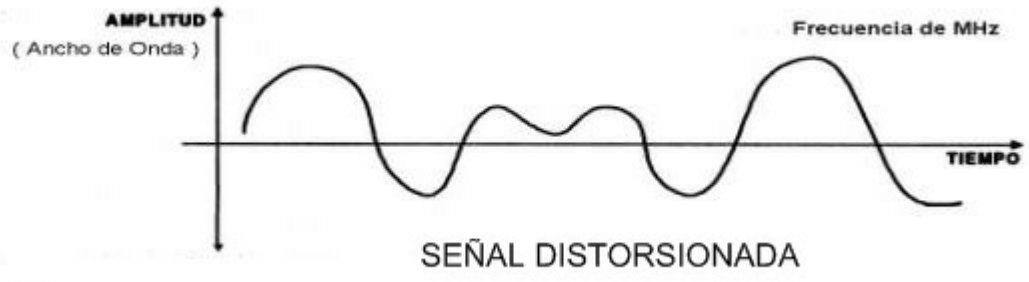
Como ya se ha indicado anteriormente, en todo canal de transmisión (sea cableado o inalámbrico) existen elementos perturbadores externos que provocan que la señal original emitida no llegue correctamente al receptor.
Las técnicas de transmisión de datos evitan o minimizan estos efectos con objeto de que la señal emitida pueda llegar al receptor y con ello recibir el mensaje enviado.
Existen fundamentalmente tres elementos perturbadores en todo medio de transmisión:

- La atenuación.
- La distorsión.
- El ruido.

Cualquiera de estos elementos (o incluso todos) pueden estar presentes en todo canal de transmisión creando incluso un efecto suma o multiplicador como elemento perturbador de la señal deseada a transmitir.
Vemos con más detalle en qué consiste cada una de estar perturbaciones y cómo afecta a una transmisión bien sea digital o analógica.

Atenuación y distorsión de la atenuación

Se define la atenuación como la disminución de la amplitud de la señal a medida que ésta va recorriendo el medio de transmisión.
La atenuación está directamente relacionada con la distancia recorrida, por lo que a mayor distancia más atenuación introduce el canal o medio de transmisión.
La atenuación no es más que una magnitud física debida a la resistencia que ofrece el medio a la propagación de la señal, siendo proporcional a su longitud e inversamente proporcional a su sección.
Esto último es la razón por la que cables más gruesos tienen menos atenuación que cables más finos, cuando el medio de transmisión sea cableada.
También por esta razón es el por qué los medios de transmisión (sobre todo cableados), que suelen especificar entre sus características la atenuación en dB/m.
Las atenuación se produce en cualquier medio independientemente de que la transmisión sea analógica o digital, pero su tratamiento y corrección es diferente si la transmisión es una u otra.
Por ejemplo, en una transmisión analógica, la pérdida de amplitud de la señal se puede compensar con repetidores, que no son más que amplificadores que incrementan la amplitud de la señal de entrada.
En una transmisión digital, lo que se emplea son repetidores regenerativos que lo que hacen es generar una nueva señal de salida con la misma información que tenía a la entrada.
La ventaja que tiene la regeneración en una transmisión digital con respecto a la analógica, es que en toda amplificación además de amplificar la señal también se amplifica el ruido que pueda llevar la señal, con lo cual tras muchos repetidores analógicos es posible que el ruido 'enmascare' la señal deseada y no pueda regenerarse la señal original. En cambio, en la transmisión digital no ocurre, ya que tras cada repetidor se ha generado una nueva señal idéntica a la emitida y sin acumular el ruido que haya podido acoplarse por el canal.
En cualquier caso, los repetidores deben colocarse a una distancia suficiente que permita poder captar señal suficiente a la entrada para poderla regenerar y a continuación retransmitir. Este es el motivo de que cada cierta distancia debe haber un repetidor.
Además se debe tener en cuenta que los repetidores siempre introducen retardos en la señal debido a su procesamiento.
Pero la atenuación no es uniforme en toda la señal, sino que todos los medios de transmisión introducen atenuación que varía con la frecuencia.
Esto quiere decir que a una frecuencia f1 el canal introduce una atenuación X dB, pero a una frecuencia f2 el canal introduce otra atenuación Y dB (para la misma distancia recorrida). Esto es lo que se conoce como distorsión de la atenuación, ya que en definitiva además de atenuar la señal la distorsiona y la amplitud atenuada varía con la frecuencia.
Lo vemos en la siguiente figura:



SEÑAL DISTORSIONADA

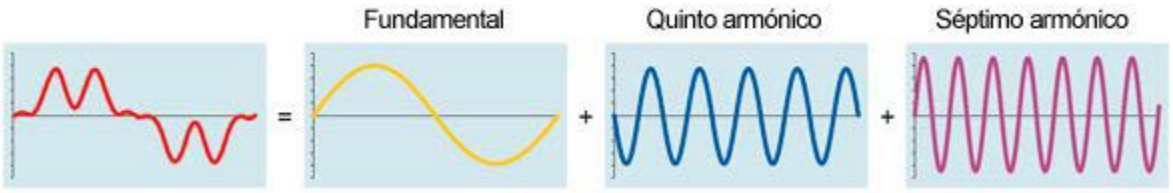
La atenuación con la frecuencia depende del medio de transmisión empleado, ya que es una característica del medio y para la misma señal la distorsión puede ser diferente.

Así hay medios que atenúan más a bajas frecuencias que a altas frecuencias, y otros medios en cambio es al revés.

Vemos un **ejemplo**:
Una señal de 500 dBm se transmite por un cable conductor de 100 metros de longitud. Si la atenuación del cable es 1 dB/m, calcula la potencia que llegará al otro extremo.
Solución:
Calculamos en primer lugar la atenuación introducida por el cable sabiendo que atenúa a 1 dB/m, por lo que para 100 metros la atenuación total introducida será de:
Atenuación total (100 m) = 1 dB/ m x 100 m = 100 dB.
Por tanto, la señal recibida en el otro extremo será la potencia emitida menos la atenuación, es decir:
Potencia recibida = 500 dBm – 100 dB = 400 dBm

Distorsión del retardo

Cualquier señal que se transmite por un medio de transmisión se compone de un conjunto de ondas monocromáticas, tiene una sola longitud de onda (según la serie de Fourier).
Cualquier señal cuando se transmite por un medio de transmisión sufre un retardo que se define como el tiempo que transcurre durante el recorrido de la señal en ese medio de transmisión.
El canal además de atenuar de forma diferente en función de la frecuencia (como se ha visto anteriormente) también propaga de forma diferente en función de la frecuencia.
Esto se traduce que para una señal con numerosos armónicos, cada armónico se propaga a velocidades diferentes, y esto genera retardos diferentes en cada armónico y genera lo que se define como distorsión del retardo.
Por tanto la distorsión del retardo no es más que la deformación que sufre la señal cuando traspasa por un medio de transmisión debido a los retardos diferentes que sufre cada armónico que forma la señal emitida.



Para entender el concepto de armónico, podemos decir que una señal "real" la podemos descomponer en una señal **Fundamental** + el resto que son los armónicos, que son múltiples enteros de la fundamental.

Ruido térmico

El ruido se define como toda perturbación o interferencia no deseada que se introduce en el medio de transmisión y que se acopla a la señal deseada transmitida.
Las fuentes de ruido pueden ser diversas: transmisión de otras señales, motor de un coche, maquinaria en movimiento, etc.
El ruido no puede ser eliminado sino minimizado o acotado en sus implicaciones.
Existen numerosos tipos de ruidos destacando entre las siguientes:

- Ruido blanco.
- Ruido impulsivo.
- Ruido térmico.

Una técnica eficaz para evitar el ruido es apantallar el medio guiado por el que se transmite la información ya que esta pantalla metálica evita el acople de señales externas a la señal transmitida en el interior del cable, y además evita que las interferencias que pueda producir la señal transmitida salgan al exterior para acoplarse a otras señales.
El ruido siempre está presente (al menos el ruido blanco) en todo medio de transmisión.
Se debe tener en cuenta que un amplificador -dispositivo que se instala en los repetidores para regenerar la señal transmitida y conseguir así mayores alcances-, también amplifica (además de la señal transmitida) el ruido que lleva acoplado la señal.

Este es el motivo por el cual está limitado el número de amplificadores puestos en serie en una transmisión, ya que el ruido se va acumulando en cada salto regenerativo hasta que llega a un punto donde la relación señal / ruido (medida de la calidad de la señal) es muy baja e impide la regeneración de la señal.
Esta relación señal / ruido viene dada por la siguiente expresión:

$$S / N = 10 \times \log \left(\frac{\text{Potencia señal en watios}}{\text{Potencia ruido en watios}} \right)$$

Es un parámetro adimensional y que determina en gran medida el alcance de una señal transmitida y el ancho de banda de un medio de transmisión
A continuación vamos a ver con más detalle cada uno de los tipos de ruido mencionados anteriormente.

- Ruido **blanco**: Es un tipo de ruido que está presente en todas las frecuencias (de ahí el nombre de blanco) y afecta a cualquier señal transmitida.
  No puede ser eliminado pero sí minimizado.
- Ruido **impulsivo**: Es un ruido con un pico de potencia muy pronunciado y de corta duración y suele ser de origen externo como por ejemplo, el encendido del motor de un coche, el encendido de un relé, etc.
  Puede ser evitado en la medida de lo posible.
- Ruido **térmico**: Es un tipo de ruido generado por el movimiento aleatorio de electrones en movimiento a causa de la temperatura.
  Está presente en todas las frecuencias y por tanto se trata de un ruido blanco. No puede ser eliminado pero sí minimizado.
  Se puede observar que tiene una densidad espectral plana.
  Se puede calcular la potencia de ruido en un determinado ancho de banda mediante la siguiente expresión:

  $$N = N_o \times Bw$$

  Siendo N la potencia de ruido introducida y Bw el ancho de banda en el que se quiere calcular dicha potencia de ruido. Esta potencia de ruido se mide en watios.
  N_o es una constante que depende de la temperatura (el ruido térmico es generado por la temperatura) y viene dado por:

  $$N_o = K \times T$$

  Siendo K la constante de Boltzmann (1,38 x 10-23 J/ºK) y T la temperatura medida en ºK.

Veamos un **ejemplo**:
Calcula el ruido térmico introducido en un conductor metálico a la temperatura de 15º cuando se emplea como medio de transmisión para una señal cuyo ancho de banda es de 1 Mhz.
Solución:
El ruido térmico introducido por un conductor a una temperatura viene dado por la siguiente expresión:

$$N = N_o \times Bw$$

siendo $N_o = K \times T$ donde K = 1,38 x 10-23 J/ºK y T medida en ºK, luego:

$$T = 293^o + 15^o = 288\ ^oK$$

Por lo que se obtiene que:

$$No = 1{,}38 \times 10\text{-}23 \times 288^o = 397{,}44 \times 10\text{-}23\ w/hz$$

Para el ancho de banda de la señal tenemos:

$$N = 397{,}44 \times 10\text{-}23 \times 1\ Mhz = 397{,}44 \times 10\text{-}17\ w$$

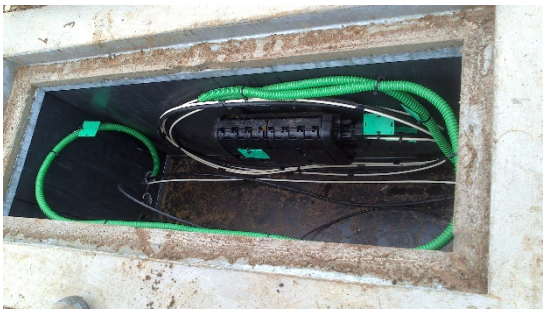
La potencia generalmente se expresa en dB por lo que pasando a escala logarítmica queda:

$$N\ (dB) = 10 \times \log (N) = 10 \times \log (397{,}44 \times 10\text{-}17) = -14{,}40\ dB$$

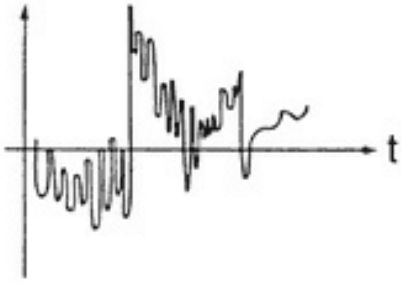
El anterior resultado indica que -14,40 dB es la potencia de ruido térmico que introduce el conductor en la señal transmitida.

Ruido de intermodulación, diafonía y ruido impulsivo

- Ruido de **intermodulación**:
  El ruido de intermodulación es la energía del ruido generado en los productos de intermodulación cuando una señal pasa por un amplificador no lineal.
  Como ya se ha comentado anteriormente, un amplificador aumenta (amplifica) el nivel de la señal de entrada, pero esta señal suele ser una combinación de armónicos.
  Por el desarrollo de Fourier, cuando se amplifican se generan armónicos, que son señales cuya frecuencia son combinaciones lineales de los armónicos de la señal de entrada. Estos armónicos llamados (frecuencias de intermodulación) como cualquier señal transportan energía y en definitiva son señales espurias o ruidos de intermodulación.
  En ella se puede observar el amplificador al amplificar la señal con frecuencia f1 y la señal con frecuncia f2 genera armónicos de f1+f2, f1-f2, 2f1 + f2, etc., que son los productos de intermodulación. Si calculamos su energía (o potencia de señal) nos dará el ruido de intermodulación.
- **Diafonía**:
  La diafonía se define como la señal que se acopla de un conductor a otro cuando ambos conductores transportan señales y transcurren por el mismo trazado y es debido a los desequilibrios de admitancias de los hilos de ambos conductores.
  La diafonía se puede minimizar o evitar adoptando las siguientes medidas:
  - ⇨ **Separar** ambos conductores a la mayor distancia posible:
    Esto no siempre es posible, ya que es habitual que muchos conductores empleen la misma canalización (tubo, bandeja o canaleta) y discurran por el mismo trazado.
  - ⇨ **Apantallar** ambos conductores.
    Se trata de rodear ambos conductores de una malla metálica de hilos de cobre o de aluminio que actúan como barreras para señales externas y que las internas salgan hacia fuera.
    Su inconveniente es que encarece el conductor por sus características constructivas y lo hace menos ligero.

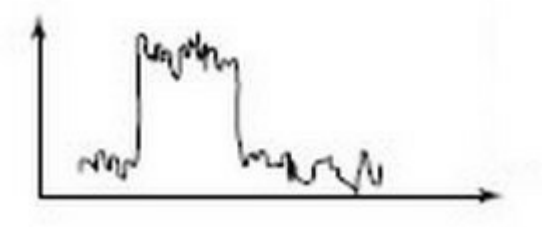


- Ruido **impulsivo**:
  Es un tipo de ruido que se caracteriza por tener un pico de potencia muy pronunciado y de corta duración. Suele ser un ruido generado de forma artificial o natural pero es de origen externo al medio de transmisión.
  Ejemplos de este tipo de ruido pueden ser el ruido generado en el arranque del motor de un coche, el movimiento de una maquinaria, el encendido en un relé, etc.
  Este tipo de ruido puede provocar gran atenuación en determinados puntos y momentos de la transmisión sobre todo si las señales transmitidas son débiles.
  A diferencia del ruido térmico, puede ser evitado en la medida de lo posible adoptando las medidas oportunas.
  En la siguiente imagen se puede ver el aspecto de una señal distorsionada por ruido impulsivo.



Este tipo de ruido se puede minimizar aumentando la distancia entre el medio de transmisión y la fuente generadora del ruido.
Su banda de frecuencias puede ser muy amplia, pudiendo tener componentes espectrales en baja, media o alta frecuencia.
Se puede calcular su potencia integrando su amplitud dentro de la banda de frecuencias en la cual hay energía de este tipo de ruido impulsivo.

Veamos un **Ejemplo**:
Dada una fuente generadora de ruido, el cual ha sido medido y donde se ha obtenido el siguiente espectro, calcula la potencia de ruido generado.



Solución:
Según el espectro de la figura, podemos ver que se trata de un ruido impulsivo, ya que sólo está presente en un intervalo corto de tiempo.
Para calcular su potencia debemos integrar su valor en amplitud en el tiempo que transcurre, es decir, t=0 hasta t=1 seg.
Dado que a la vista del espectro, éste tiene forma rectangular, podemos realizar la aproximación (sin equivocarnos demasiado en los resultados) que puede asemejarse a un rectángulo cuya altura es la amplitud del ruido y cuyo largo es el tiempo que dura el ruido, es decir, de 1 seg.
Como la integral en definitiva es el cálculo de un área, sabemos que el área de una rectángulo es su altura por su longitud, es decir:

Área rectángulo = altura x longitud

Aplicando esta aproximación a nuestro caso obtenemos que:

Potencia de ruido = área rectángulo (alt = 5 , long= 1) = 5 x 1 = 5 W

Como la potencias de ruido suelen darse en dB, aplicamos logaritmos:

Potencia ruido (dB) = 10 x log (Potencia ruido en W) = 10 x log (5) = 4,88 dB

Efectos del ruido sobre una señal digital

El ruido, como se ha comentado anteriormente y como elemento perturbador, afecta a cualquier tipo de transmisión sea analógica o digital.
No obstante, sobre una transmisión digital su perturbación es diferente y por ello los elementos correctores empleados para minimizarlos también son diferentes.
El ruido en una transmisión digital puede afectar en la codificación de la señal recibida, de forma que el receptor interprete el bit recibido de forma errónea a causa del ruido.
Es decir, en una transmisión digital el receptor basa su procesado en la detección o no de señal. De esta forma si hay señal lo interpreta como un 1 y si no hay señal lo interpreta como un 0.
Pero el ruido introducido en el canal puede hacer que donde se había transmitido un 1, ahora el ruido introduce señales que pueden tener una amplitud o energía suficiente de forma que el receptor lo interprete como presencia de señal y por tanto lo codifique como 1 y no como 0 transmitido.
Este es el principal efecto del ruido en una transmisión digital.
Por tanto en una transmisión digital siempre se producirá un número de bits que se han recibido de forma errónea con respecto a los bits transmitidos.
Existe una medida denominada BER (que se verá más adelante) que relaciona el número de bits erróneos recibidos con respecto al número de bits transmitidos y que es un parámetro de la calidad de la transmisión digital.

Por tanto un canal o medio de transmisión con un BER alto indica que es un canal ruidoso, mientras que un canal o medio de transmisión con un BER bajo indica que un canal poco ruidoso.
Para evitar los efectos del ruido en la transmisión digital se emplean técnicas detectoras de errores (detectan los bits erróneos recibidos) y técnicas correctoras de errores (una vez detectados los errores son capaces de corregir los bits erróneos).

2.2.8. Decibelio y potencia de señal. Relación señal-ruido

El decibelio (dB) es una unidad de medida logarítmica muy usado en comunicaciones.
Representa una relación entre valores de potencia, tensión o intensidad pero en escala logarítmica, ya que en una transmisión podemos encontrar valores muy pequeños (del orden de 10-6 o inferiores) y/o valores muy altos (del orden de 109 o mayores).
Así en comunicaciones podemos encontrar 1µV (10-6 V) y 1 Ghz (109 Hz). Este el motivo por el que se emplea escala logarítmica.
Por tanto cuando a dicha magnitud le aplicamos logaritmos obtenemos decibelios y siempre es relativa a una magnitud de referencia.
Así podemos hablar de potencias en decibelios (con respecto a 1 W de refencia):
Pot (dB)= 10 x log (Potencia en W)
El decibelio es la magnitud empleada cuando hablamos de ganancia o de atenuación de una señal o medio de transmisión.
Así hablamos de ganancia de potencia:

$$G_p\,(db) = 10 \times \log\left(\frac{Pot2}{Pot1}\right)$$

siendo Pot2 el nivel de potencia obtenido tras un amplificador o medio de transmisión y Pot1 el nivel de potencia a la entrada de un amplificador o medio de transmisión.
También podemos hablar de ganancia de tensión dada por la siguiente expresión:

$$G_v(db) = 20 \times \log\left(\frac{Voltaje2}{Voltaje1}\right)$$

siendo Voltaje el nivel de señal (medido en V) obtenido tras un amplificador o medio de transmisión y Voltaje 1 el nivel de señal (medido en V) a la entrada de un amplificador o medio de transmisión.
El mismo concepto es extrapolable cuando hablamos de ganancia en intensidad:

$$G_i\,(db) = 20 \times \log\left(\frac{Intensidad\ 2}{Intensidad\ 1}\right)$$

siendo Intensidad 2 la corriente (medido en A) obtenido tras un amplificador o medio de transmisión e Intensidad 1 la corriente (medido en A) a la entrada de un amplificador o medio de transmisión.
Las pérdidas o atenuaciones pueden expresarse como ganancias negativas, o lo que es igual:

$$Ap\,(db) = 10 \times \log\left(\frac{Pot\ 1}{Pot\ 2}\right)$$

$$Av(db) = 20 \times \log\left(\frac{Voltaje\ 1}{Voltaje\ 2}\right)$$

$$Ai\,(db) = 20 \times \log\left(\frac{Intensidad\ 1}{Intensidad\ 2}\right)$$

siendo los parámetros los mismos que los indicados anteriormente.
Habitualmente en la amplificación hablamos de ganancia (ya que los niveles de señal de salida serán superior a los de entrada por el efecto de la amplificación) y en los medios de transmisión hablamos de atenuación (ya que los niveles de señal de salida serán inferiores a los niveles de señal de entrada).
Se puede deducir de las expresiones anteriores que la atenuación no es más que ganancia con valor negativo.
A (dB) = - G (dB)
La potencia de una señal es una magnitud que indica la cantidad de energía que transporta esa señal.
Es una magnitud que se mide en watios (W) y puede expresarse en unidades logarítmicas tomando como referencia la potencia de 1 W, es decir:

Pot (dB) = 10 x log (Pot en W)
Como ya se ha comentado anteriormente, la potencia de una señal puede ser aumentada (mediante dispositivos de amplificación) o disminuida (cuando se propaga por un medio de transmisión).
Toda señal tiene un nivel de potencia (medido en W o en dB) incluido el ruido.
La relación entre el nivel de potencia y el nivel de ruido presente en un dispositivo o medio de transmisión es lo que se denomina relación Señal/ruido y viene dada por la siguiente expresión:

$$S / N\ (dB) = SNR = 10 \times \log \left(\frac{\text{Potencia señal (w)}}{\text{Potencia ruido (w)}} \right)$$

La relación SNR es un parámetro que indica la calidad de la transmisión.
Veamos un ejemplo:
Si una señal es de 1 W de potencia es procesada por un amplificador de 20 dB, calcula cuál será el nivel de potencia de señal tras la salida del amplificador.
Solución:
En primer lugar debemos poner todas las magnitudes en la misma escala para poder operar entre ellas.
Así una señal de 1 W de potencia, su potencia en dB vendrá dado por:
Pot (dB) = 10 x log (Pot en w) = 10 x log (1) = 0 dB
Como el amplificador introduce 20 dB ello quiere decir que suma a la señal 20 dB luego a la salida tenemos del amplificador tenemos:

$$\text{Potencia}_{\text{salida amplificador}}\ (dB) = \text{Potencia}_{\text{entrada amplificador}} + G_{\text{amplificador}} = 0 + 20\ dB = 20\ dB$$

Ahora esta potencia de señal de salida lo pasamos a unidades de watios con lo que se obtiene:
Potencia (w) = 100 W
Veamos otro ejemplo:
Supongamos ahora la misma señal que el ejemplo anterior, pero con un amplificador de 50 dB. Calcula de nuevo el nivel de potencia a la salida del amplificador.
Solución:
El nivel de potencia de la señal de entrada es el mismo, por lo que a la salida lo que tenemos es una señal amplificada en 50 dB, es decir:

$$\text{Potencia}_{\text{salida amplificador}}\ (dB) = \text{Potencia}_{\text{entrada amplificador}} + G_{\text{amplificador}} = 0 + 50\ dB = 50\ dB$$

Ahora esta potencia de señal de salida lo pasamos de nuevo a unidades de watios con lo que se obtiene:
Potencia (w) = 100000 = 100 Kw
Veamos un ejemplo más.
Dada una señal de potencia de 15 W que se transmite por un canal de transmisión que introduce una atenuación de 10 dB y un ruido de 5 dB.
Calcula el nivel de señal a la salida del medio de transmisión así como la relación señal ruido a la salida.
Solución:
En primer lugar debemos poner todas las magnitudes en la misma escala para poder operar entre ellas.
Así una señal de 10 W de potencia, su potencia en dB vendrá dado por:
Pot (dB) = 10 x log (Pot en w) = 10 x log (15) = 11,67 dB

El medio de transmisión introduce una atenuación de 10 dB por lo que tras ello el nivel de potencia de la señal vendrá restada en:

$$\text{Potencia}_{\text{tras medio transmisión}}\ (dB) = \text{Potencia}_{\text{entrada señal}} - \text{Atenuación}_{\text{medio transmisión}} = 11{,}67\ dB - 10\ dB = 1{,}67\ dB$$

Ahora esta potencia de señal de salida lo pasamos a unidades de watios con lo que se obtiene:
Potencia (w) = 1,46 W
La relación SNR vendrá dada por el nivel de potencia a la señal a la salida del amplificador con respecto al nivel de señal del ruido presente, es decir:

$$SNR = 10 \times \log \left(\frac{\text{Potencia señal (w)}}{\text{Potencia ruido (w)}} \right)$$

El nivel de señal de ruido será de
Potencia del ruido (dB) = 5 dB = 3,16 w
Sustituyendo valores en la expresión anterior obtenemos:

$$SNR = 10 \times \log\left(\frac{1,46}{3,16}\right)$$

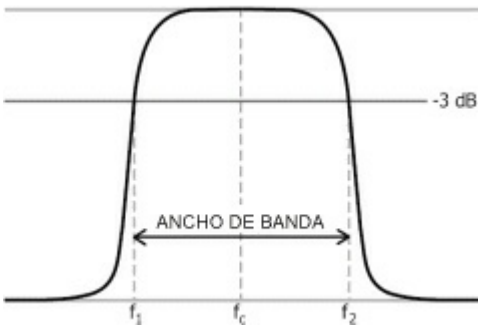
Un resultado negativo en el SNR indica que la calidad de transmisión mala ya que el medio introduce mucha atenuación y ruido.

2.2.9. Capacidad del canal, ancho de banda de una señal, velocidad de transmisión, tasa de error

La capacidad de un canal de transmisión se define como el límite superior de bits/seg que es capaz de transmitir ese medio de transmisión para un ancho de banda dado y en presencia de ruido.
Dicha capacidad viene establecida por el teorema de Shannon que establece que:

$$C_{max}\ (bit/seg) = BW \times \log_2 (1 + SNR)$$

siendo BW el ancho de banda del medio de transmisión en hercios y SNR la relación señal-ruido.
Por otro lado el ancho de banda de una señal (bw) se define como el intervalo de frecuencias en la cual se concentra la mayor parte de la energía de una señal y se mide en Hz.
Analizando el espectro de una señal se puede comprobar que la mayor parte de la energía (si hacemos la integral de la señal) se concentra en la cresta principal de la señal. Es en estos límites de esta cresta principal donde están la frecuencia máxima y mínima y su diferencia es el ancho de banda.
El ancho de banda es también una medida indicador de la capacidad de un medio de transmisión ya que indica el rango de frecuencias en el que el canal deja pasar la mayor parte de la energía de la señal transmitida y fuera de ese rango de frecuencias no la deja pasar o su atenuación es muy grande.
Así, un canal con un ancho de banda de 10 Mhz indica que tiene una ventana o rango de frecuencia de 10 Mhz, donde pasan por ella todas las señales cuyas frecuencias estén en ese rango. El canal transmite la señal y fuera de ella las elimina (destacar que además el canal debe indicar la frecuencia mínima y máxima de la ventana de transmisión).
El ancho de banda es una medida esencial en comunicaciones ya que indica, como se ha comentado anteriormente, la capacidad de un canal o dispositivo de comunicación.
En este último sentido, es una medida que caracteriza a los filtros de comunicaciones.
Un filtro es un dispositivo electrónico que deja pasar un rango de frecuencias de señales y elimina el resto de frecuencias que no esté en ese rango de frecuencias. Viene definido por la frecuencia máxima y mínima del filtro y su diferencia es el ancho de banda de filtro.
Este ancho de banda se establece como la diferencia de frecuencias en la cual la atenuación que sufre la señal que la traspasa es igual o inferior a 3 dB con respecto a la frecuencia central y de pico del filtro.
Lo vemos en la siguiente figura.



Existen diversos tipos de filtros de comunicaciones:
–Filtro paso bajo.
–Filtro paso alto.
–Filtro paso banda.
–Filtro banda eliminada.
Los filtros deben verse como ‘cajas negras’ de forma que tienen a la entrada señales de diferentes frecuencias y a la salida señales filtradas.

2.3. Codificación de datos

La codificación es una técnica usada en comunicaciones que consiste en la conversión de un sistema de datos en otro sistema de datos.
Cuando queremos transmitir datos por un medio de transmisión no podemos transmitirlos tal cual sino debemos convertirlos en otro formato adaptados al medio de transmisión para que puedan ser transmitidos. Esto es codificar los datos.
La codificación la realiza unos dispositivos denominados CODEC (Codificación- Decodificación) que se encargan (antes del envío del datos) de codificarlos (en la parte del emisor) y de decodificarlos (en la parte del receptor).
Evidentemente emisor y receptor deben emplear el mismo código de codificación para codificar y decodificar la información transmitida.
Dado que existen dos tipos de transmisión -analógica y digital-, se emplean técnicas de codificación diferentes para cada una de ellas.
Así encontramos:

- Técnicas de codificación de datos digitales.
  Para una transmisión digital.
- Técnicas de codificación de datos analógicos.
  Para una transmisión analógica.

Veremos a continuación con más detalle cada una de estas técnicas.

2.3.1. Técnicas de codificación de datos digitales

En una transmisión digital lo que se transmite son 0 y 1.
Pero estos 0 y 1 no se pueden transmitir tal cual sino que debe ser codificadas (traducidas) a estados de una señal como por ejemplo:

- Ausencia o presencia de señal.
- Cambio del voltaje de una señal.
- Diferencias de voltajes con respecto a una señal de referencia.
- Etc.

Esta traducción de 0 y 1 a estados de una señal es lo que realiza un CODEC y que emplea para ello diferentes técnicas de codificación de datos digitales.
Lo vemos en la siguiente figura:

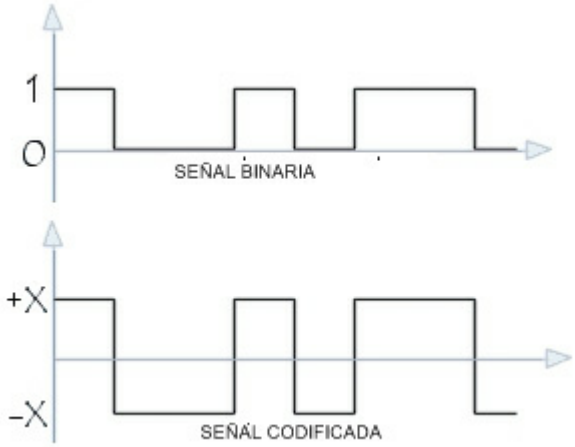
En la anterior figura podemos ver cómo el flujo de bits tras pasar por el códec se ha transformado en flujo de estados de una señal que es lo que realmente se transmite.
El receptor detectará estos cambios de señal y empleando la misma técnica de codificación será capaz de traducirlo en señales binarias de 0 y 1 tal y como se enviaron por parte del emisor.
Existen numerosas técnicas de codificación de señales digitales destacando como las más utilizadas las siguientes:

- Codificación NRZ.
- Codificación NRZI.
- Codificación Manchester.
- Codificación de Miller.
- Codificación bipolar.

A continuación veremos con más detalle el funcionamiento de cada uno de ellas.

Codificación NRZ:

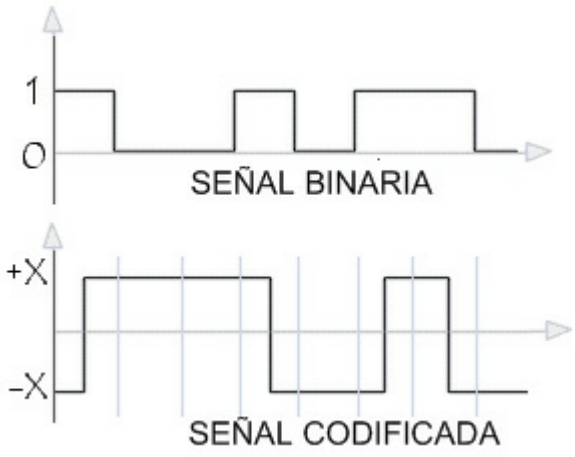
Se trata de una de las técnicas de codificación de señales digitales más sencillas y simples ya que fue de las primeras que aparecieron.
Se trata de una codificación de no retorno a cero (Not Return zero) y consiste en transmitir un valor de amplitud de señal X cuando queremos transmitir un 1 y un valor de amplitud de señal negativo –X cuando queremos transmitir un 0.
Nunca hay un valor 0 voltaje de señal en el canal (por eso lo de no retorno a cero).
En la siguiente figura puede verse cómo funciona esta codificación:



La figura de arriba representa el flujo de bits a transmitir y cuando queremos transmitir un 1 enviamos una señal con voltaje X y cuando queremos transmitir un 0 enviamos la misma señal y con el mismo voltaje pero en negativo.
Así el receptor en función del voltaje recibido (X o –X) decodificará si se ha enviado un 1 o un 0.

Codificación NRZI:

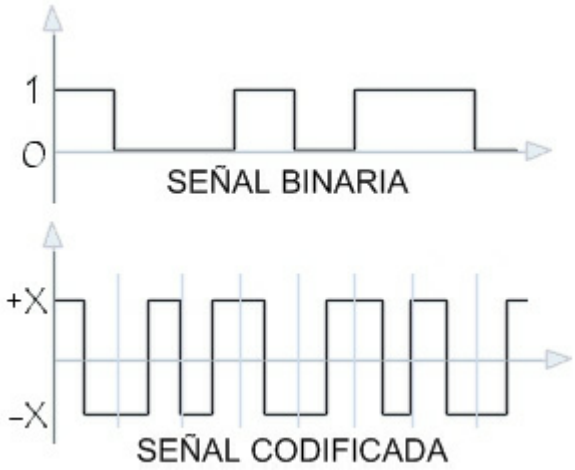
Se trata de una codificación de datos digitales en la cual la señal que se transmite por el canal cambia de estado cuando queremos transmitir un 1 y permanece en el mismo estado cuando transmitimos un 0.
Lo vemos en la siguiente figura:



La figura de arriba representa el flujo de bits a transmitir y cuando queremos transmitir un 1 provocamos un cambio de estado en la señal y si en cambio queremos enviar un 0 no cambiamos el estado de la señal transmitida.
Así el receptor en función de los cambios de estado de la señal recibida va decodificando si el emisor ha enviado un 0 o un 1.

Codificación de Manchester:

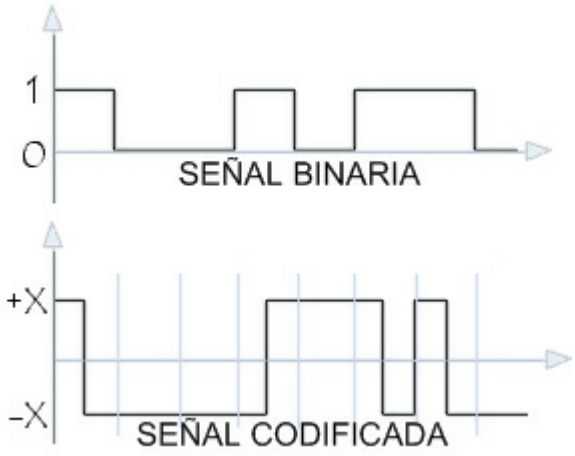
Se trata de una codificación de datos digitales en la cual se introduce una transición del estado cada vez que transmitimos un bit. Es por ello que también se le denomina codificación en dos fases.
Esta codificación podría equivaler realizar una OR exclusiva (XOR) con la señal de reloj de la transmisión digital.
En la siguiente figura podemos ver cómo funciona esta codificación:



La figura de arriba representa el flujo de bits a transmitir y cuando queremos transmitir un 1 enviamos un pulso con una transmisión de X a –X; y en cambio cuando queremos enviar un 0 enviamos un pulso con un transición de –X a X.
Así el receptor en función de estos pulsos y sus transiciones va decodificando si el emisor ha enviado un 0 o un 1.

Codificación de Miller:

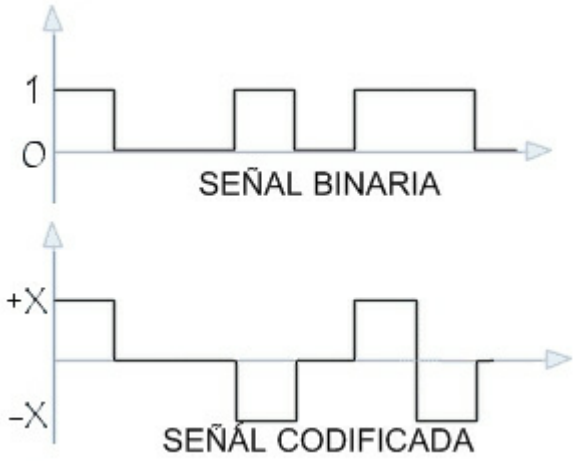
Se trata de una codificación de datos digitales muy similar al código Manchester pero en este caso la transición en medio del intervalo sólo se produce cuando se transmite un 1.
Lo vemos en la siguiente figura:



La figura de arriba representa el flujo de bits a transmitir y cuando queremos transmitir un 1 la señal incluye una transición en medio del intervalo. En cambio cuando queremos enviar un 0 no provocamos ningún cambio de la señal.
Esta técnica permite un mayor índice de datos a transmitir.

Codificación Bipolar:

Se trata de una codificación de datos digitales que a diferencia de los anteriores presenta tres estados (los anteriores sólo 2).
En esta codificación cuando se quiere transmitir un 0 se envía una señal con valor 0 y cuando se quiere enviar un 1 se envía la misma señal con valor X y –X alternativamente.
En la siguiente figura puede verse cómo funciona esta técnica de codificación:

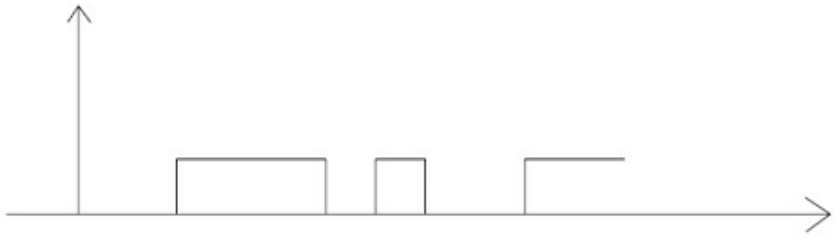


La figura de arriba representa el flujo de bits a transmitir y cuando queremos transmitir un 1 la señal incluye una transición en medio del intervalo. En cambio cuando queremos enviar un 0 no provocamos ningún cambio de la señal.
Esta técnica permite un mayor índice de datos a transmitir.

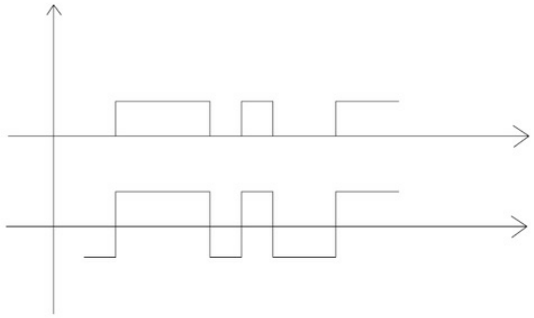
Veamos un **ejemplo**.
Queremos transmitir la siguiente secuencia de bits por un medio digital en la cual se va emplear la codificación NRZ.

0	1	1	1	0	1	0	0	1	1

Dibuja la secuencia de bits codificada que se envía al canal.
Solución:
Dibujemos en primer lugar en un diagrama de tiempos los bits originales que se quieren enviar, es decir:



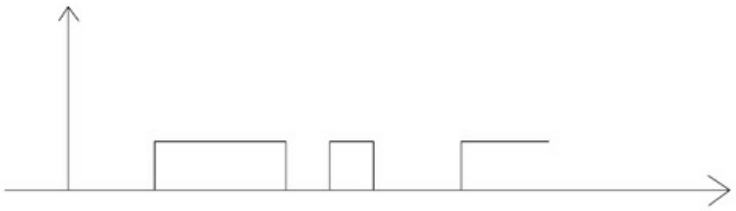
La codificación NRZ consiste en transmitir un pulso con amplitud –X cuando se quiere transmitir un 0 y un pulso con amplitud +X cuando se quiere transmitir un 1.
Superponemos en el mismo diagrama de tiempo los bits originales a enviar y la señal codificada según codificación NRZ.



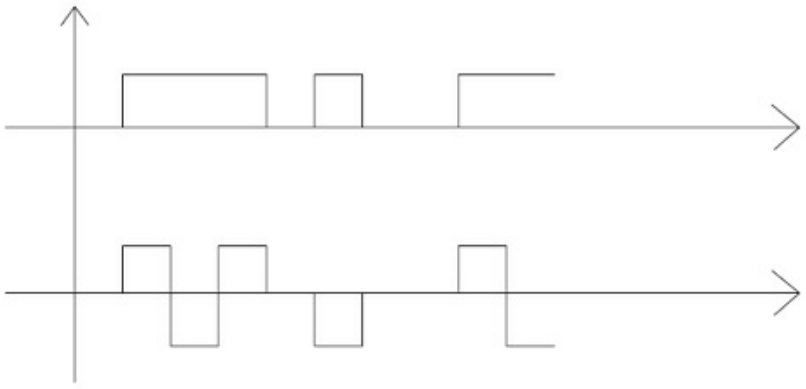
El hecho de que siempre se envíe una señal (negativa o positiva) favorece que el canal tenga siempre señal y sea más inmune al ruido.
Por otro lado su espectro es mayor por lo que requiere más ancho de banda.
Veamos otro ejemplo.
Queremos transmitir la misma secuencia de bits del ejemplo anterior pero ahora empleando la codificación bipolar.

0	1	1	1	0	1	0	0	1	1

Dibuja la secuencia de bits codificada que se envía al canal.
Solución:
Al igual que en el ejemplo anterior debemos dibujar en un diagrama temporal los bits originales que se quieren enviar:



La codificación bipolar cuando se quiere enviar un 0 no se transmite señal y cuando se quiere enviar un 1 se envía alternativamente una señal con amplitud X y – X.
Superponemos en el mismo diagrama de tiempo los bits originales a enviar y la señal codificada según codificación bipolar.



Esta es una de las codificaciones que se caracteriza por tener tres estados: ausencia de señal, señal positiva y señal negativa.

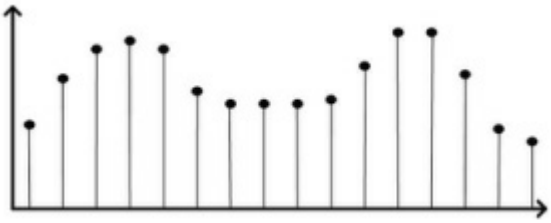
2.3.2. Técnicas de codificación de datos analógicos

Los datos analógicos se caracterizan porque pueden adoptar un número infinito de valores.
Los datos analógicos pueden ser transmitidos por medios analógicos o digitales, ya que el formato que tenga el dato es independiente del medio de transmisión por el que se quiere transmitir.
Para ello, se emplean técnicas de codificación que permiten traducir estos datos analógicos a estados de una señal adaptada al medio de transmisión (analógica o digital) y así poder transmitir los datos analógicos.
Existen diferentes técnicas de codificación para datos analógicos si los transmitimos por un canal digital o por un canal analógico.
Así que si los queremos transmitir por un canal digital lo primero que se realiza es una digitalización de la señal (pasamos el dato de analógico a digital) y obtenemos un flujo de bits el cual podemos emplear cualquiera de las técnicas de codificación de datos digitales descritos anteriormente.
Pero también podemos transmitir dichos datos analógicos empleando un medio analógico (transmisión analógica) y para ello existen, entre otras, las siguientes técnicas de codificación:

- Modulación en amplitud.
- Modulación en frecuencia.
- Modulación en fase.

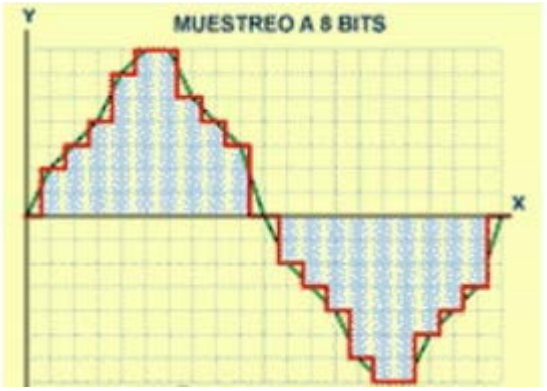
Técnicas de modulación existen muchas, aunque las tres anteriores son las más sencillas y básicas, ya que el resto suelen ser combinaciones de las tres anteriores.
Veremos a continuación cómo funciona cada una de estas técnicas de codificación de datos analógicos.
Hemos comentado anteriormente que los datos analógicos los podemos transmitir por un canal digital empleando la digitalización de la señal.
Veamos en qué consiste esta técnica.
La digitalización consiste en ir tomando muestras de la señal analógica en intervalos regulares y cuantificando la amplitud en cada una de las muestras tomadas.
Si cuantificamos (tomamos valores discretos de la amplitud de cada muestra) obtenemos así un flujo de bits que representa la digitalización en cada tiempo de la señal analógica y con ello ya podemos enviarlo por un canal digital empleando cualquiera de las técnicas de codificación digital.
En la siguiente figura podemos ver cómo funciona la digitalización de una señal analógica:

En la figura de arriba podemos ver el ejemplo de una señal analógica la cual puede adoptar cualquier tipo de valor de amplitud.
Con la digitalización tomamos valores a intervalos regulares a frecuencias f1, 2 x f1, 3 x f1, 4 x f1, etc., y en cada uno de ellos tomamos el valor que le corresponde en la señal analógica.
Si luego dibujamos la señal a partir de sus muestras podemos obtener una representación digitalizada de la señal analógica.
Lo vemos en la siguiente figura:



Pero la digitalización implica también una cuantificación de los valores de la señal muestreada ya que el valor tomado puede ser infinito.

Para ello cuantificamos la señal, es decir, tomamos el valor máximo y mínimo de la señal analógica y podemos cuantificarlo en un número discreto de valores, por ejemplo, 2, 4, 8, 16, etc.
Si por ejemplo tomamos un número discreto de 4 valores eso indica que la señal digitalizada sólo podrá tener uno de esos posibles valores y el valor tomado es el valor más cercano al valor de la señal analógica.
En cada una de las muestras se toman los valores de la señal analógica pero la cuantificación implica que debemos ajustarnos a uno de los 4 valores discretos posibles y esos valores son los que se transmite.
Esos cuatros valores posibles se pueden representar mediante 2 bits (2^2=4 valores).
A partir de estos cuatro valores a intervalos regulares podemos obtener la señal digitalizada.
Si en vez de cuatro valores, cuantificamos 8 valores, ello implica que podemos obtener una señal digitalizada más fiel a la señal analógica original, pero también transmitir más bits. Ocho valores implica tres bits (2^3=8 valores).
Lo vemos en la siguiente figura:



Lo mismo ocurre si muestreamos a intervalos de mayor frecuencia. Obtenemos una señal digitalizada más fiel a la señal analógica original pero ello implica un mayor número de bits a transmitir.
El teorema del Muestreo nos indica que con una frecuencia de muestreo de al menos el doble de la frecuencia máxima de la señal analógica es suficiente para no perder información.

2.4. Multiplexación

En una red de comunicaciones se transmite mucha información de diferentes usuarios y a diferentes puntos. Es por ello que se basa en una arquitectura e infraestructuras compartidas que es usada por muchos usuarios y equipos.
Para que sobre un mismo soporte pueda transmitirse información de diferentes usuarios, es preciso emplear técnicas como la multiplexación que permita que cada información llegue a su destino correcto y no se solape con el resto de información de otros usuarios.
A continuación veremos estas técnicas y en especial la multiplexación, técnica más habitualmente usada en las modernas redes de comunicaciones.

2.4.1. Concepto

En un enlace de comunicaciones entre dos o más equipos siempre se busca maximizar la capacidad del canal, es decir, buscar el máximo rendimiento de las comunicaciones.
Esto se consigue utilizando el mismo canal para transmitir varias comunicaciones independientes a la vez.
Una de las técnicas más empleadas para esto es la multiplexación.
Se define la multiplexación como la técnica que permite la transmisión por el mismo canal de diferentes comunicaciones independientes entre sí y de diferentes dispositivos o equipos, asegurando que la transmisión de cada una de ella sea fiable, segura y que no interfiera entre ellas consiguiendo con ello la máxima eficiencia de transmisión del canal.
Existen tres tipos de técnicas de multiplexación claramente diferenciadas:

- Multiplexación por división en frecuencia (FDM).
- Multiplexación por división en el tiempo (TDM).
- Multiplexación por división en la longitud de onda (WDM).

Cada una de ellas presenta sus ventajas e inconvenientes que veremos a continuación.

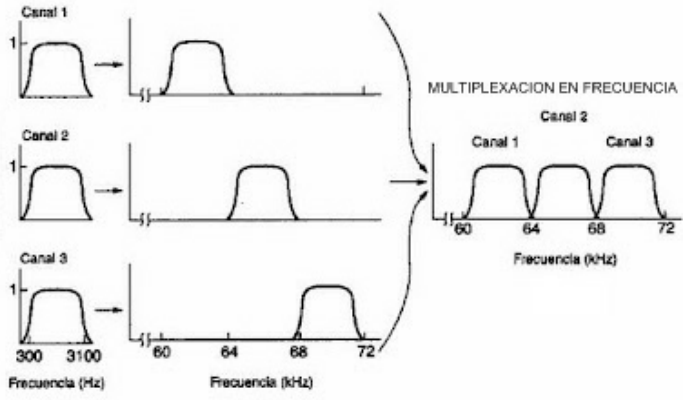
2.4.2. Multiplexación por división en frecuencias (FDM)

La multiplexación por división en frecuencias o FDM (Frecuency División Multiplexing) tiene sus orígenes en las transmisiones analógicas.

Se basa en transmitir cada comunicación en diferentes ventanas de frecuencias no solapadas entre sí y con ventanas de guardas.

De este modo aprovechamos al máximo todo el ancho de banda de canal, dividiendo este ancho en canales donde en cada uno de ellos transmitimos un canal de comunicación independiente del otro.

La capacidad del canal está limitada por el propio ancho de banda del canal.



La multiplexación por división en frecuencias presenta las siguientes ventajas:

- Bajo coste al ser una tecnología ya muy madura.
- Posibilidad de conectarse en cascada entre varios equipos.

Las desventajas que ofrece son las siguientes:

- Presenta un número limitado de canales a transmitir en función del ancho de banda del canal.
- Presenta baja eficiencia al precisar bandas de guarda.
- Necesidad de mantener el sincronismo en las frecuencias de funcionamiento.
- Necesidad de utilizar filtros en los equipos.

2.4.3. Multiplexación por división en el tiempo (TDM)

La multiplexación por división en el tiempo o TDM (Time División Multiplexing) surge a partir de las transmisiones digitales cuando se emplea la transmisión de datos binarios (bits).

Se basa en dividir el tiempo en intervalos donde en cada intervalo se envía una trama de bits de una comunicación.

De este modo aprovechamos al máximo todo el ancho de banda de canal dividiendo dicho ancho de banda en canales donde en cada uno de ellos transmitimos un canal de comunicación independiente del otro.

La capacidad del canal está limitada por el propio ancho de banda del canal.

2.4.4. Multiplexación por división de longitud de onda (WDM)

La multiplexación por división de longitud de ondas o WDM (WaveLength División Multiplexing) es un tipo de multiplexación similar a la multiplexación por división de frecuencias pero en vez de hablar de frecuencias hablamos de longitud de ondas (λ).

Este tipo de multiplexación se emplea en transmisiones por infrarrojos donde el canal de transmisión se divide en ventanas de longitud de onda y cada canal de comunicación se envía en una determinada ventana de transmisión.

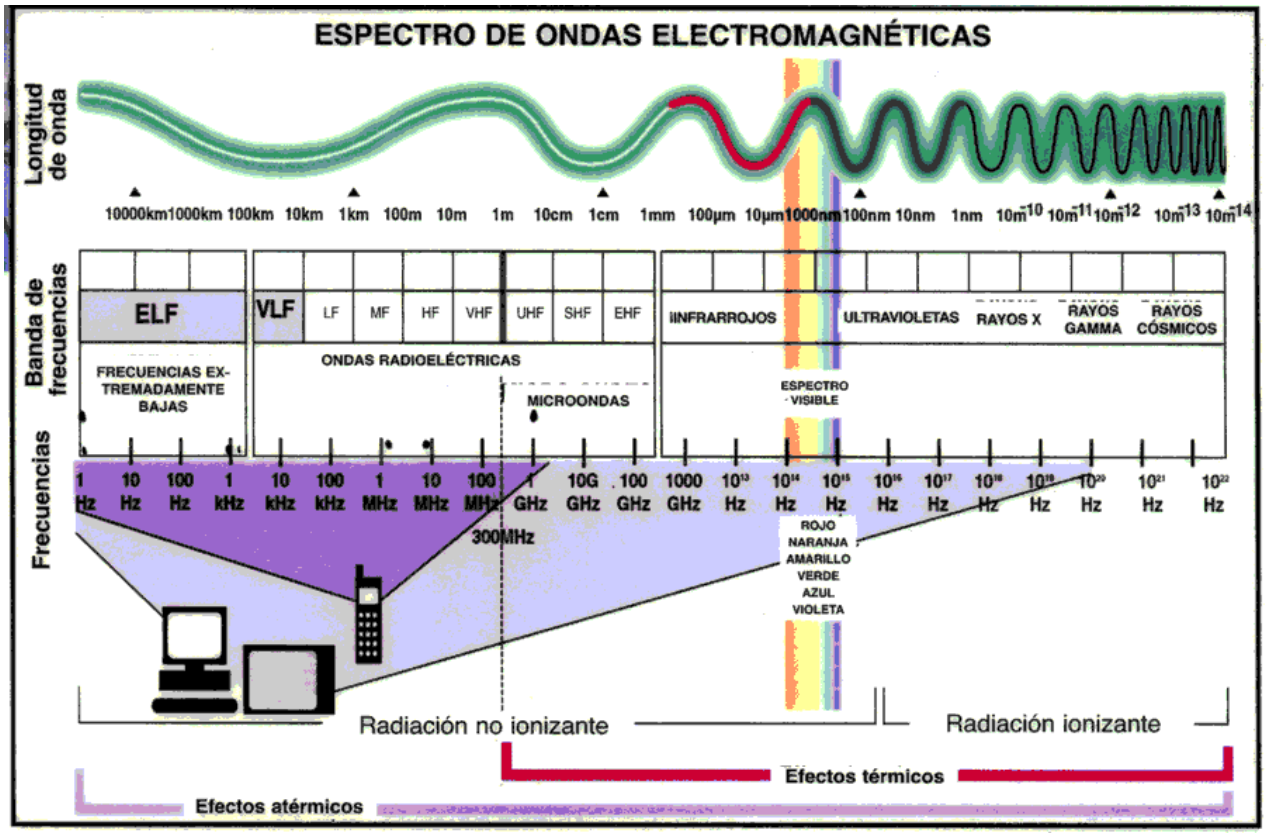
De este modo somos capaces de enviar n comunicaciones simultáneamente, cada una de ella en una ventana o longitud de onda diferente.

El número de ventanas o canales que se pueden transmitir dependerá de la longitud de la ventana de cada canal y de la longitud de la ventana total del medio de transmisión.

La multiplexación por división de longitud de onda se emplea cada vez más en las transmisiones ya que suelen ofrecen un gran ancho de banda para los nuevos servicios de telecomunicaciones.

En el emisor requiere de un multiplexor óptico y en el receptor de un demultiplexor óptico.

Videos de la NASA sobre el espectro electromagnético…: https://youtu.be/ixwxOQf50kc



Como funciona Internet: https://youtu.be/rw41W8crZ_Y

Video sencillo sobre frecuencias: https://www.youtube.com/watch?v=v-7kwC3pqcE

Otros Vídeos interesantes, aunque no tengan que ver con el curso:

https://www.youtube.com/watch?v=i985eNEB2QM (Ondas de radio)

https://www.youtube.com/watch?v=VWWSu0BrQkk (Microondas)

https://www.youtube.com/watch?v=8ybXNZQGzSQ (Infrarrojos)

https://www.youtube.com/watch?v=YCWvxv__nmQ (Luz visible)

https://www.youtube.com/watch?v=MM6BjtLEH34 (Ondas ultravioletas)

https://www.youtube.com/watch?v=OD8Ff1hHk1U (Rayos X)

https://www.youtube.com/watch?v=4tK-FRo9Ktk (Rayos Gamma)

2.5. Conmutación

La conmutación es una técnica ampliamente utilizada en comunicaciones consistente en poner en contacto un equipo con otro empleando una infraestructura común de comunicaciones para la transmisión de los datos.
Con ello se pretende dar eficiencia al sistema ya que varios equipos pueden emplear la misma infraestructura para enviar datos y no crear redes y recursos individuales para cada transmisión que encarecería enormemente la infraestructura.
Esta técnica por tanto permite que en un momento dado equipo emisor y equipo receptor estén conectados para la transferencia de la información y cuando termina la transferencia libera los recursos para que puedan ser usados para otra transmisión de otros equipos.
Existe dos tipos o técnicas de conmutación:

- Conmutación de **circuito**.
- Conmutación de **paquetes**.

Lo vemos ahora con más detalle.

Conmutación de circuitos:
Es una técnica de conmutación basada en el establecimiento de una conexión física entre los dos extremos (emisor y receptor) empleando para ello y conectando todos los elementos y nodos intermedios para que durante la transferencia exista ese camino físico para el intercambio de la información.
Cuando se termina la transferencia se liberan todas las conexiones intermedias y queda a disposición de la red para otra comunicación del mismo o de diferentes equipos.
Esta conmutación de circuitos permite ser implementados de dos formas:

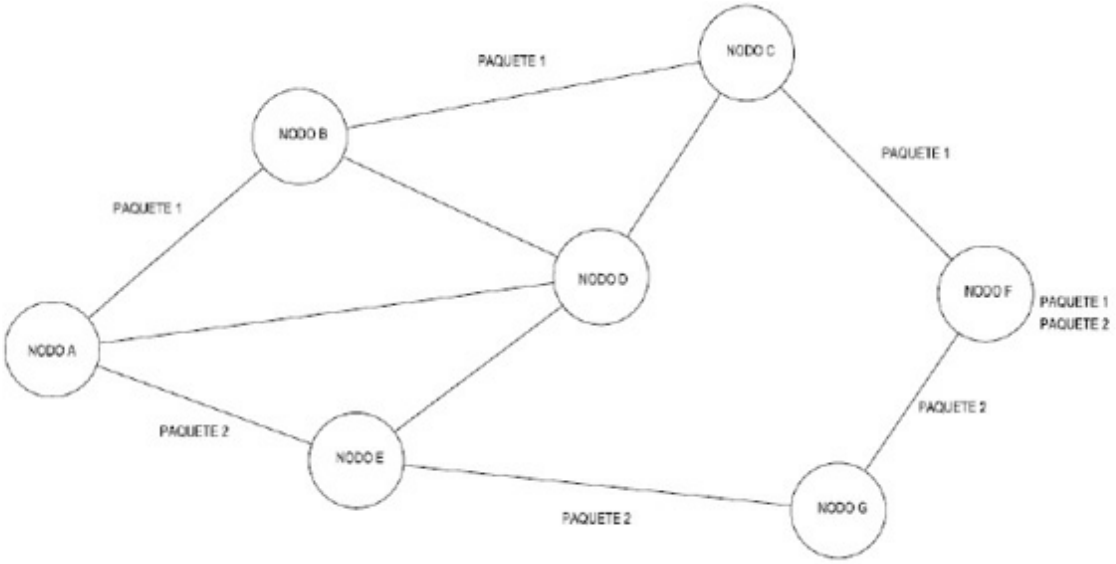
- Conmutación de circuitos espacial:
  Es aquella que durante la transferencia el circuito establecido está permanente y en exclusiva para el emisor y receptor y sólo se libera cuando haya finalizado la transferencia.
- Conmutación de circuitos temporal:
  En esta se crean espacios temporales de transmisión de forma que cada comunicación emplea una serie de intervalos de tiempo para transmitir pero todas las comunicaciones emplean el mismo circuito o enlace físico.

En la conmutación de circuitos se establece una conexión física a través de varios enlaces y nodos intermedios para unir emisor y receptor.
En la conmutación de circuitos temporales en cambio se establecen slots temporales.
Cada slot temporal es utilizado por un canal de comunicaciones pero todos ellos usan el mismo enlace o circuito de conexión.
Este tipo de conmutación es el empleado por el servicio telefónico RTC (red telefónica conmutada).

Conmutación de paquetes:
La conmutación de paquetes es una técnica que 'trocea' la información en paquetes de longitud fija y envía cada paquete desde el emisor al receptor.
Cada paquete puede utilizar una ruta diferente para llegar al destino y para poder llegar a ese destino cada paquete incluye una cabecera (además de la información) que contiene la dirección origen y destino del paquete.
Cada nodo de la red analiza la cabecera del paquete y decide si es para él o si debe enrutarla a otro nodo para hacerlo llegar a su destino.
Este tipo de conmutación es más eficiente que la conmutación de circuito ya que aprovecha mejor los recursos del sistema.
Internet utiliza para la transmisión de los datos la conmutación de paquetes.
Uno de los problemas de este tipo de conmutación es el retardo sufrido por los paquetes (al tener que pasar por muchos nodos), las pérdidas de paquetes y la llegada desordenada de paquetes del mismo mensaje en el receptor (ya que llegan por rutas diferentes). Estos dos últimos problemas implican que el sistema debe incluir técnicas de detección y corrección de paquetes.
La conmutación de paquetes admite dos implementaciones:

- Modo circuito virtual u orientado a conexión:
  En este tipo de conmutación de paquetes, todos los paquetes pertenecientes al mismo mensaje siguen la misma ruta, por lo que previamente se debe establecer un circuito virtual entre emisor y receptor.
  Así cada paquete además de la dirección origen y destino incluye el número de conexión por el que va dirigido.
  La ventaja es que evita la llegada desordenada de paquetes aunque incluye más retardo debido al tiempo de establecimiento del circuito virtual.
- Modo datagrama u orientado a no conexión:
  En este tipo de conmutación de paquetes, cada paquete puede ir por rutas diferentes dependiendo del estado de la red y de cada uno de los enlaces.
  Esto implica que los paquetes puedan llegar desordenados y serán aplicaciones de niveles superiores a nivel de red quienes deban aplicar técnicas de detección y corrección de paquetes.
  La ventaja es que hay menos retardo que en el modo circuito virtual u orientado a conexión.

Veamos un **ejemplo**.
Dada la siguiente red formada por el conjunto de nodos y en que se quiere enviar un mensaje del nodo A al nodo F.



Para ello el mensaje se paquetiza en 2 paquetes y donde cada uno de ellos sigue la ruta marcada en la figura y donde el tiempo de retardo de conmutación es de 2 mseg, averigüe lo siguiente:

- ⇨ De qué tipo de conmutación se trata.
- ⇨ El tiempo total de retardo de cada paquete para llegar a su destino.

Solución:
El enunciado nos introduce que el mensaje se paquetiza en dos paquetes por lo que de ello se deduce que se trata de una conmutación de paquetes.
El problema es que debemos discernir si se trata de una conmutación de paquetes orientado o no a conexión. Dado que los paquetes a la vista de la figura siguen rutas diferentes (aun siendo del mismo mensaje original) se concluye que se trata de una conmutación de paquetes modo datagrama u orientado a no conexión.
En cuanto al retardo, el retardo total de cada paquete será la suma de todos los retardos acumulados por cada uno de los nodos por lo que debe conmutar.
En el caso del paquete 1 debe pasar por tres nodos, por lo que el retardo del paquete será de:

$$Retardo_{paquete}\ 1 = 3 \times retardo_{conmutación} = 2 \times 3\ mseg = 6\ mseg$$

En el caso del paquete 2 debe pasar por cinco nodos, por lo que el retardo del paquete será de:

$$Retardo_{paquete}\ 2 = 5 \times retardo_{conmutación} = 5 \times 3\ mseg = 15\ mseg$$

3. Medios de transmisión guiados

3.1. El par trenzado

Un medio de transmisión es un canal por el cual se pueden transmitir datos o información entre dos equipos.
Sin un medio de transmisión por tanto no existirían las redes cuyo objetivo principal es enviarse datos entre los equipos o elementos que forman la red.
Una primera clasificación de los medios de transmisión es:

- Medios de transmisión guiados:
  Son aquellos que precisan de un medio físico (generalmente un cable) por donde va guiada la información o datos a transmitir.
- Medios de transmisión no guiados:
  Son aquellos donde la información se transmite por un medio (también físico) pero no van guiados o encapsulados. Es el caso de las transmisiones por radiofrecuencia. En este caso se emplean antenas.

El emplear uno u otro medio de transmisión dependerá de la información que se quiera transmitir (tasa binaria a transmitir, disponibilidad, costes, etc).
Dentro de cada uno de ellas existirán diferentes implementaciones que veremos a continuación.
Como se ha descrito anteriormente, los medios de transmisión guiados suelen emplear un cable para transmitir la información de un equipo a otro.

Entre los cables más empleados actualmente como medio de transmisión destacan:

- El par trenzado.
- El cable coaxial.
- La fibra óptica.
- El hilo telefónico.

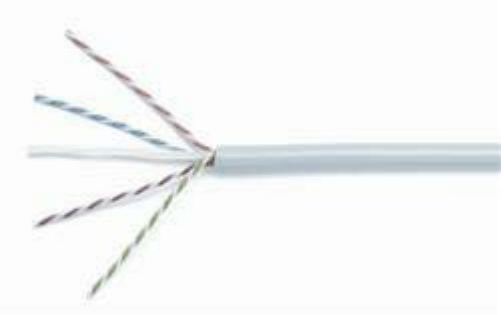
Cada uno de los cables anteriormente citados presenta una serie de ventajas e inconvenientes que lo hacen más adecuado para un tipo de servicio de telecomunicación u otro.
Así por ejemplo, el par trenzado se emplea sobre todo para redes de datos, mientras que el cable coaxial para redes multimedia (televisión, megafonía, etc.).
La fibra óptica se está imponiendo cada vez más como medio de transmisión tanto para servicio de datos como por servicios multimedia debido a su baja atenuación y por la alta tasa binaria de transmisión que ofrece.
El par de hilo telefónico, aunque ya está quedando relegado por su bajas prestaciones, tiene la gran ventaja de estar implantado en el mercado (prácticamente toda la red telefónica se ha realizado bajo este cable), por ello se utiliza en la actualidad.
Los medios de transmisión cableados, a diferencia de los medios no guiados, por regla general suelen tener mejores prestaciones de seguridad, tasa binaria de transferencia, etc., aunque presentan como inconveniente que es más cara su instalación (requiere la tirada del cableado y de las canalizaciones que lo soporten).

Entre los servicios de telecomunicaciones que emplean estos medios de transmisión guiados destacamos:

- Transmisión de datos.
- Servicios de radio y televisión
- Servicio telefónico.
- Servicio de control y gestión de red.

En los medios de transmisión guiados también es importante destacar el elemento de los conectores que son los dispositivos que permiten el empalme de estos cableados con la electrónico o los equipos remotos o la unión de cables del mismo tipo o de diferentes tipos.
La compleja red de distribución que se emplea para la transmisión de información hace frecuente que en numerosas ocasiones en un mismo enlace encontremos tramos con diferentes tipos de cable. Es el ejemplo de las redes HFC (hybrid fibre coaxial) donde se mezclan tramos con cable coaxial y tramos con fibra óptica.

A continuación, veremos con más detalle cada uno de estos medios de transmisión guiados que se emplean en la actualidad y los servicios de telecomunicación que la soportan.
El par trenzado es uno de los medios de transmisión guiados más empleados actualmente, sobre todo en el ámbito de la conexión de equipos y redes de ordenadores.
Fue creado por Graham Bell y ha sido el cable de transmisión para las líneas telefónicas, de ahí su amplia difusión y comercialización.
A lo largo de la historia ha sufrido notables mejoras en características constructivas y de transmisión, que lo hace aún imprescindible en los nuevos servicios de telecomunicaciones y futuros.
Ampliamente consolidado, se caracteriza por su bajo coste y fácil instalación, existiendo además, como veremos más adelante, diferentes categorías y modelos, cada uno adaptado para el servicio o señales que se quiere transmitir por él.



3.1.1. Características constructivas

El par trenzado es un cable basado en dos conductores eléctricos de cobre entrelazados entre sí para anular las interferencias que se generan entre sí y la diafonía.
Aunque existen varias variantes, el más común es el par trenzado de 4 pares de cobre. Se trata como su propio nombre dice de 4 pares de cobre (8 hilos) entrelazados por parejas.
El entrelazado es lo que lo hace inmune a las interferencias y a la diafonía, por lo que cuanto más entrelazado vaya más inmune es a estos dos problemas.
El cable puede incluir además una malla de cobre rodea al par de conductores que lo blinda de interferencias exteriores.
En base a la presencia de esta malla de cobre y su configuración, existen tres tipos de par trenzado:

- UTP (Unshielded twisted pair)
- STP (Shielded twisted pair)
- FTP (Foiled twisted pair)

Veremos a continuación las características de cada uno de ellos.

UTP (Unshielded twisted pair):

Es el par trenzado sin apantallar. En este caso los pares de hilos trenzados no incluyen una malla de cobre que lo hace de blindaje contra las interferencias externas. Por ello es más barato, de menor peso y más fácil de instalar. Es el tipo de par trenzado más habitualmente utilizado.

STP (Shielded twisted pair):

Es el par trenzado que incluye una malla de cobre que por cada par y que lo hace más inmune a las interferencias exteriores. Es más caro que el UTP, es de mayor peso y más difícil de instalar. Esto último además porque requiere que los cables estén conectados a un buen nivel de tierra que no siempre es fácil de conseguir.

FTP (Foiled twisted pair):

Es el par trenzado que incluye (sobre el STP) un blindaje global, es decir, además posee una malla de cobre que rodea a todos los pares y que lo hace aún más inmune a las interferencias. Presenta las mismas ventajas e inconvenientes que el STP pero en este caso es más caro aún, de mayor peso y más difícil de instalar. Se usa en entornos muy profesionales.

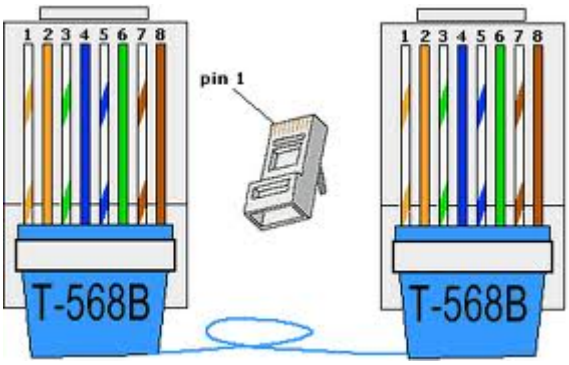
El par trenzado en sus extremos utiliza un conector denominado conector RJ-45.

Se trata de un conector que admite hasta 8 hilos y que para su conexión o crimpado debe seguir lo que se denomina un código de colores.
El código de colores no es más que la disposición que debe seguir los hilos (el cual se le asigna un color según la norma EIA/TIA 568) y que establece qué función tiene cada hilo (transmisión, recepción, etc).
En base a esto el par trenzado se puede configurar en modo recto (o normal) o en modo cruzado.
En modo recto se emplea para conectar equipos a un dispositivo de interconexión (por ejemplo a una red LAN) y en modo cruzado se emplea para conectar equipos entre sí.
A continuación veremos con más detalle cada uno de estos modos.

Configuración en modo recto:

El par trenzado crimpado en modo recto o normal se utiliza para conectar equipos a una red local (LAN) que emplea dispositivos de interconexión como hub, switch, router, etc.
Para ello los extremos del par trenzado deben ser crimpados según la norma EIA/TIA 568-B que establece cómo se debe seguir el orden de disposición de los hilos de cobre cuando se crimpa en el conector RJ-45.
Esta norma establece la siguiente disposición de los hilos:

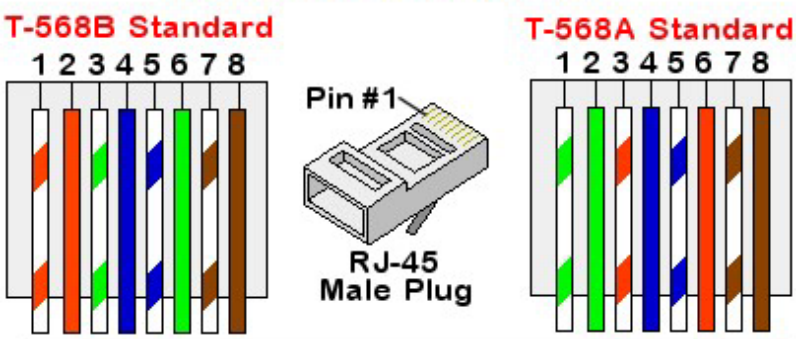
EXTREMO 1		EXTREMO 2	
PIN	Hilo de color	PIN	Hilo de color
1	Blanco-naranja	1	Blanco-naranja
2	Naranja	2	Naranja
3	Blanco-verde	3	Blanco-verde
4	Azul	4	Azul
5	Blanco-azul	5	Blanco-azul
6	Verde	6	Verde
7	Blanco-marrón	7	Blanco-marrón
8	Marrón	8	Marrón



Configuración en modo cruzado:

El par trenzado crimpado en modo cruzado se utiliza cuando queremos conectar dos equipos directamente para la transmisión de datos sin ningún elemento intermedio.
Para ello los extremos del par trenzado deben ser crimpados según la norma EIA/TIA 568-A que establece cómo se debe seguir el orden de disposición de los hilos de cobre cuando se crimpa en el conector RJ-45.
Esta norma establece la siguiente disposición de los hilos:

EXTREMO 1		EXTREMO 2	
PIN	Hilo de color	PIN	Hilo de color
1	Blanco-naranja	1	Blanco-verde
2	Naranja	2	Verde
3	Blanco-verde	3	Blanco-naranja
4	Azul	4	Azul
5	Blanco-azul	5	Blanco-azul
6	Verde	6	Naranja
7	Blanco-marrón	7	Blanco-marrón
8	Marrón	8	Marrón



Aquí tenéis un enlace a un video "comercial" que explica como crimpar los cables de par trenzado y luego testearlos usando las herramientas que hemos visto en el curso.

3.1.2. Características de transmisión

El par trenzado como ya se ha comentado anteriormente es ampliamente utilizado sobre todo en cableado estructurado.

No obstante este tipo de transmisión tiene una fuerte dependencia con la distancia (a mayor distancia más se atenúa la señal) y una fuerte dependencia con la frecuencia. Estos dos factores limitan a que el par trenzado no pueda ser usarse para distancias mayores a 100 m, con objeto de mantener sus propiedades eléctricas y de transmisión.

Es decir, podremos usar dicho par trenzado hasta una distancia de 100 metros (sin dispositivos de interconexión intermedios). Para distancias superiores, debemos utilizar otro cable bien coaxial o sobre todo fibra óptica.

No obstante, si empleamos dispositivos intermedios (hub, switch, router, etc) podemos aumentar la distancia en tramos de 100 metros (estos dispositivos regeneran la señal).

La fuerte dependencia con la frecuencia limita también el ancho de banda del par trenzado y su tasa de datos.

La interferencia externa y el ruido externo también son factores importantes.

No obstante, para redes locales (donde las distancias son relativamente cortas) es el medio de transmisión guiado por excelencia por sus buenas prestaciones, bajo coste y fácil instalación.

Proporciona para estas distancias gran ancho de banda (10 Gbps) gracias a las nuevas categorías que existen ya en el mercado y por tanto lo hace claramente apto para los nuevos servicios de telecomunicaciones como streaming, VoIP, televisión sobre IP, etc.

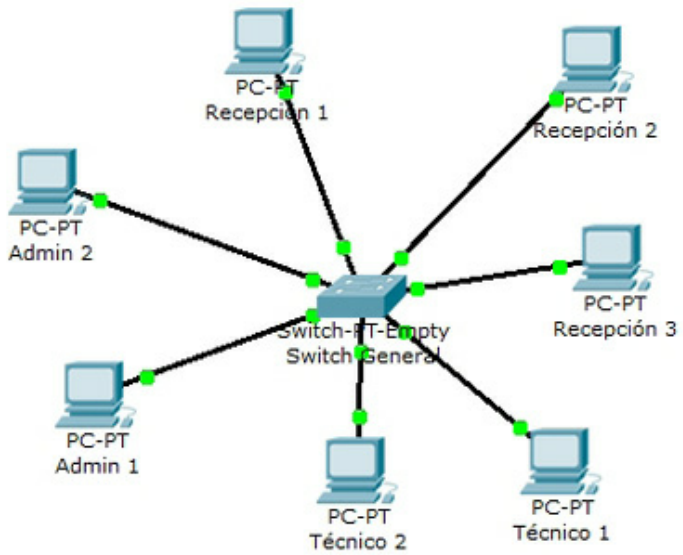
3.1.3. Aplicaciones

Aunque ya se ha comentado anteriormente el par trenzado es utilizado en una amplia variedad de aplicaciones destacando las siguientes:

- Redes de datos con velocidades de hasta 10 Gbps.
- Telefonía sobre IP (VoIP).
- Streaming de video y televisión sobre IP.
- Conexiones punto a punto entre equipos.
- Enlaces submarinos.

Veamos un **ejemplo**.

Dado el siguiente esquema de red de área local, indica qué tipo de cable de par trenzado emplearía en cada una de las conexiones.

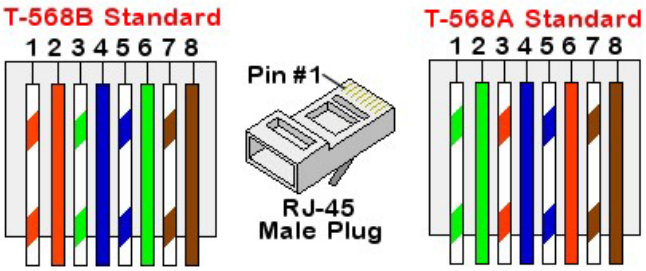


Solución:
Dado que todos los equipos están conectados a un elemento de interconexión, se debe emplear el par trenzado en modo normal o recto.
Para ello se debe crimpar el cable en sus extremos a un conector RJ-45 según la normativa EIA/TIA-568-B.

Veamos otro **ejemplo**.
Dado el siguiente esquema de conexión de dos ordenadores, indica qué modo de configuración debería tener el par trenzado y cumplimenta la tabla de la asignación de hilos al conector RJ-45.

Solución:
En este caso para conectar dos ordenadores para la transmisión de datos debemos emplear un par trenzado en modo configuración cruzada. Para ello debemos seguir el código de colores según la normativa EIA/TIA 568-A.
La asignación de los pares quedaría como sigue:

EXTREMO PC 1		EXTREMO PC 2	
PIN	Hilo de color	PIN	Hilo de color
1	Blanco-naranja	1	Blanco-verde
2	Naranja	2	Verde
3	Blanco-verde	3	Blanco-naranja
4	Azul	4	Azul
5	Blanco-azul	5	Blanco-azul
6	Verde	6	Naranja
7	Blanco-marrón	7	Blanco-marrón
8	Marrón	8	Marrón



3.1.4. Tipos de cables y categorías. Ancho de banda

La norma EIA/TIA 568 anteriormente citada clasifica el par trenzado en diversas categorías en función del ancho de banda que ofrece, que viene determinado por su construcción.
Dependiendo de este ancho de banda, cada categoría podrá soportar unos servicios u otros.

Categoría	Ancho de banda	Aplicaciones
Cat3	16 Mhz	10-BaseT y 100-BaseT
Cat5	100 Mhz	100-BaseT y 1000-BaseT
Cat5e	100 Mhz	100-BaseT y 1000-BaseT
Cat6	250 Mhz	1000-BaseT
Cat6e	500 Mhz	10G-BaseT
Cat7	600 Mhz	10G-BaseT y 100G-BaseT
Cat7e	1200 Mhz	10G-BaseT y 100G-BaseT

En la actualidad la Cat 8 con las normas ISO Clase I, II permite anchos de banda máximos de 2000 MHz con aplicaciones 25/40G Base-T
Algunas categorías no se mencionan porque han quedado ya obsoletas y no se utilizan actualmente.

Ejemplo:
Supongamos que queremos transmitir un archivo de 10 Mbytes por un canal de transmisión basado en un par trenzado **Cat5e**. con velocidad nominal de 100-Base-T.
Calcula el tiempo de transmisión de dicho mensaje por ese medio de transmisión.
Solución:
Antes de todo debemos pasar ambas magnitudes (la de velocidad de transmisión y del tamaño del archivo) a la misma magnitud ya que en un caso hablamos de bits/seg y en otro de bytes, sabiendo que 1 byte = 8 bits.
En base a lo anterior un archivo de 10 Mbytes en bits será:
10 Mbytes = 10 x 1024 Kbytes x 1024 bytes x 8 bits = 83.886.080 bits.
Ahora sólo se trata de dividir el tamaño de ese archivo por la velocidad de transmisión del canal, es decir, 100 Mbps, con lo que el resultado que se obtiene es el siguiente:

$$T_{transmisión} = \frac{83.886.080 \text{ bits}}{100 \times 1024 \text{ kbps} \times 1024 \text{ bits}} = 0,8 \text{ seg}$$

Veamos otro **ejemplo**.
Supongamos que queremos transmitir el mismo archivo del ejemplo anterior empleando ahora un par trenzado de categoría **6a**. Calcula el nuevo tiempo de transmisión y obtén conclusiones al compararlo con el resultado anteriormente obtenido.
Solución:
En este caso aplicamos el mismo procedimiento que en el caso anterior, pero modificando la velocidad de transmisión ya que en este caso es de 10 Gbps, por lo que el tiempo de transmisión obtenido será el siguiente:

$$T_{transmisión} = \frac{83.886.080 \text{ bits}}{100 \times 1024 \text{ Mbps} \times 1024 \text{ kbps} \times 1024 \text{ bits}} = 0,0078 \text{ seg}$$

Como puede observarse se tiene un tiempo de transmisión menor, es decir, es un canal para transmitir datos a mayor velocidad.

3.1.5. Ventajas e inconvenientes

El par trenzado es ampliamente utilizado como medio de transmisión guiado en numerosas aplicaciones por sus grandes ventajas.
No obstante también presenta algunos inconvenientes que presentamos a continuación.
Las **ventajas** principales que presenta el par trenzado son:

- Bajo coste.
- Fácil instalación.
- Gran ancho de banda (hasta 10 Gbps).
- Buenas prestaciones frente a interferencias y diafonía.
- Permite la escalabilidad, es decir, crear redes con un alto número de equipos.
- Ampliamente consolidado.

En cambio también presenta los siguientes **inconvenientes**:

- Presenta la limitación de 100 metros sin elementos de interconexión para mantener sus propiedades de transmisión. Limitación por segmento.
- Baja inmunidad al ruido
- Alta tasa de error a altas velocidades.

No obstante, a pesar de estas limitaciones es el medio de transmisión más empleado para redes de área local (LAN) donde con ellos se pueden transmitir los nuevos servicios de telecomunicaciones que exigen gran ancho de banda como el streaming de vídeo o la televisión por Internet.

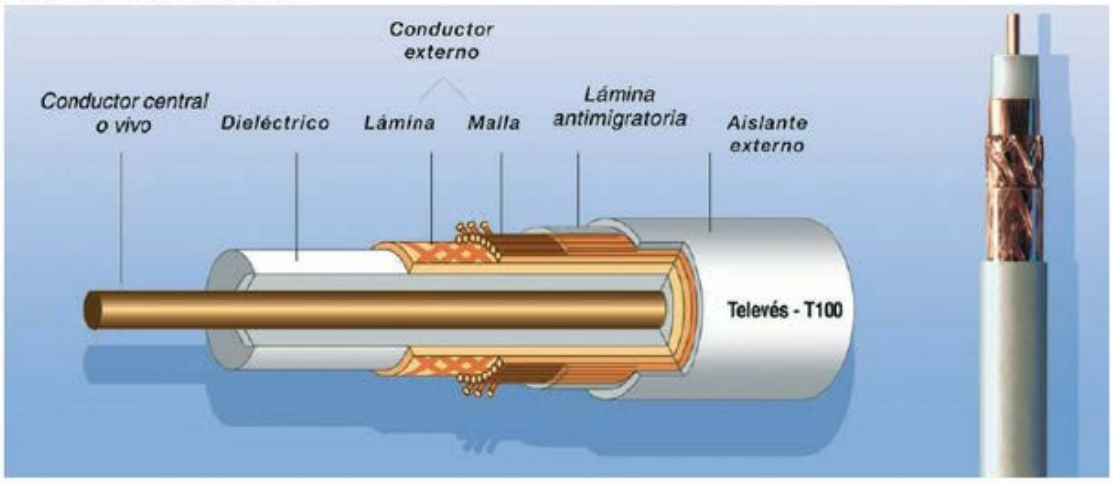
3.2. El cable coaxial

El cable coaxial es uno de los medios de transmisión guiados más empleados actualmente sobre todo en el ámbito multimedia, es decir, para transmisión de audio y vídeo.
Fue creado en los años 30 para transportar señales eléctricas de alta frecuencia pero actualmente y debido a que cada vez se utilizan señales de más alta frecuencia y a la digitalización de las transmisiones ha sido sustituido por el par trenzado (en distancias cortas) y por la fibra óptica para distancias superiores de centenares de metros y de kilómetros.

3.2.1. Características constructivas

El cable coaxial se compone de un hilo conductor central de cobre (denominado vivo) rodeado de una malla de hilos de cobre. En medio del hilo conductor y la malla de hilo se encuentra un dieléctrico (materiales que no conducen la electricidad) que separa ambos conductores para mantener las propiedades eléctricas de transmisión. Además todo el cable está cubierto por otro material aislante para reducir de las interferencias electromagnéticas del entorno y de otros cables y finalmente lo cubre un material de plástico para dar rigidez e indeformabilidad al conjunto. Normalmente usa una lámina antimigratoria que evita la migración de los aditivos de la cubierta y la humedad al interior del cable, evitando así el deterioro de sus características. En la imagen siguiente puede verse cómo es la estructura del cable coaxial:

Detalle del corte del cable coaxial



Podemos clasificar el cable coaxial en función de dos parámetros:

- Por su grosor.
- Por su banda de transmisión.

Por su grosor, el cable coaxial puede ser de dos tipos:

- Coaxial delgado (thin coaxial):
  Es el tipo de coaxial que presenta un bajo grosor (alrededor de los 7 mm de diámetro exterior) y por ello es menos rígido y más fácil de instalar. Se utiliza sobre todo para instalaciones donde las distancias no son elevadas (menos de 75 metros aproximadamente).
- Coaxial grueso (thick coaxial):
  Es un coaxial con un mayor grosor (alrededor de los 11 mm o incluso más de diámetro exterior). Es más rígido y por tanto más difícil su instalación, en cambio, atenúa menos la señal y por ello es más adecuado para instalaciones donde haya un mayor número de metros de distancias (algunos centenares de metros).

En función de su banda de transmisión podemos también encontrar dos tipos de coaxial:

- Coaxial en banda base:
  Es el tipo de coaxial donde se transmiten señales en baja frecuencia, generalmente digitales, con una resistencia de 500 Ω y se empleaba para redes de ordenadores, aunque ya se ha visto anteriormente que ha sido sustituido en este campo por otros medios de transmisión como el par trenzado y la fibra óptica.
- Coaxial en banda ancha:
  Es el tipo de coaxial donde se transmite señales de mayor frecuencias (generalmente del entorno de Mhz) y se utiliza para señales analógicas multiplexadas (combinar dos o más señales, y transmitirlas por un solo medio de transmisión) como por ejemplo de radio y televisión. De ahí su uso para aplicaciones de audio y vídeo. Presenta unas buenas prestaciones de calidad para este tipo de servicio y su instalación es barata y rápida.

En la tabla siguiente mostramos un resumen de los diferentes tipos de coaxial en función de su grosor y de su banda de transmisión:

Parámetro de clasificación	Tipo de coaxial
Por su grosor	Coaxial delgado
	Coaxial grueso
Por su banda de transmisión	Coaxial de banda base
	Coaxial de banda ancha

Cada tipo de coaxial será más adecuado para la transmisión de un tipo u otro servicio de telecomunicación. También es importante en los coaxiales su nivel de impedancia (resistencia a la corriente eléctrica) siendo de 50 Ω para los cables delgado y de 75 Ω para los cables gruesos. En audio menor impedancia equivale a más volumen (lo que no significa que sea de mayor calidad)

3.2.2. Características de transmisión

El cable coaxial, como todos los medios de transmisión cableados, atenúa la señal que transmite con la distancia.

Además, el cable coaxial es fuertemente dependiente con la frecuencia, es decir, presenta atenuaciones diferentes de la señal transmitida en función de qué frecuencia va la señal.

En función de cómo atenúa la señal según la frecuencia, podemos encontrarnos cables coaxiales de alta y de baja atenuación. El grosor es un parámetro constructivo esencial en esta atenuación con la frecuencia estableciéndose la relación de que cuanto más grueso es el cable coaxial menor es la atenuación del cable (en toda la banda de frecuencia de trabajo).
El problema, como ya se ha comentado anteriormente, es que un coaxial grueso es más rígido, más difícil de instalar y más caro, y por ello se emplea sólo cuando es esencialmente imprescindible.
En la siguiente tabla podemos ver cómo es la atenuación con la frecuencia de un cable coaxial:

Atenuaciones			
Frecuencia	200	MHz	0.09
	500		0.14
	800		0.18
	1000		0.20
	1350		0.23
	1750		0.27
	2050		0.29
	2150		
	2300		0.31

En base a lo anterior, podemos ver cómo una señal que se transmite a la frecuencia de 200 Mhz sufre menos atenuación que si la señal se transmite a la frecuencia de 800 Mhz, y a esta última frecuencia su atenuación es menor que si es a 2150 Mhz.

Lo vemos con el siguiente **ejemplo**:
Dado coaxial cuya tabla de atenuación es la mostrada a continuación, calcula qué atenuación introduce el coaxial para una señal monocromática que se transmite en la frecuencia de 1000 Mhz en un cable de 50 metros.

Solución:
Según la tabla de atenuación mostrada por el fabricante, a la frecuencia que se transmite la señal el cable introduce una atenuación de 0,195 dB/m, por lo que a 50 metros introducirá una atenuación de:
0,195 x 50 m = 9,75 Db

Atenuación / 100m	50 MHz	dB	4,4
	100 MHz		6,2
	200 MHz		8,7
	300 MHz		10,7
	470 MHz		13,4
	600 MHz		15,1
	860 MHz		18,1
	1000 MHz		19,5
	1350 MHz		22,7
	1500 MHz		23,9
	1750 MHz		25,8
	2050 MHz		27,9
	2150 MHz		28,6

Veamos ahora otro **ejemplo**.
Queremos transmitir un canal de televisión captado por una antena de UHF a través del cable coaxial de antena hasta la toma de usuario al cual conectamos un televisor convencional.
Si la señal captada por la antena es de 70 dB, calcula el nivel de señal que se recibirá en la toma de usuario a la frecuencia de 860 Mhz (frecuencia central del canal de televisión captada) si la distancia existente entre la antena y la toma de usuario es de 45 m.
Solución:
Según la tabla de atenuación del fabricante, el coaxial introduce un atenuación de 17,4 db/100 metros.
En nuestro caso al ser la distancia de 45 metros debemos ponderarlo a esta distancia, es decir:

$$\frac{17,4}{100} \times 45 \text{ m} = 7,83 \text{ dB}$$

Esta es la atenuación que introduce el cable. Como la señal captada es de 70 db, en la toma de usuario tendremos el nivel de señal captada menos la atenuación que introduce el coaxial, es decir:

$$70 \text{ dB} - 7,83 \text{ dB} = 62,17 \text{ dB}$$

Atenuación / 100m	50 MHz	dB	4,8
	100 MHz		6,4
	200 MHz		8,5
	300 MHz		9,8
	470 MHz		12,3
	600 MHz		14,5
	860 MHz		17,4
	1000 MHz		22,3
	1350 MHz		22,2
	1500 MHz		23,3
	1750 MHz		25,8
	2050 MHz		28,2
	2150 MHz		29,6

En el ejemplo anterior cambiamos el cable coaxial por uno de mejores prestaciones, es decir, por un coaxial que introduce menos atenuación en la señal.
Su tabla de atenuación con la frecuencia dada por el fabricante es:

Atenuación / 100m	50 MHz	dB	2,7
	100 MHz		3,8
	200 MHz		5,4
	300 MHz		6,6
	470 MHz		8,3
	600 MHz		10,2
	860 MHz		12,3
	1000 MHz		13,5

Calcula bajo las mismas circunstancias anteriores, el nuevo nivel de señal en la toma de usuario si empleamos este nuevo coaxial:
Solución:
En este caso el coaxial a la misma frecuencia de 860 Mhz introduce una atenuación de 12,3 db/100 m por lo que para 45 metros la atenuación introducida es de:

$$\frac{12,3}{100} \times 45 \text{ m} = 5,53 \text{ dB}$$

El nivel de señal en la toma de usuario la atenuación sobre los niveles de señal captada por la antena es de:

$$70 \text{ dB} - 5,53 \text{ dB} = 64,47 \text{ dB}$$

Es decir, como se decía en el enunciado, este coaxial es de mejores prestaciones porque el nivel de atenuación es menor y como consecuencia se obtiene mayor nivel de señal en las tomas de usuario. El inconveniente es que este coaxial es más grueso (de unos 11 mm de diámetro frente a los 6,6 mm del anterior) y por ello más difícil de instalar (menos radio de cobertura) y más caro.

3.2.3. Aplicaciones

Como ya se ha comentado anteriormente, el cable coaxial se usa sobre todo para la transmisión multimedia, es decir de audio y vídeo.

En este sentido podemos encontrarnos el cable coaxial en los siguientes entornos:

- En las instalaciones de televisión de los edificios.
- En las redes de distribución de televisión por cable de los operadores (redes CATV).
- En redes de megafonía.
- En redes de sonorización.
- En algunos equipos de radioaficionados.
- En redes de datos antiguas.

3.2.4. Ventajas e inconvenientes

El cable coaxial presenta una serie de ventajas:

- Es un cable ampliamente consolidado con buenas propiedades eléctricas para la transmisión de vídeo entre los Khz hasta los 2500 Mhz.
- Presenta buen comportamiento frente a las interferencias electromagnéticas gracias a su apantallamiento.
- Es apto para transmisiones de señal de corta y media distancia (hasta pocos centenares de metros).
- Tienen un bajo coste y en general son fáciles de instalar y mantener.

En cambio presenta una serie de desventajas que son las siguientes:

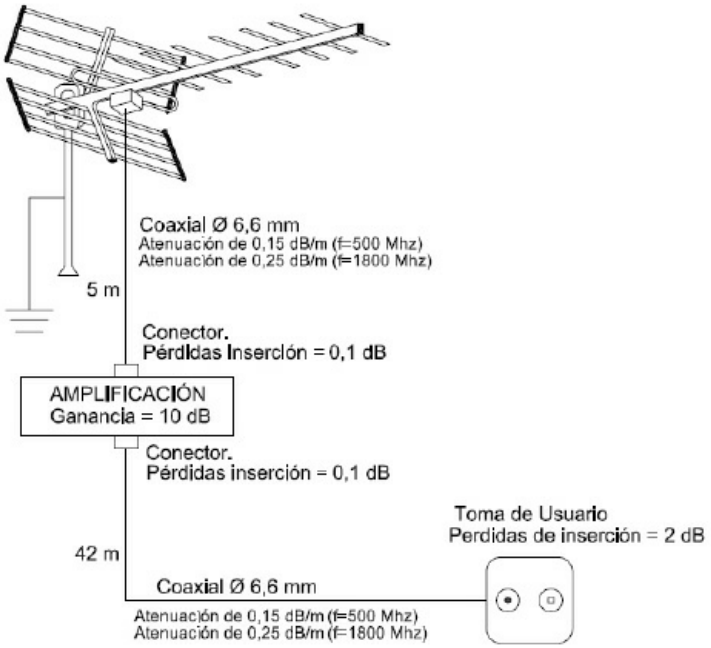
- Tiene una fuerte dependencia con la frecuencia.
- No es apto para transmisiones de largo alcance.
- No presenta una buena inmunidad frente al ruido.

Supuesto práctico:

Dada la siguiente instalación de antena donde se incluye una serie de elementos de atenuación hasta la toma de usuario, calcula en base a este esquema y a las características técnicas de cada uno de los elementos lo siguiente:

- ⇨ Atenuación introducida por todos los elementos de la instalación.
- ⇨ Nivel de señal en dB en la toma de usuario sabiendo que el nivel de señal captada es de 72 dB a la frecuencia de 500 Mhz.

Ten en cuenta que la ganancia de la antena introduce a diferencia de la atenuación un valor positivo en el valor de la señal. Las pérdidas de inserción son equivalentes a introducción de atenuación en la señal.



Solución:

- ⇨ La atenuación introducida por todos los elementos serán las pérdidas del coaxial, de los conectores y de las pérdidas de inserción de la toma de usuario, es decir, la atenuación de la instalación será la suma de todas ellas.
  Atenuación total = 2 x Perdidas conectores + Atenuación coaxial antena-amplificador + Atenuación coaxial amplificador-toma usario + Perdidas toma usuario =
  2 x 0,1 dB + 5 metros x 0,15 dB/m + 42 metros x 0,15 dB/ m + 2 dB = **9,25 dB**
- ⇨ El nivel de señal en la toma de usuario será el nivel de señal captada menos la atenuación introducida por la instalación más la ganancia que pueda introducir la instalación en este caso del amplificador. Así obtenemos:
  Nivel señal obtenida = Nivel captada – Atenuación sistema + Ganancia sistema =
  72 dB -9, 25 dB + 10 dB = 72,75 dB

Podemos observar que **la ganancia del amplificador compensa las atenuaciones introducidas por el sistema por el coaxial, conectores y toma de usuario**.

3.3. La fibra óptica

La fibra óptica es otro de los medios de transmisión guiados más habitualmente utilizado (sobre todo en los últimos tiempos) para la transmisión de datos a alta velocidad y/o largas distancias.

Videos de Introducción a la fibra óptica: https://youtu.be/zZ7ay-j6ZQQ https://youtu.be/BxDM0MpZGBI

Su baja atenuación y su inmunidad a las interferencias electromagnéticas (transmite impulsos ópticos y no eléctricos) lo hace ideal para la transmisión de datos en entornos de operadores y grandes empresas. Aunque inicialmente su coste era mayor, ya es plenamente competitivo con los medios de transmisión anteriormente descritos (coaxial y par trenzado) ya que además es un cable ligero y de fácil instalación.

A continuación veremos sus propiedades constructivas y de transmisión.

3.3.1. El sistema de transmisión óptico

La fibra óptica es un cable formado por uno o más hilos de fibra de vidrio por la cual viaja un haz de luz.
La fibra óptica está basada en el principio de la transmisión óptica.
Este principio se fundamenta en confinar una señal de luz dentro un hilo conductor de vidrio (núcleo) utilizando para ello una capa exterior que refleja la luz transmitida haciendo que ésta permanezca confinada dentro del núcleo. Esto es lo que se conoce como Ley de Snell donde en ella se relacionan los ángulos de ángulos de refracción de la luz en un cambio de medio con los índices de refracción de cada medio.
Esta Ley de Snell establece que:

$$n_1 \text{ x seno } (Ø_1) = n_2 \text{ x seno } (Ø_2)$$

siendo n_1 y n_2 los índices de refracción de los medios de transmisión: núcleo y cubierta respectivamente.
Durante el proceso de fabricación de la fibra, éstas son recubiertas con una protección de 250 µm, que cubre el conjunto de núcleo y cubierta.
Esta protección garantiza una indeformabilidad y dureza mínima para su uso en sistemas de transmisiones.

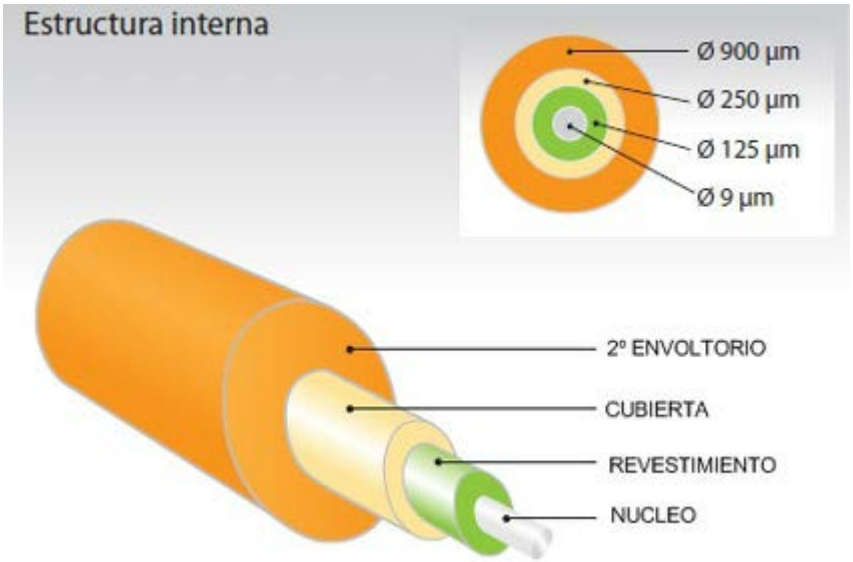
Sobre esta protección se aplica además un recubrimiento que puede ser dos tipos:

- Fibras de tubos sueltos:
  Este tipo de fibra se utiliza sobre todo para instalaciones de exterior, ya que el cable se expone a cambios de temperatura donde el recubrimiento permite cierta holgura en el caso de dilatación.
- Fibra de recubrimiento ajustado:
  Este tipo de fibra se utiliza en entorno de interiores. En este caso la fibra queda totalmente recubierta por una protección plástica de 900 µm. Es por tanto más sensible a los cambios de temperatura ya que no permite dilatación de sus componentes sin que afecte a sus propiedades de transmisión.

3.3.2. Características constructivas

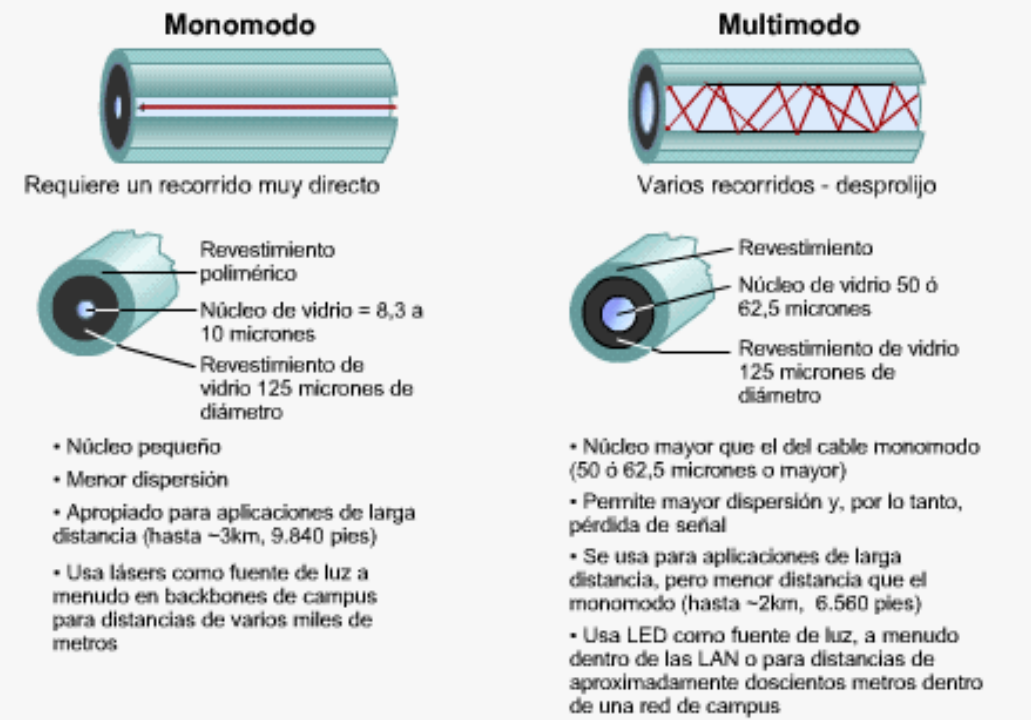
La fibra óptica es una composición de uno o más hilos de vidrio formando una estructura como lo siguiente:

- Un núcleo central de fibra (hilo de vidrio) con un alto índice de refracción.
- Una cubierta que recubre el núcleo de material similar pero con un índice de refracción menor.
- Una envoltura que aísla las fibras y evita que se produzcan interferencias entre ellas además de dar protección al núcleo.



La fibra sólo transmite luz porque la información debe ser convertida en haces de luces (mediante dispositivos emisores tipo Led o Láser y receptores ópticos en sus extremos).
Uno de los parámetros básicos en la fibra óptica es la relación o ratio existente entre los índices de refracción de núcleo y cubierta, dando lugar a dos tipos de fibra:

- Fibra **monomodo**:
  Este tipo de fibra es aquel en que la relación de los índices de refracción de núcleo y cubierta sólo permiten la transmisión de un único modo de transmisión. De ahí su nombre de monomodo.
  Un modo se puede interpretar como un único canal de transmisión. En este caso se consigue un alto rendimiento al no haber interferencias intermodales alcanzándose grandes ancho de banda de alrededor de 50 y 100 Ghz.
- Fibra **multimodo**:
  Este tipo de fibra es aquel en que la relación de los índices de refracción de núcleo y cubierta permiten la transmisión de varios modos de transmisión. De ahí su nombre de multimodo
  La propagación de varios modos de transmisión hace que aparezca dispersión intermodal que se traduce en un peor rendimiento de la transmisión y como consecuencia en menor velocidad de transmisión que alcanza el 1 Ghz.
  Dentro de las fibras multimodo existe de dos tipos: de salto de índice y de índice gradual.



3.3.3. Características de transmisión

La fibra presenta una serie de características que la hacen ideal para la transmisión de datos a altas velocidades.

Estas características principalmente son:

- Presenta un gran ancho de banda (alrededor de los 50 y 100 Gps) para voz, datos, vídeo, etc.
- Presenta una muy baja atenuación con la distancia (0.1 dB/km). Ideal para largas distancias
- Una tasa de error BER < 10-11 por lo que la velocidad de transferencia que se puede obtener es muy alta.
- Inmune a las interferencias electromagnéticas. Transmite haces de luz y no impulsos eléctricos.
- Resistente a la corrosión y buen comportamiento a la temperatura.

Estas propiedades son comunes a los diferentes tipos de fibra existente (monomodo y multimodo) aunque como ya se ha comentado anteriormente, en el caso de monomodo el ancho de banda que se alcanza es mayor que en multimodo.

3.3.4. Aplicaciones. Utilización de frecuencias

La fibra óptica presenta una serie de formatos comerciales donde cada uno de ellos tiene unas características singulares que los hacen apropiados para una aplicación u otra.

Estos formatos comerciales son las siguientes:

Tipo de fibra óptica	Denominación comercial	Diámetro núcleo/cubierta	Distancia máxima Aplicaciones Gbps
Multimodo	OM1	62,5 / 125 µm	32 m
	OM2	50 / 125 µm	85 m
	OM3	50 / 125 µm	300 m
	OM4	50 / 125 µm	550 m
Monomodo	OS1	50 / 125 µm	2 km
	OS2	50 / 125 µm	10 km

En la práctica los formatos normalizados OM1 y OM2 están en desuso por lo que ya sólo se utilizan los formatos OM3 y OM4 para la gran mayoría de instalaciones y los formatos OS1 y OS2 para largas distancias.

Veamos un **ejemplo** de transmisión con fibra óptica.
Disponemos de un enlace con fibra óptica entre dos equipos A y B para la transmisión de datos.
Si la distancia que separa entre los dos equipos es de 2, 5 km y lo conectamos con una fibra monomodo que trabaja en la ventana de los 1300 nm y con una atenuación de 3,5 dB/km, calcula la atenuación que introduce el sistema de transmisión.

Solución:
Tal y como nos dice el enunciado la fibra introduce una atenuación de 3,5 dB/km en la ventana de trabajo.
Como la distancia que separa ambos equipos es de 2,5 km, luego la atenuación que introduce el sistema en esa distancia será de:
Atenuación del cable = 3,5 dB/ km x 2, 5 km = 8,75 dB.

Pongamos otro **ejemplo**.
Supongamos que disponemos de un enlace mediante fibra óptica entre dos estudios de grabación de televisión que están separados 10 km.
El esquema del enlace es el siguiente:

Las características de los elementos que componen el sistema de transmisión son las siguientes:

Fibra óptica	Monomodo 50/125 µm con 3,5 dB/km de atenuación
Conectores ST	Pérdida de inserción de 0,5 dB
Empalmes de la fibra	Pérdidas de conexión de 0,1 dB.

Calcula la atenuación que introduce el sistema de transmisión.
Solución:
En este caso el sistema introduce varias atenuaciones:

- Atenuación por el cable.
- Atenuación en los dos conectores.
- Atenuación por los empalmes de la fibra

Calculamos la atenuación que introduce cada uno de ellos:
Atenuación cable = 3,5 dB / km x 10 km = 35 dB.
Atenuación conectores = 2 x 0,5 dB = 1, 0 dB.
Atenuación empalmes = 2 x 0,1 dB = 0,2 dB.
La atenuación total del sistema será la suma de todas las atenuaciones anteriores:
Atenuación total = Atenuación cable + Atenuación conectores + Atenuación empalmes =
35 dB + 1,0 dB + 0,2 dB = 36,2 dB.

3.3.5. Tipos de empalmes. Ventajas e inconvenientes

En la fibra se emplean diferentes tipos de empalmes siendo los más comúnmente utilizados los siguientes:

- **FC**: empleado para fibras de largo alcance.
- **FDDI**: empleado para conexiones de medio y largo alcance.
- **LC**: es el más adecuado para transmisión de datos a altas velocidades.
- **SC**: es el más utilizado para transmisión de datos de gama media.
- **ST**: ampliamente utilizado para sistemas de seguridad.

De entre todos ellos los formatos SC y LC son los más ampliamente estandarizados.

Para transmitir señales luminosas a través de fibras ópticas se requiere en su inicio un elemento emisor que convierta las señales eléctricas en ópticas (E/O) y otro en su final que convierta las señales ópticas en eléctricas nuevamente (O/E).

Los conversores electro-ópticos se fabrican con base en la combinación de los elementos de los siguientes elementos: el Indio (In), Gálio (Ga), el Germanio (Ge), el Silicio (Si), el Arsénico (As), el Fósforo (P), que han demostrado ser los más aptos para la fabricación de estos dispositivos.

La tecnología de los semiconductores posibilitó construir emisores y detectores de luz de pequeñas dimensiones y bajo coste.

Existen dos opciones de fuentes semiconductoras para ser utilizadas en fibras ópticas como emisores de luz:

- Diodos LED.
  Es un diodo de material semiconductor que forma una unión P-N de las mismas características que un diodo convencional de germanio o silicio.
  La diferencia principal con los diodos convencionales radica en que ciertos materiales que se utilizan como dopadores en el LED son elegidos de tal manera que el proceso de recombinación electrónica sea radiactivo y se genere luz.
  En función del material usado en su fabricación se diodo LED emitirá luz visible u otro color.
  Debido a la gran dispersión de luz y a la distribución espectral tan amplia que presenta un diodo LED, es usado sólo cuando se requiere realizar transmisiones a distancias cortas y con poca salida de potencia. Son relativamente baratos y poseen un tiempo de vida útil muy largo (107 horas).
- Diodo Láser:
  El LÁSER es básicamente un diodo semiconductor que cuando se polariza directamente emite una luz coherente, monocromática y muy estrecha en su ancho espectral, de 1 a 5 mm.

Esta luz debido a su espectro tan estrecho, no se dispersa tanto como la luz producida por diodo LED, por lo que se puede emplear eficientemente para transmisiones a mucha distancia y a frecuencias muy superiores a los 300 Mhz.
Es un dispositivo más caro que el diodo LED pero se emplea para transmisiones a largas distancias, aunque hoy día con su amplia difusión y por cuestiones de economía de escala su precio es ya competitivo con el diodo LED.

Para la recepción de señales ópticas y su conversión a señales eléctricas se usan dispositivos receptores ópticos que pueden ser de dos tipos:

- Fototransistores:
  Son receptores que poseen buena sensibilidad pero no son aptos para altas tasas de velocidad.
- Fotodiodos:
  Son diodos semiconductores pero polarizados inversamente con lo cual actúan como conversores ópticos a eléctricos.
  Son dispositivos de baja latencia, muy rápidos, alta sensibilidad y que lo hacen muy adecuados para transmisiones de alta velocidad.
  Se clasifican a su vez en dos tipos:
  - Fotodiodo pin.
  - Fotodiodo APD.

3.4. Catálogos de medios de transmisión

A continuación, veremos las hojas de características técnicas (Datasheet) proporcionados por los fabricantes de los medios de transmisión vistos anteriormente, es decir, del par trenzado, del cable coaxial y de la fibra óptica.
Como se ha descrito anteriormente, las características constructivas y de transmisión de cada uno de ellos son diferentes, y en función de ello, lo hacen adecuado a la transmisión de un tipo u otro de servicio de telecomunicaciones.
Aun así, dentro de los pares trenzados, del cable coaxial o de la fibra óptica, existen diferentes implementaciones comerciales que afectan a sus características de transmisión y que veremos en detalle a continuación.

Par trenzado:

Dentro de los pares trenzados que hemos visto, existen tres tipos en función del apantallamiento que presentan:

- UTP: no incorpora apantallamiento entre los pares.
- STP: incorpora apantallamiento por cada par de cobre.
- FTP: incorpora apantallamiento por cada par de cobre y un apantallamiento global al par trenzado.

Además de esta clasificación, los pares trenzados pueden ser de diferentes categorías: Cat5, Cat5a, Cat6, Cat6a, Cat7, Cat7a y Cat8 (hemos nombrado los que aún se siguen empleando en la actualidad y no han quedado obsoletos).
Existen en el mercado numerosos fabricantes que fabrican pares trenzados, destacando principalmente Systimax, Ortronics, Nordix, entre otros.

A continuación, veremos algunos de los modelos comerciales de cada uno de estos fabricantes de pares trenzados.

- Modelo Clarity6A shielded modular patch cord 25', gray de Ortronics:
  En la siguiente imagen podemos ver una imagen del par trenzado y la hoja de especificaciones (datasheet) del fabricante.

Connectorized Info
Jacket Color: Gray
Pinning: Straight 1-1, 2-2, 3-3, etc.
Min Bend Radius: 1.00"
Connector Type End One: Shielded Plug, HSC, eight-contact, RJ45, high performance
Jacket Rating: CM
Cord Length U.S.: 25'
Connector Type End Two: Shielded Plug, HSC, eight-contact, RJ45, high performance

Dimension Info
Diameter Metric: 6.1 mm
Length Metric: 7.62 m
Diameter U.S.: 0.24"

General Info
Product Series: Clarity
Type: Patch Cords and Cables
Cable Type: Four pair
Color Cable Jacket: Gray
Termination: 8-Pos Mod
Typical Applications: IEEE 802.3 10GBase-T, 1000Base-T (Gigabit Ethernet), TIA/EIA-854 1000Base-TX, ATM OC31G

Technical Info
Wire Gauge: 25 AWG
Ohm Value: 100 Ohm
Category Rating: Cat6a
Performance Rating: Cat6a

Listing Agency Info
ETL
FCC

Analizando sus características podemos resaltar lo siguiente:

- Se trata de un par trenzado de 4 pares FTP categoría 6a muy apto también como cable para redes de datos de alta velocidad (Gigabit Ethernet y 10G-BaseT).
- El cable al presentar apantallamiento (FTP) debe emplear conectores en sus extremos adaptados para la conexión a la toma de tierra.
- El diámetro del cable es de 6,1 mm, algo habitual para este tipo de par trenzado.
- Presenta un valor óhmico de 100 Ohmios.
- Está preconectorizado, es decir, incorpora de fábrica los conectores en sus extremos RJ-45 ya conectados. Esto es muy habitual para agilizar y facilitar las tareas de instalación.

Este modelo se podría emplear también como latiguillos de conexión.

Cable coaxial:

El cable coaxial, como se ha visto, es un cable ampliamente utilizado en la transmisión de audio y vídeo.
Un característica esencial de su comportamiento de transmisión es su dependencia con la frecuencia, es decir, su atenuación depende de la frecuencia.
Con objeto de mejorar sus prestaciones, es decir, de ofrecer una menor atenuación con la frecuencia (y con ello la distancia) se fabrican cables coaxiales con un grosor mayor.
En base a esto podemos encontrar:

- Cables coaxiales finos: son los que presentan un diámetro alrededor de los Ø6-7 mm.
- Cables coaxiales gruesos: son los que presentan un diámetro mayor de Ø10mm. Son los denominados coaxiales de bajas pérdidas.

El motivo de emplear uno u otro, es en función de la distancia que deba cubrir. Para distancias cortas se emplea cable coaxial fino ya que es más barato, más ligero y más fácil de instalar (tiene un mejor radio de curvatura).
Para distancias largas (donde se prevé gran atenuación) se emplean cables coaxiales gruesos para cumplir con los niveles de señal exigidos en los extremos, aunque su instalación sea más cara y menos fácil.
Existe en el mercado una amplia gama de coaxiales de diferentes fabricantes destacando entre otros Televés, Alcad, Ikusi, Fagor, etc.
Cada uno de ellos ofrece diferentes tipos de coaxiales (finos y gruesos) para que puedan ser elegidos en función de la configuración de red que se quiera instalar.

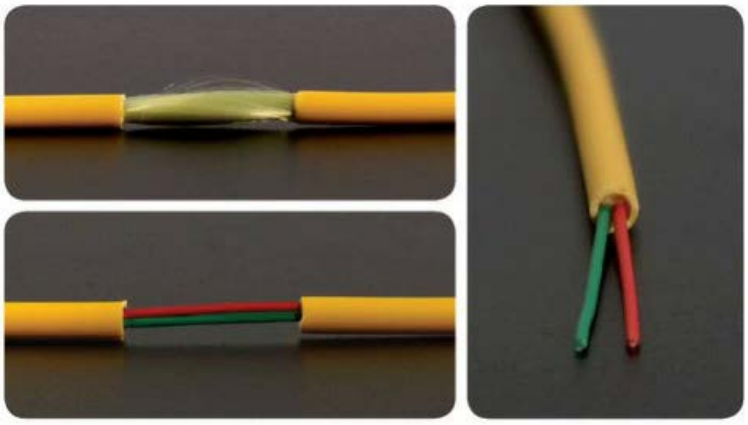
Fibra óptica:

La fibra óptica es un medio de transmisión guiado cada vez más usado en las redes de telecomunicaciones debido a sus grandes prestaciones.
A diferencia del coaxial y del par trenzado que están basados en conductores de cobre, la fibra se basa en hilos de vidrio por lo que emite luz óptica y no impulsos eléctricos.
Esto le permite obtener una muy baja atenuación (alrededor de los 0,3 db/km lo que lo hace muy apropiado para transmisiones de larga distancia), tener un buen ancho de banda (tasas de transferencias de Gigabit Ethernet) y ser inmune a las interferencias electromagnéticas.
La fibra óptica puede ser de dos tipos:

- Fibra óptica monomodo:
  Es aquella en la que sólo se transmite un modo y con ello se obtiene muy baja atenuación. Se emplea para enlaces de larga distancias (del orden de kilómetros).
- Fibra óptica multimodo:
  Es aquella en la que se transmiten varios modos y con ello la atenuación es mayor que la fibra óptica monomodo. Se emplea para instalaciones de interior.

Por sus ventajas, la fibra óptica va poco a poco reemplazando los medios de transmisión ya instalados, ya que con este cable se pueden soportar altas tasas de transferencia y que son exigidos por determinados servicios de telecomunicaciones como televisión por internet (IPTV), vídeo bajo demanda (VoD), etc.
Otra de las ventajas de este cable es su bajo peso y facilidad de instalación. No obstante presenta como inconveniente que esta instalación es más cara que los otros cables, aunque cada vez está siendo más competitivo.
Un tema importante en la fibra son los conectores. Existe una amplia tipología de conectores en el mercado aunque solo algunos de ellos están ampliamente implantados como son el conector LC o el SC entre otros.
Existen en el mercado numerosos fabricantes de fibra óptica (muchos de ellos son los mismos que los de par trenzado) entre los que destaca Systimax, Ortronic, Televés, Nordix, etc.
Vemos algunos ejemplos comerciales de fibra óptica de estos fabricantes.

- Modelo Bifibra interior LSZH de Televés:
  A continuación podemos ver una imagen de esta fibra óptica junto con la hoja de especificaciones del fabricante.

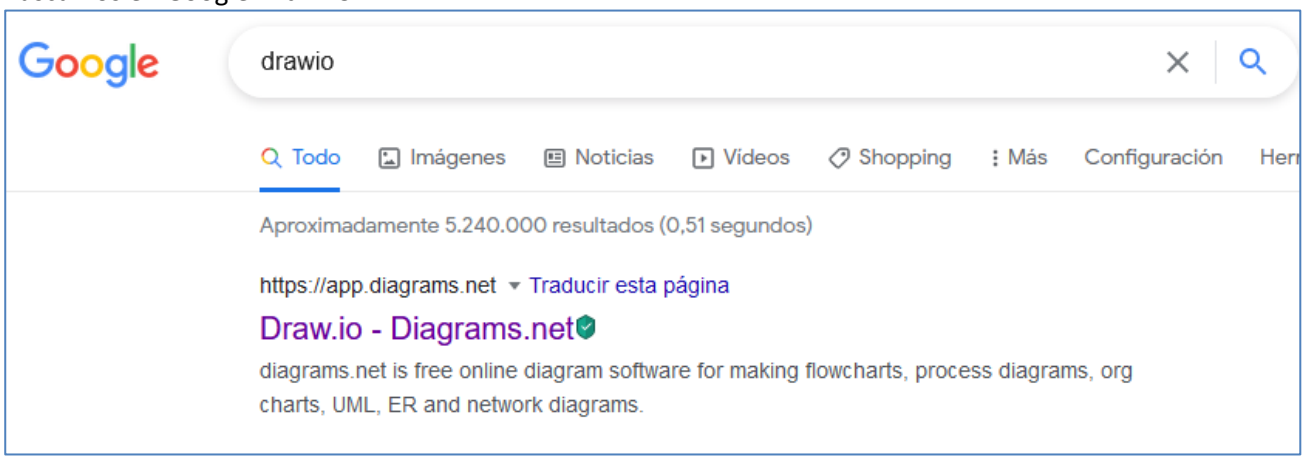


Analizando sus características podemos resaltar lo siguiente:

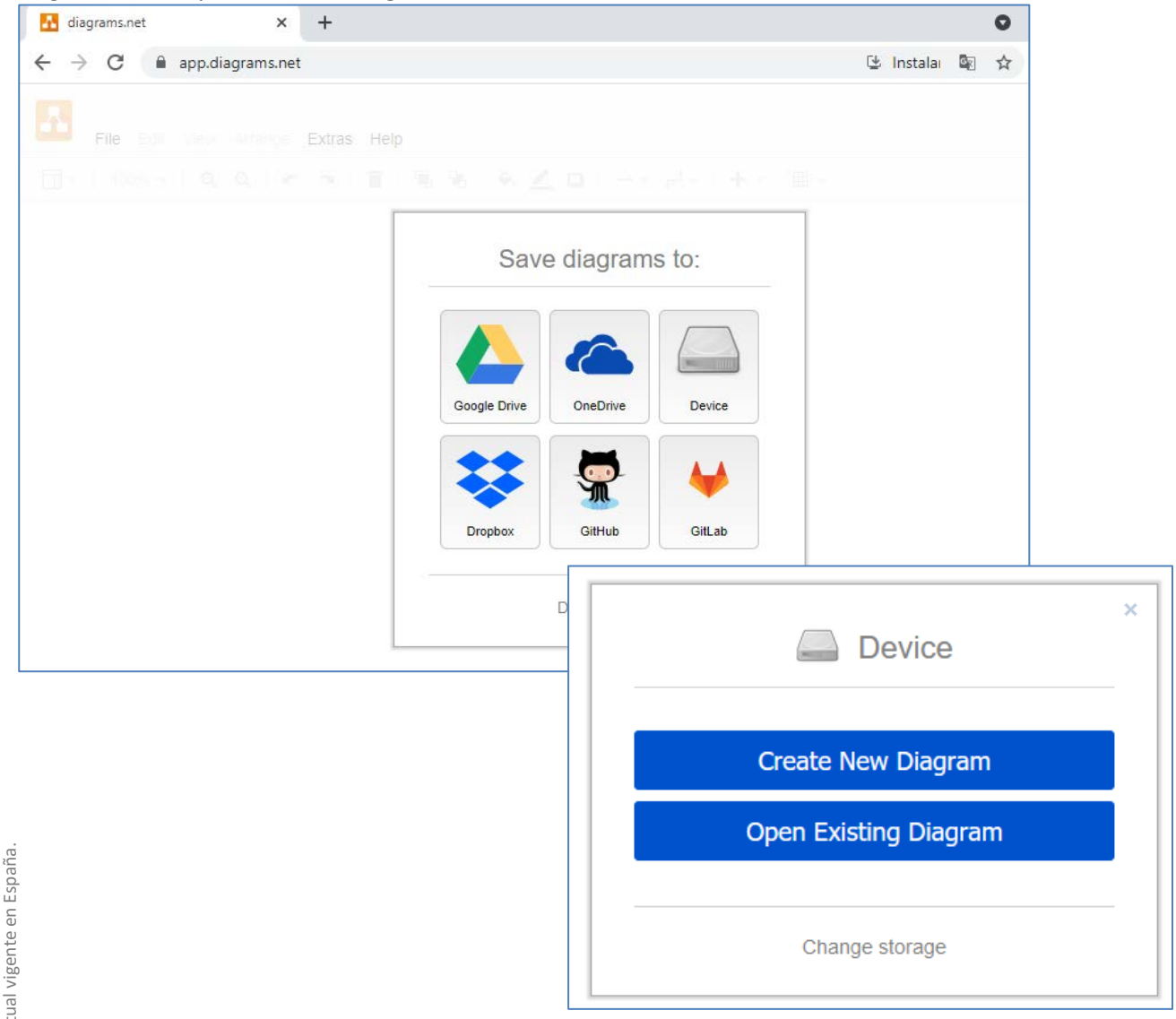
- Se trata de una fibra óptica de 2 fibras (bifibra) apto para acometidas individuales.
- El tipo de fibra es de 9/125 µm y trabaja en las ventanas de 1310 y 1550 nm.
- Presenta una atenuación de 0,4 dB/km en la ventana de ls 1310 nm y de 0,3 dB/km en la ventana de los 1550 nm.
- Su cubierta está realizada con material LSZH, es decir, de baja emisión de humos.
- Se suministra en carretes de 300 m.

Crear Diagramas de Red con Draw.io

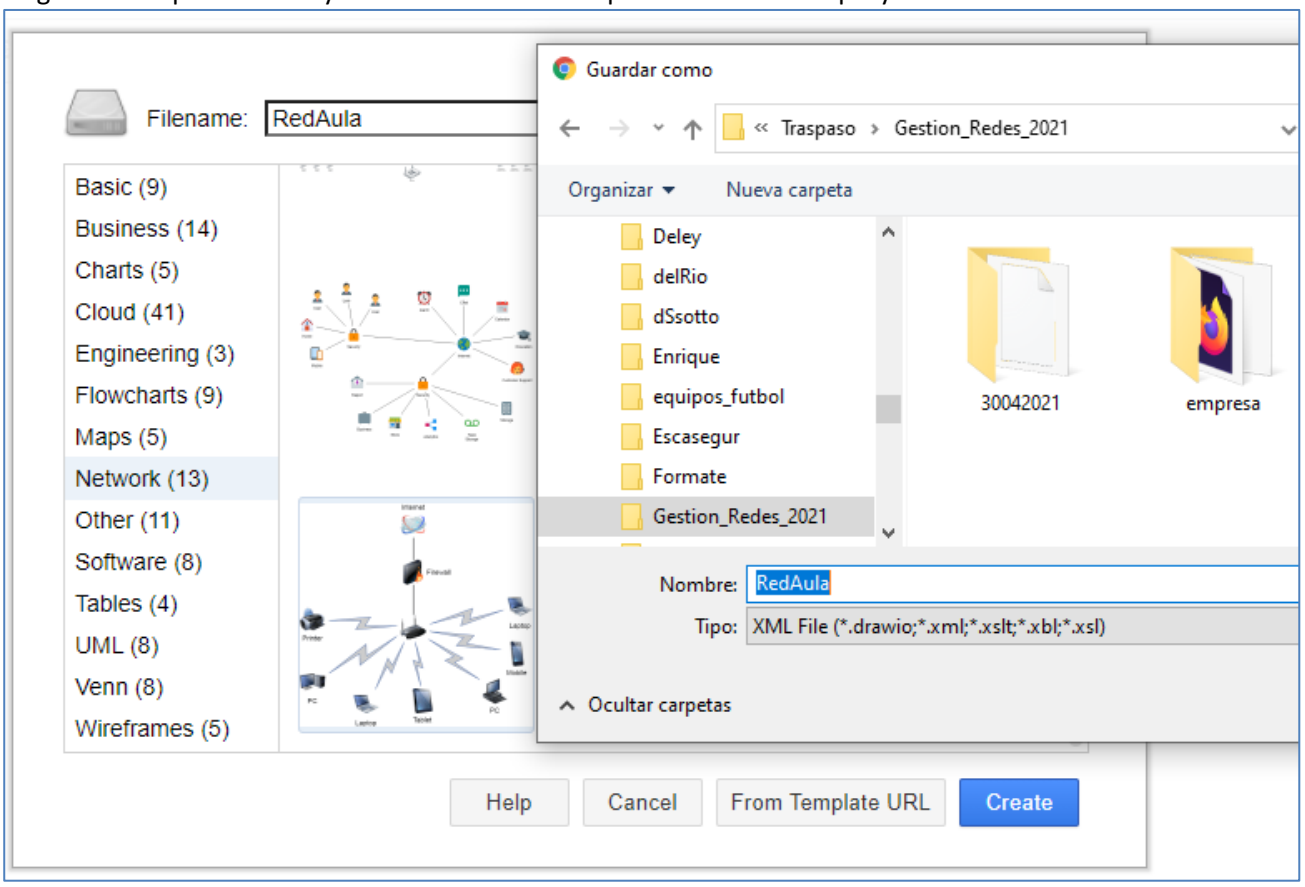
Buscamos en Google **Draw.io**



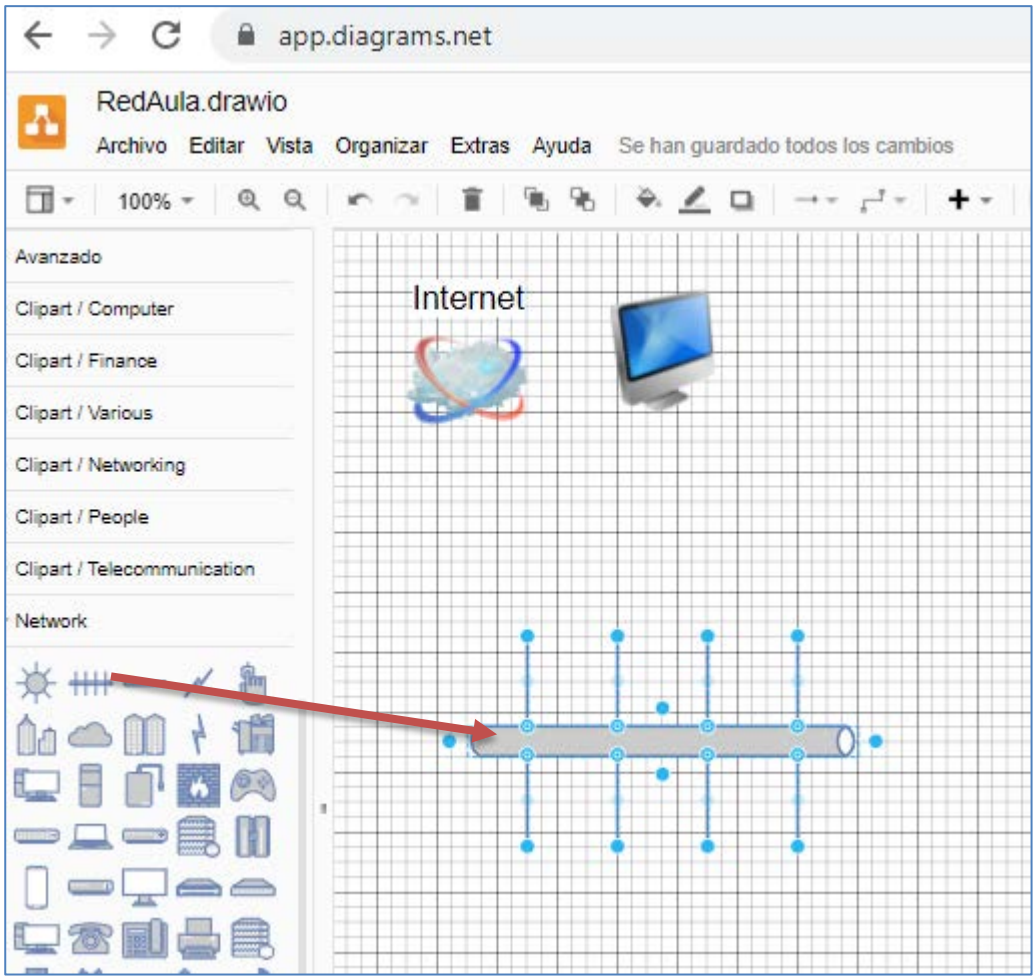
Elegimos **Device** y **Create New Diagram**



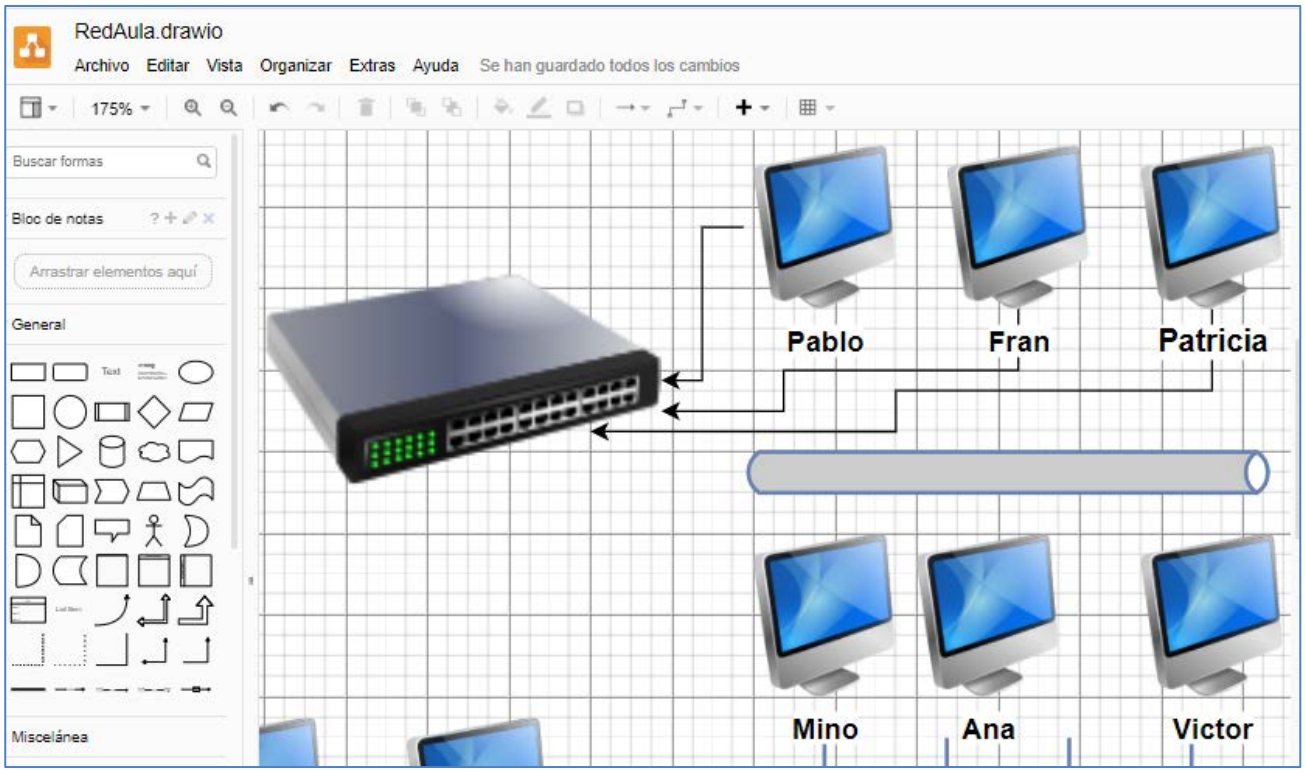
Elegimos de Tipo **Network** y seleccionamos el más parecido a nuestro proyecto:



Borramos todos los elementos menos internet y sin es la primera vez que entramos cambiamos el idioma haciendo clic en la bola del mundo de la parte superior derecha

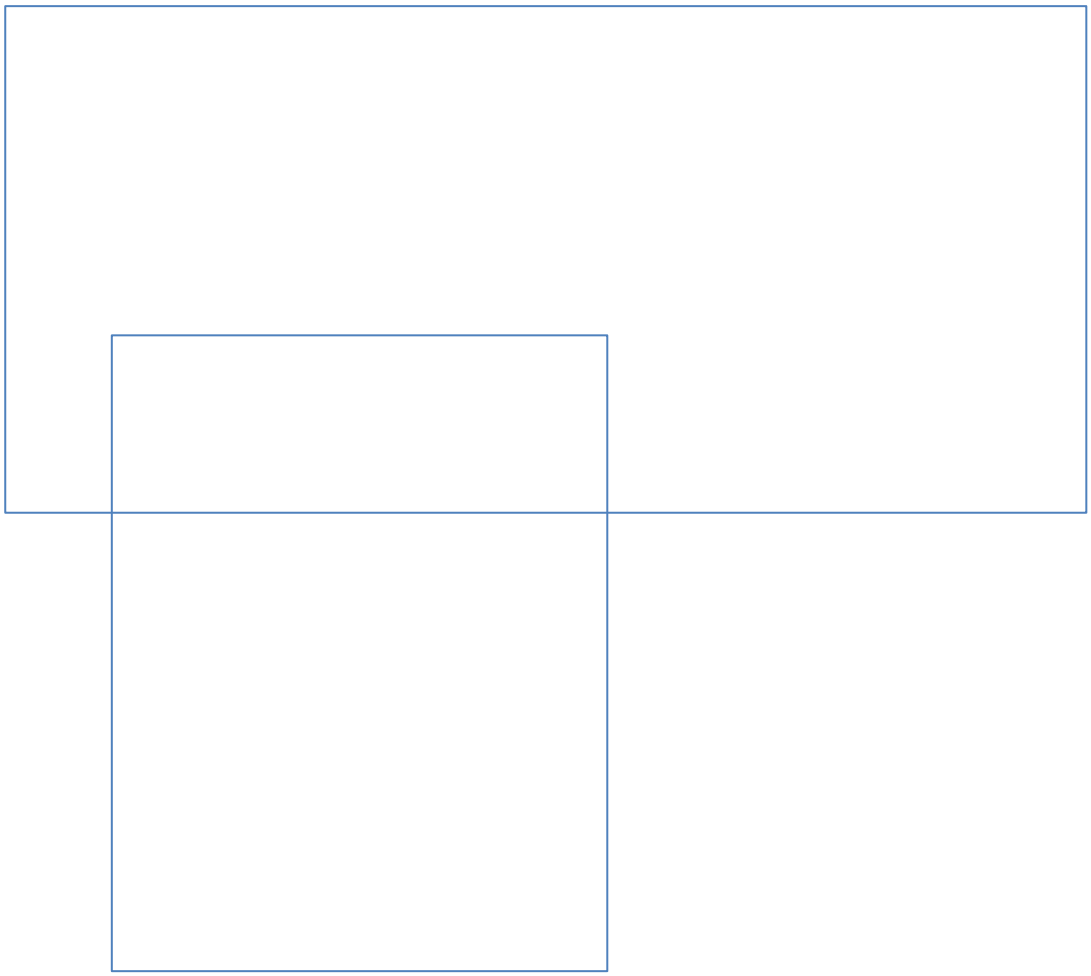


Identificamos cada ordenador



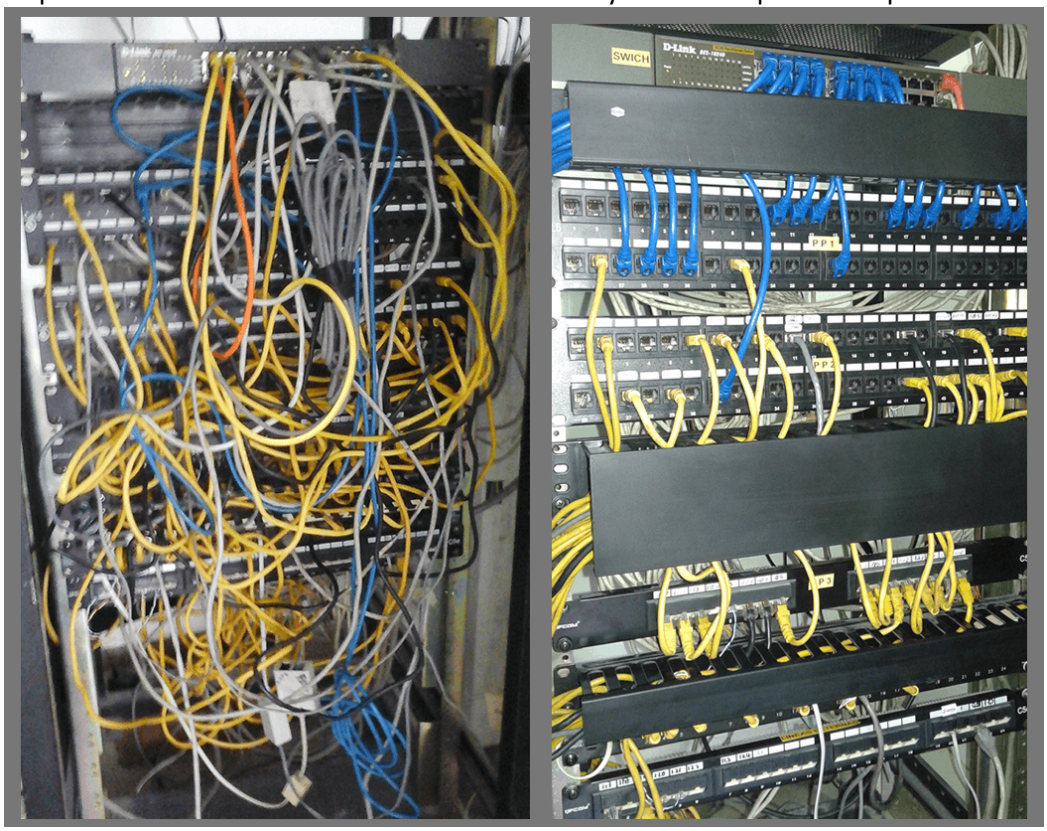
Teclas rápidas: Barra espaciadora clic movéis el dibujo completo y Alt mas rueda para el zoom

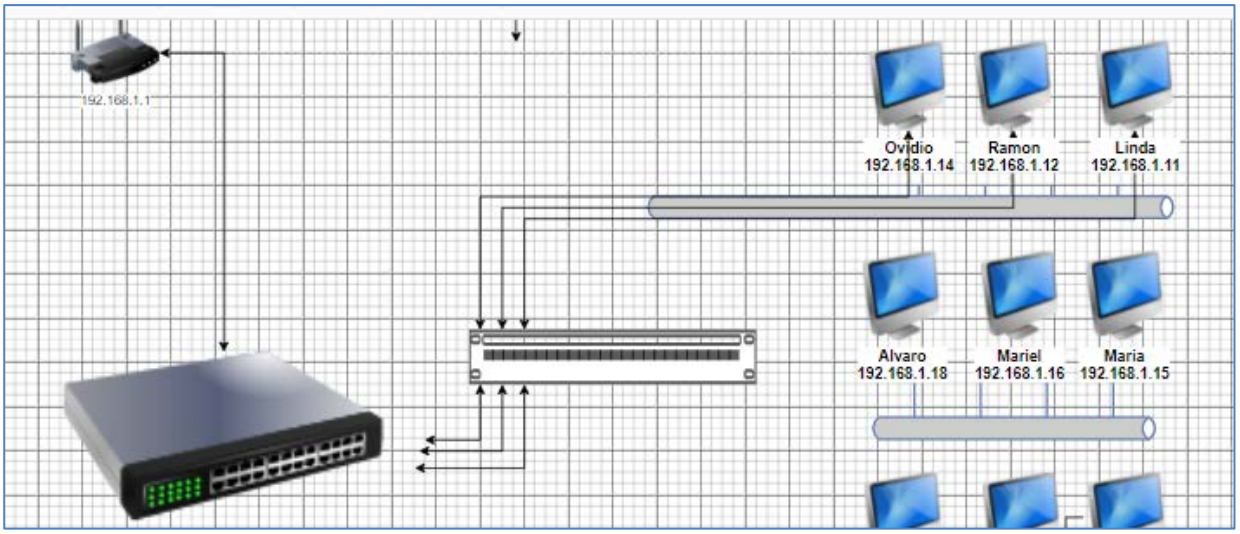
Vamos a poner una IP Fija, para lo que buscamos en Windows **red** y seleccionamos **Ver conexiones de red**



Le ponemos la IP y las DNS del router y de Google

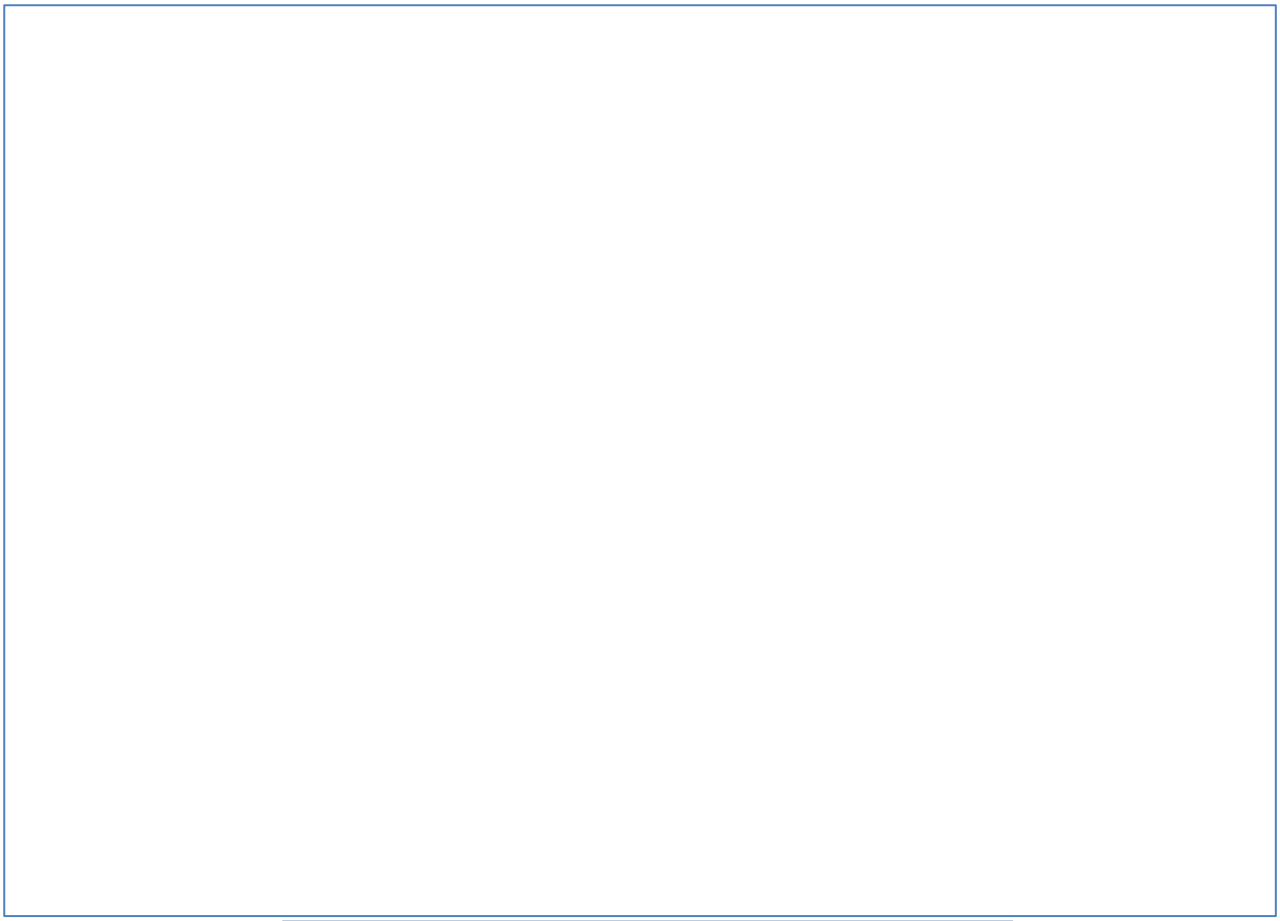
Esquema de red usando el Armario de conexiones y los cables que vienen por cada canaleta.

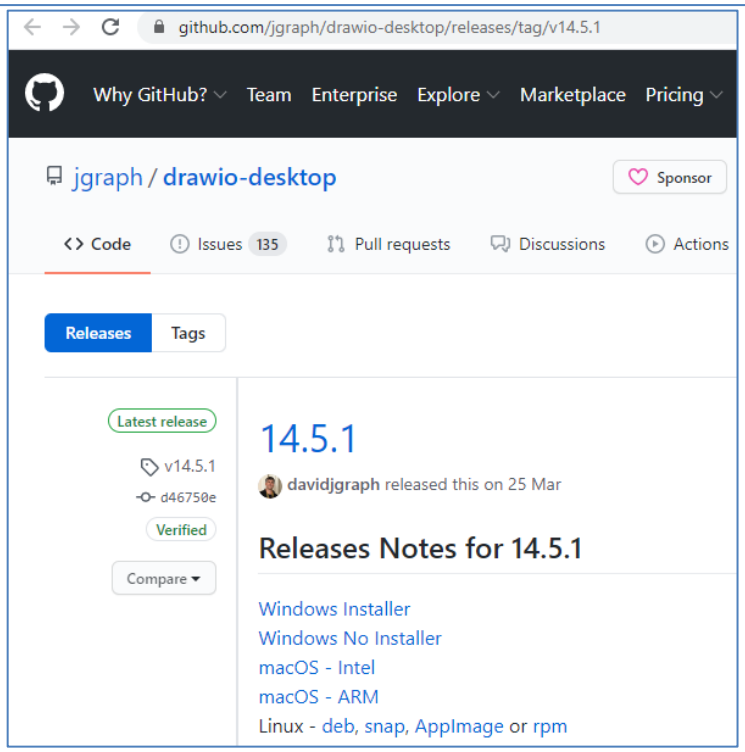




Descargar la versión de escritorio de drawio

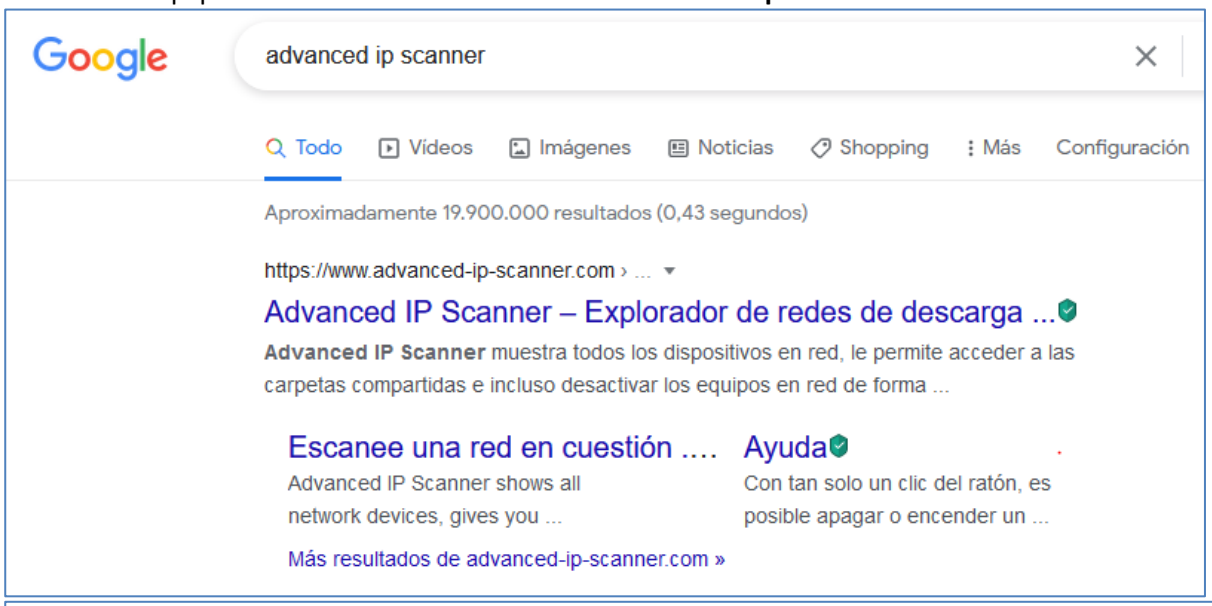
Podemos hacerlo desde este enlace https://github.com/jgraph/drawio-desktop/releases/tag/v14.5.1
O cuando abrimos un nuevo diagrama desde la web https://app.diagrams.net/ pulsamos sobre Ayuda/Obtener versión de escritorio o pulsando en el enlace publicitario que nos aparece en la parte inferior:

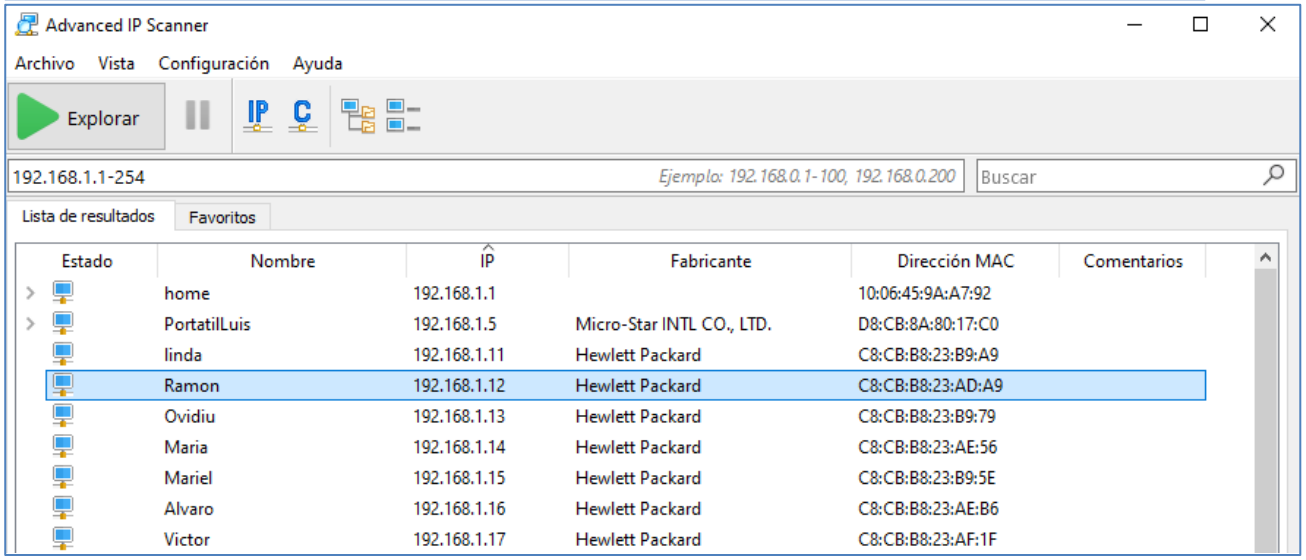




Escanear los equipos de una red:

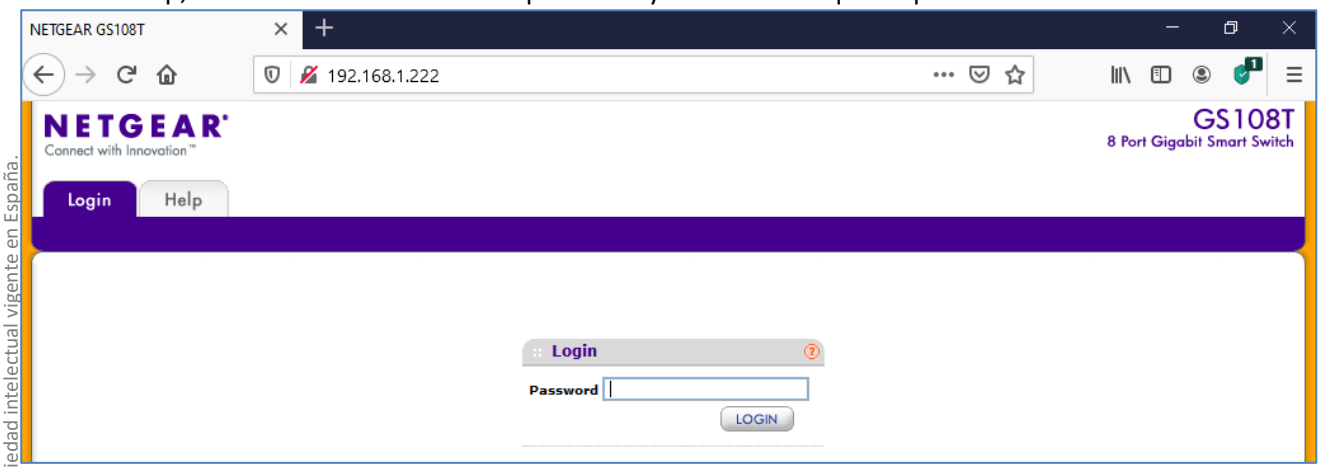
Para ver los equipos conectados a una red usaremos **advanced ip scanner**:



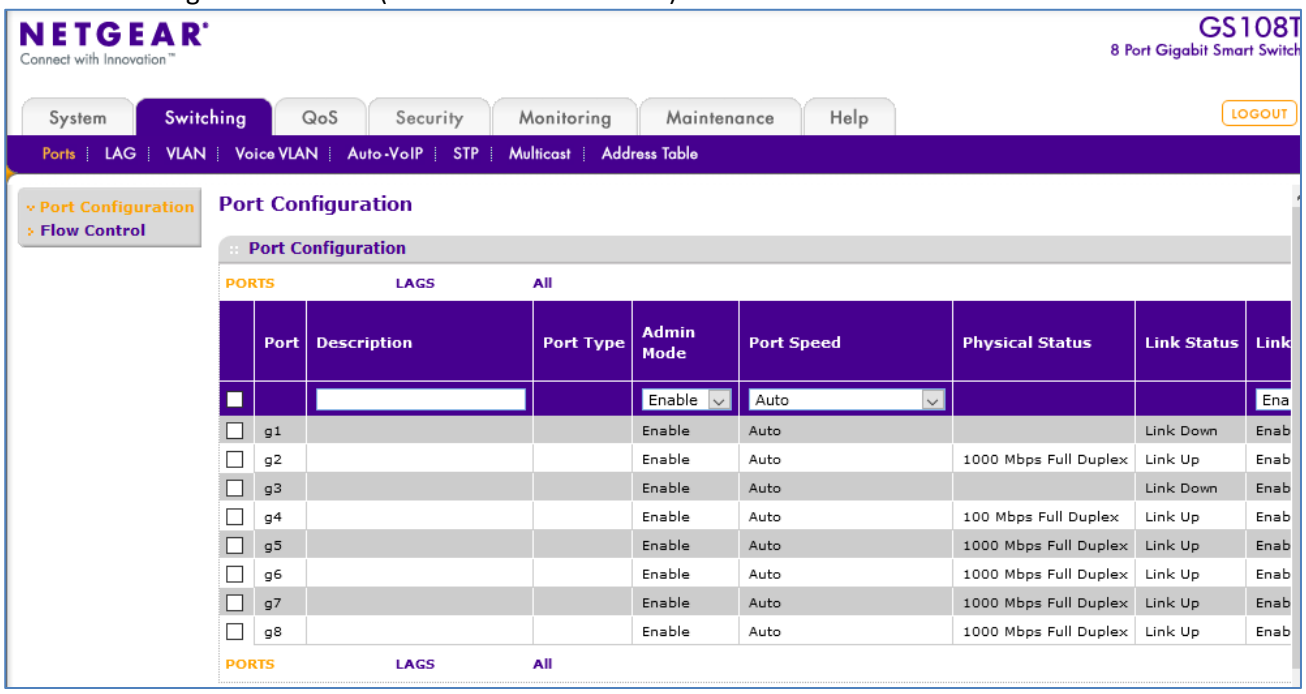


Crear varias VLAN (Virtual LAN) usando un switch gestionable

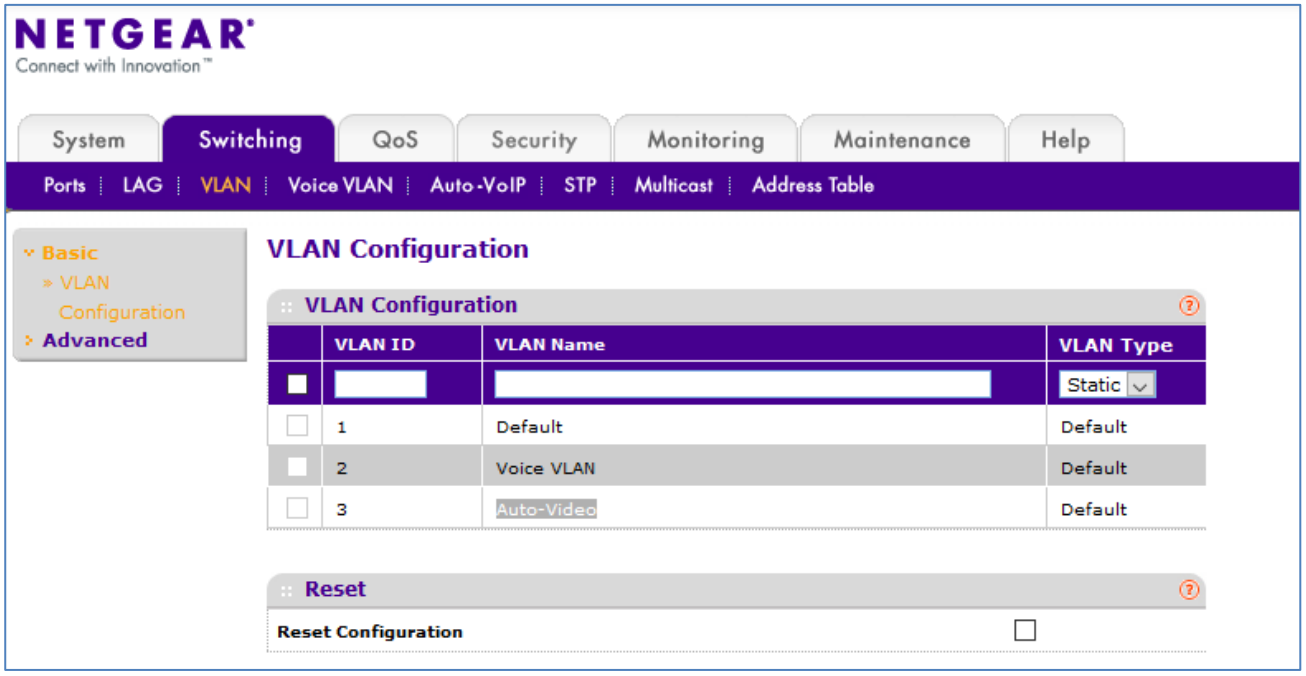
Usaremos un switch gestionable modelo GS108T. Tenemos que acceder a la ip del switch y como no sabemos la ip, escaneamos con advanced ip scanner y descubrimos que la ip es 192.168.1.222



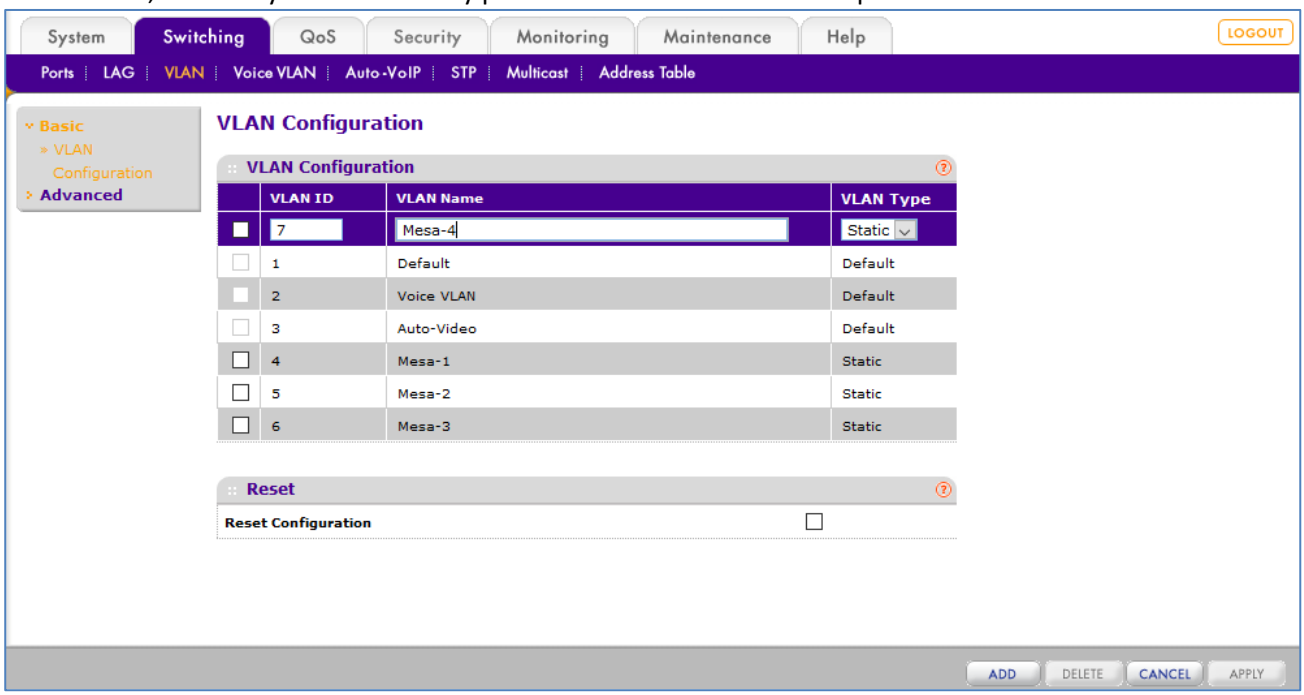
Ponemos el password que por defecto es **password**
Ahora vamos a generar 4 VLAN (red de área local virtual)



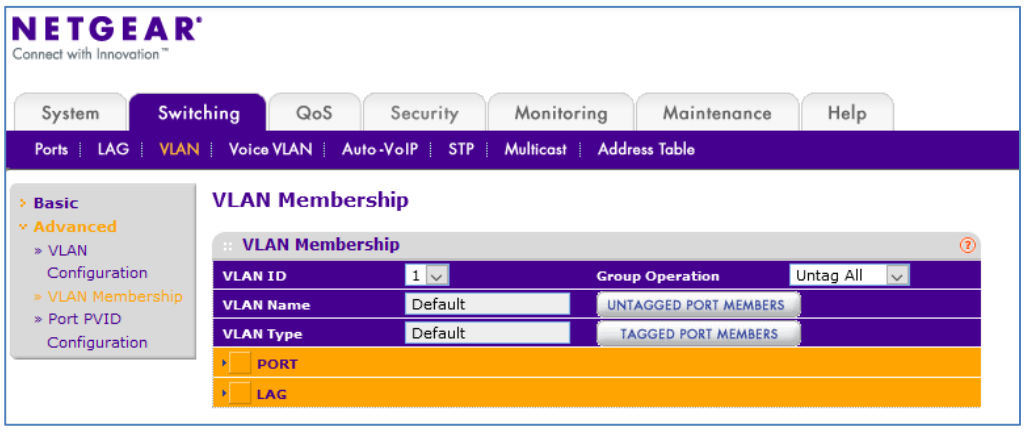
Pulsamos sobre Switching y luego sobre VLAN



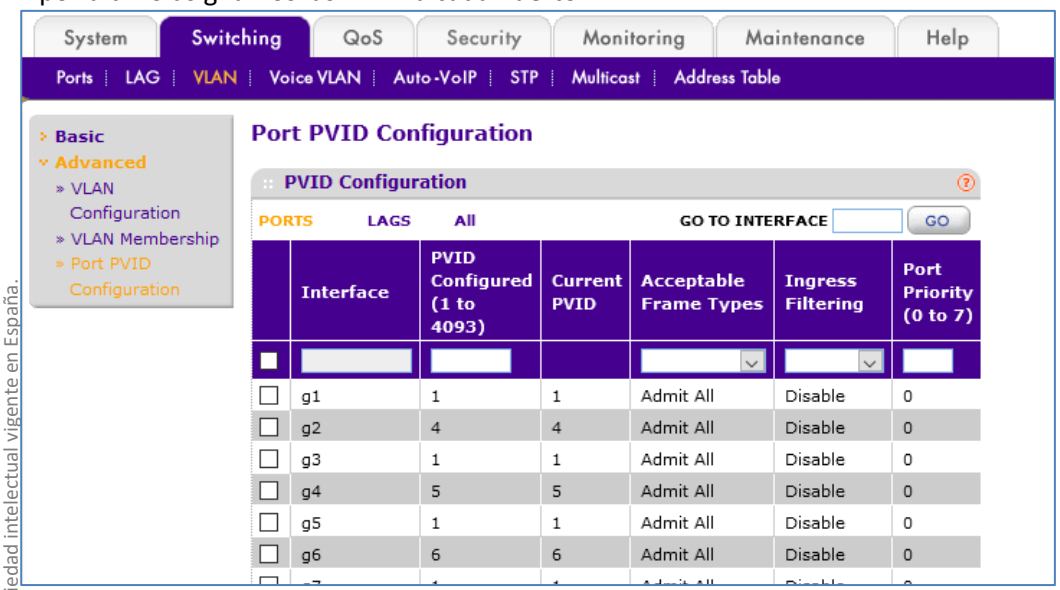
Escribo la ID, Nombre y Método Static y pulso sobre el botón ADD de la parte inferior:



Asignamos los puertos a cada VLAN desde VLAN Membership, seleccionando la VLAN ID y luego pulsando sobre PORT

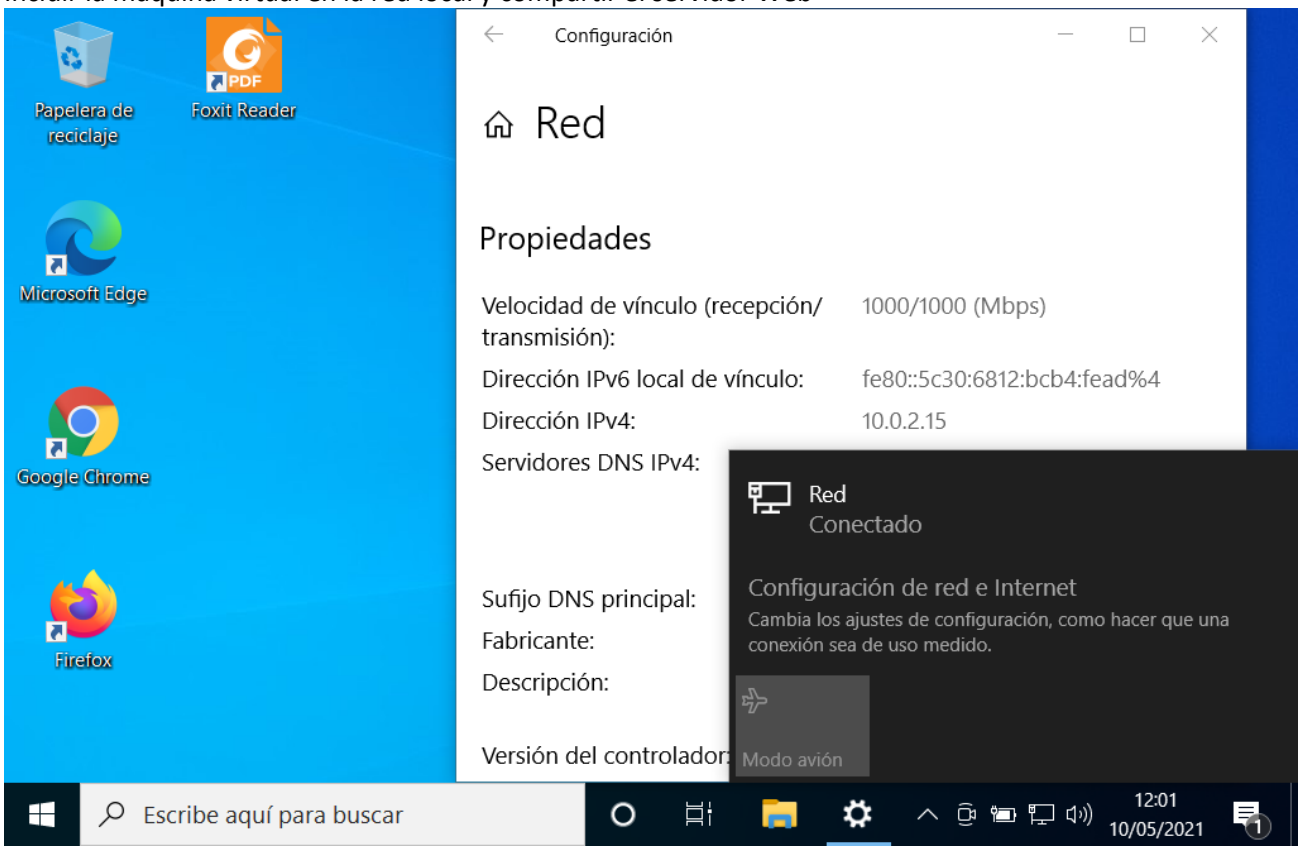


Y por último asignamos las VLAN a cada Puerto.

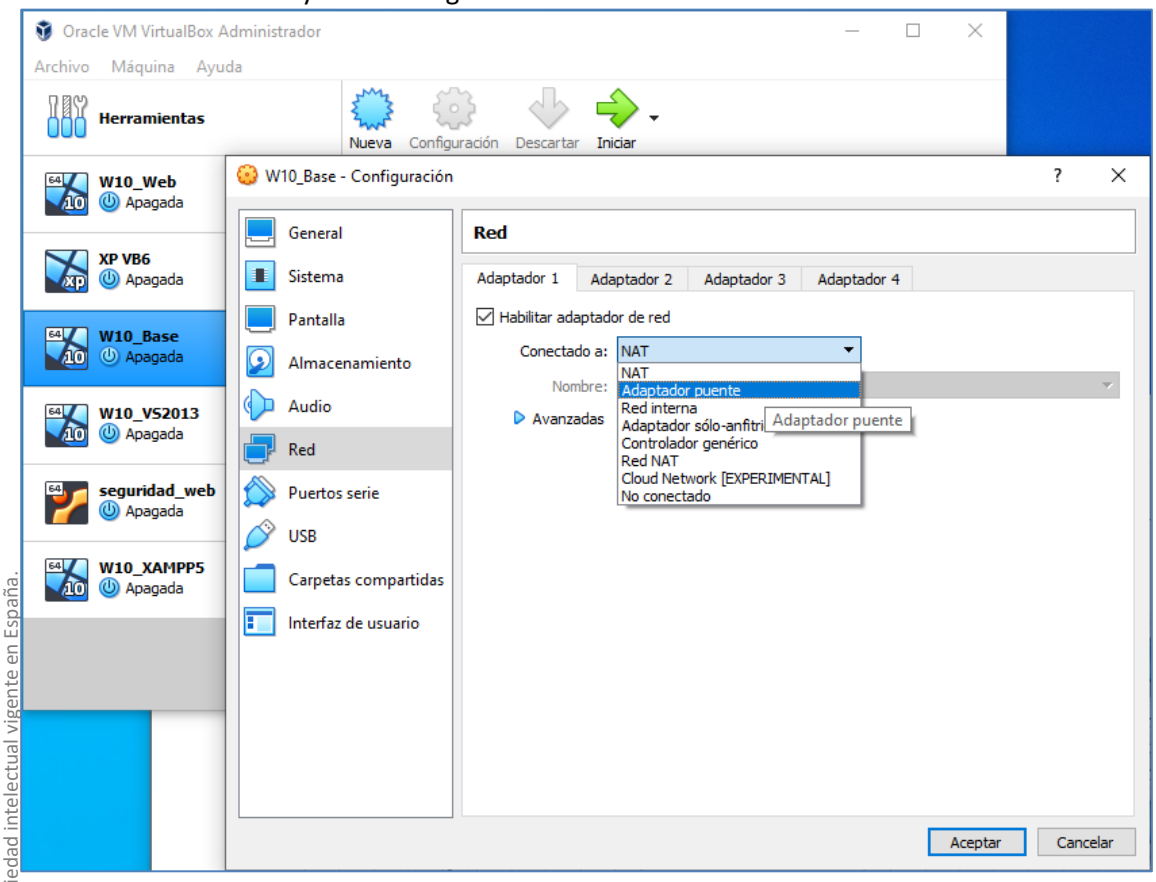


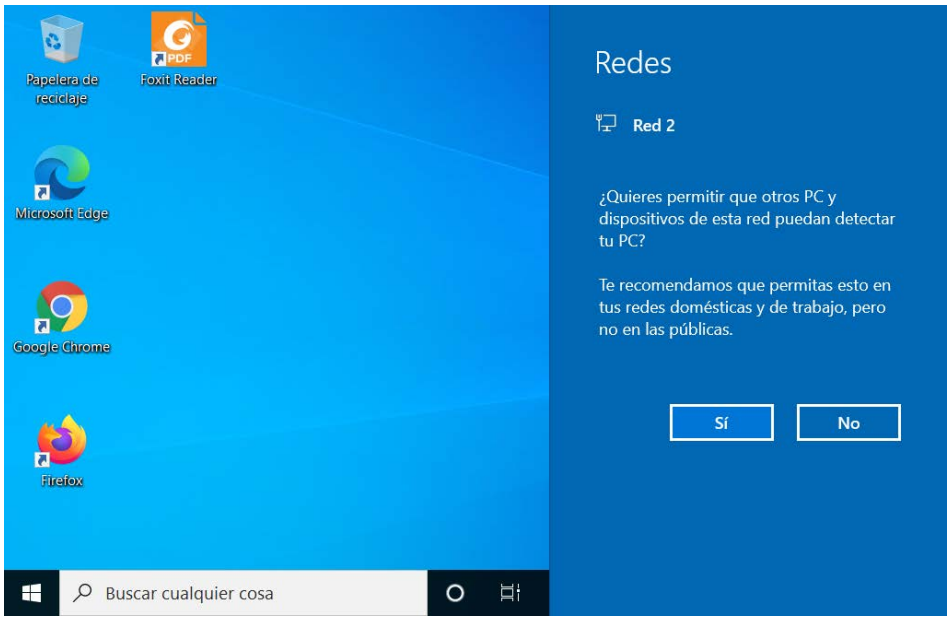
Incluir la máquina virtual en la red local

Incluir la máquina virtual en la red local y compartir el servidor Web

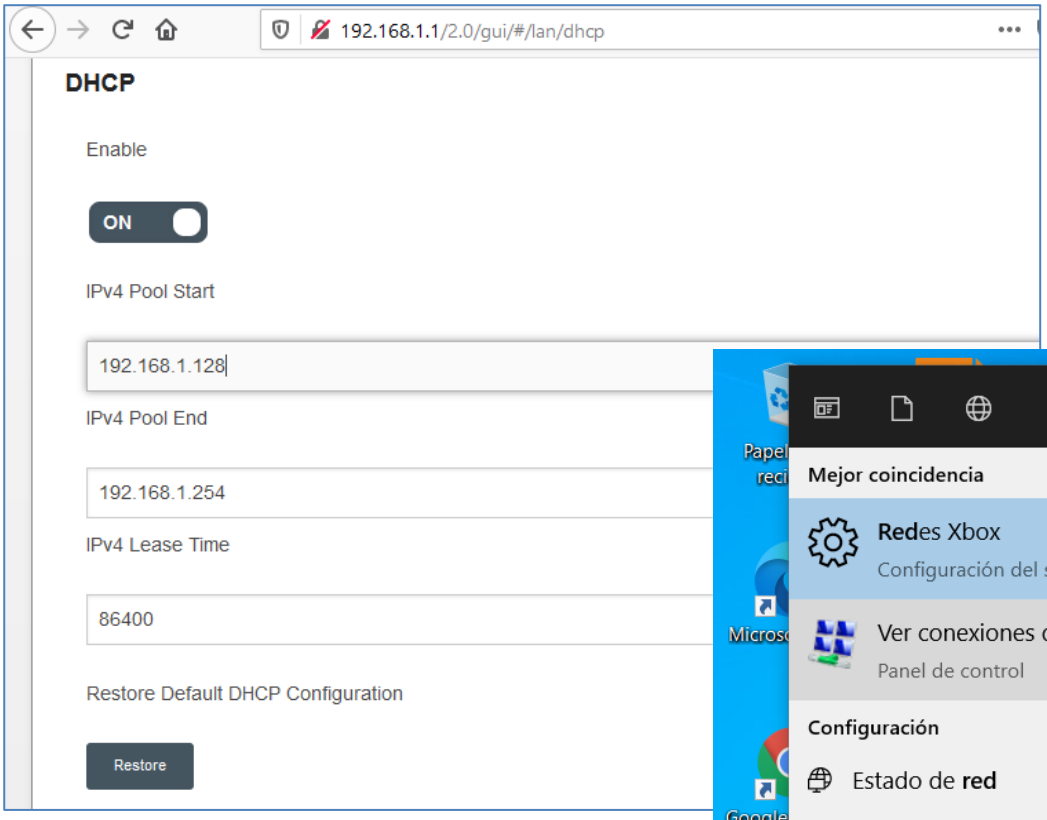


Cambiar del modo NAT y modo Bridge: Puente

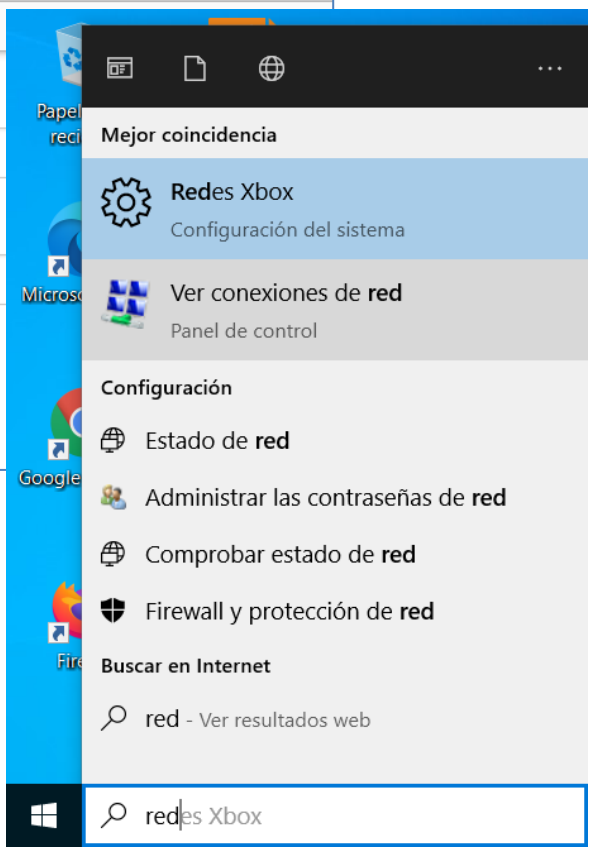




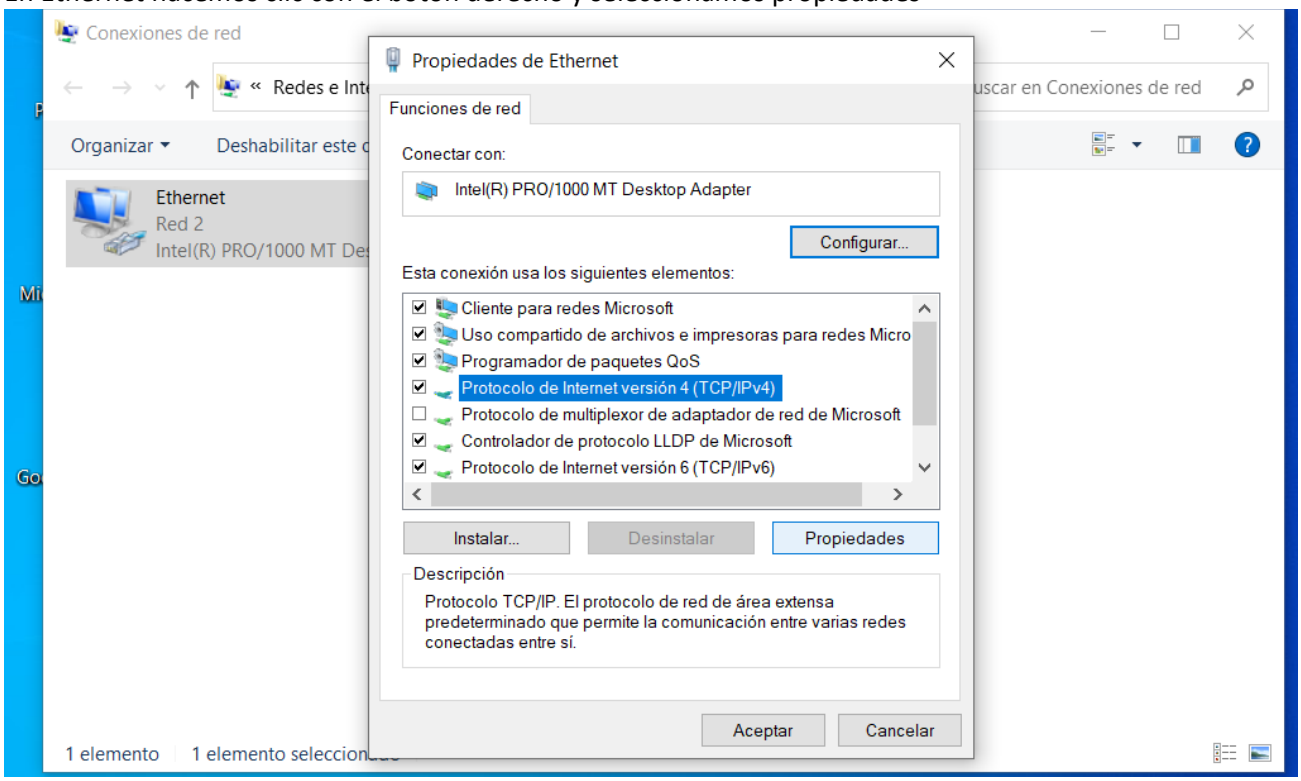
DHCP del Router:



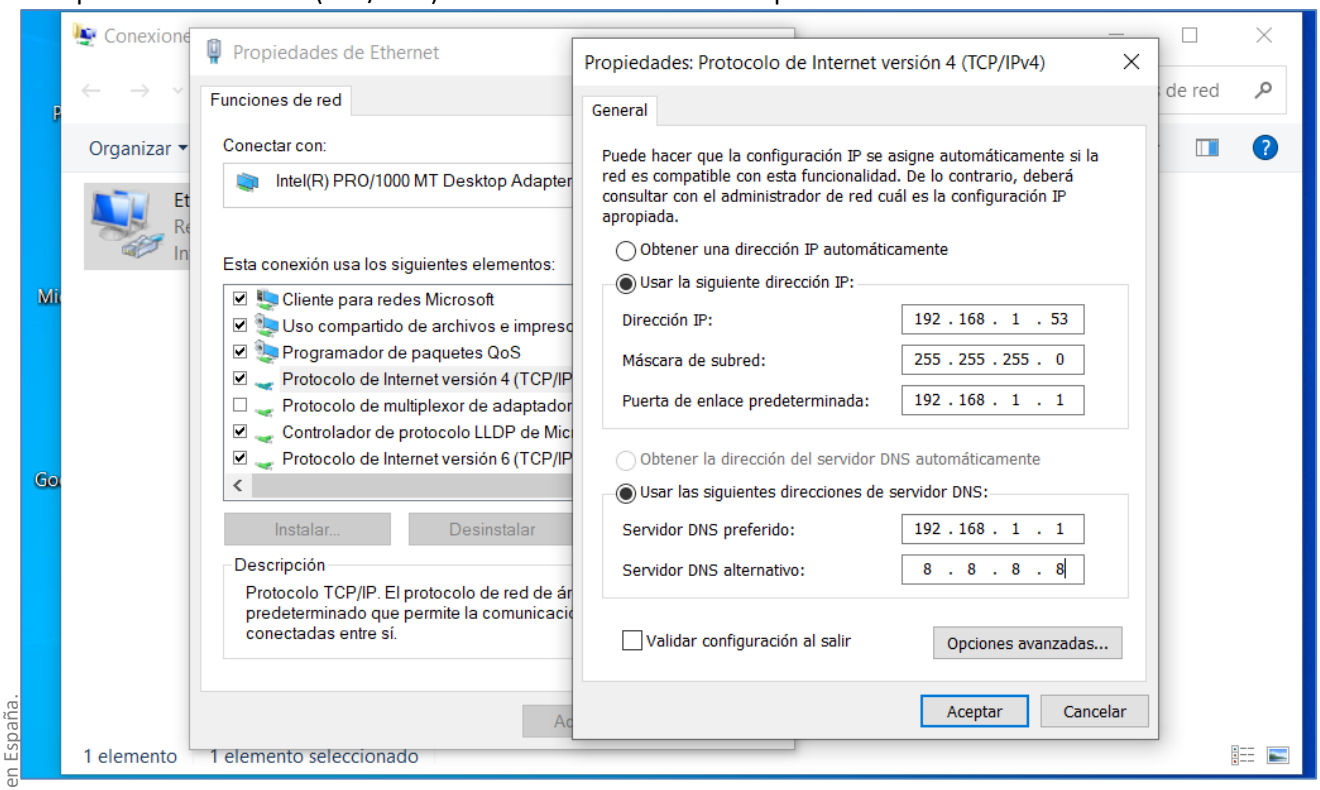
Cambiamos la IP de la máquina virtual:



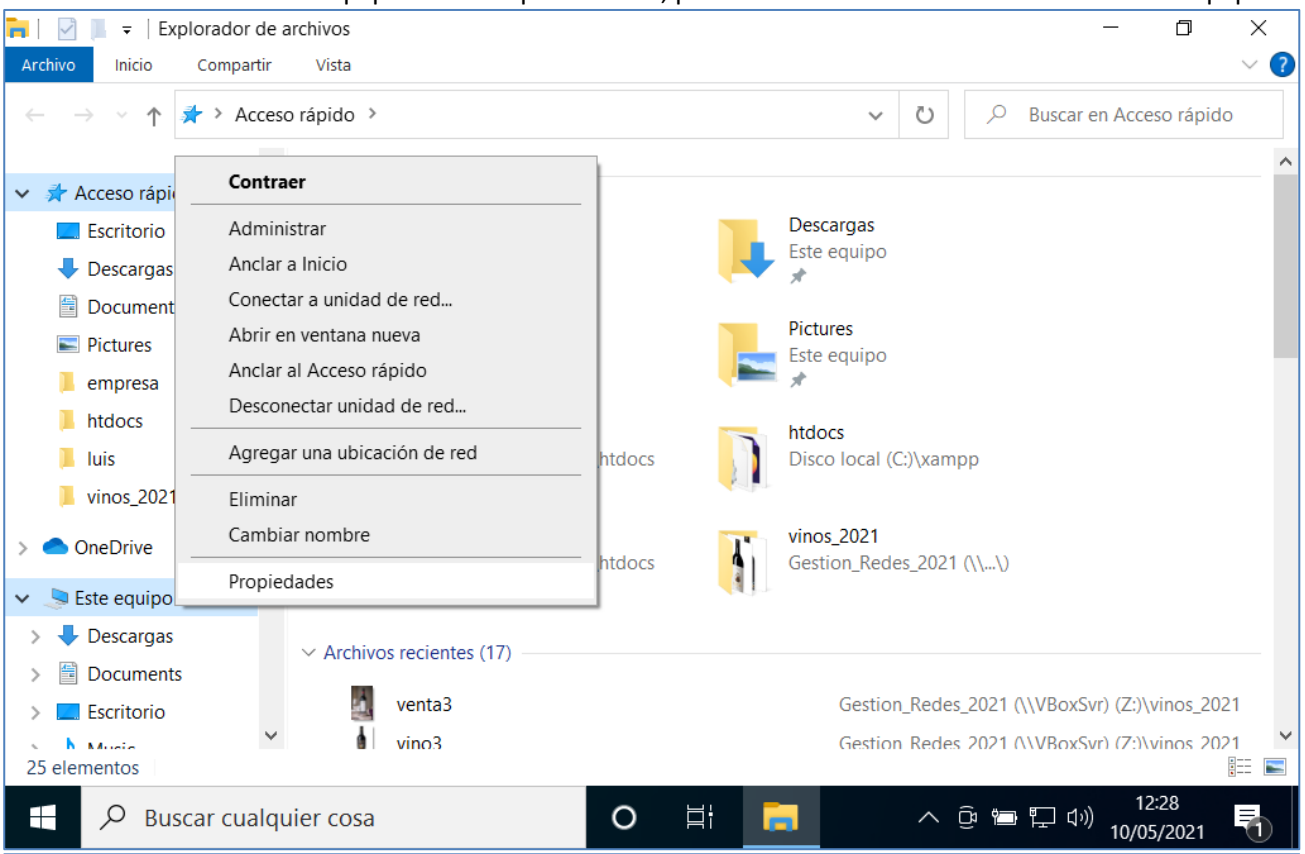
En Ethernet hacemos clic con el botón derecho y seleccionamos propiedades

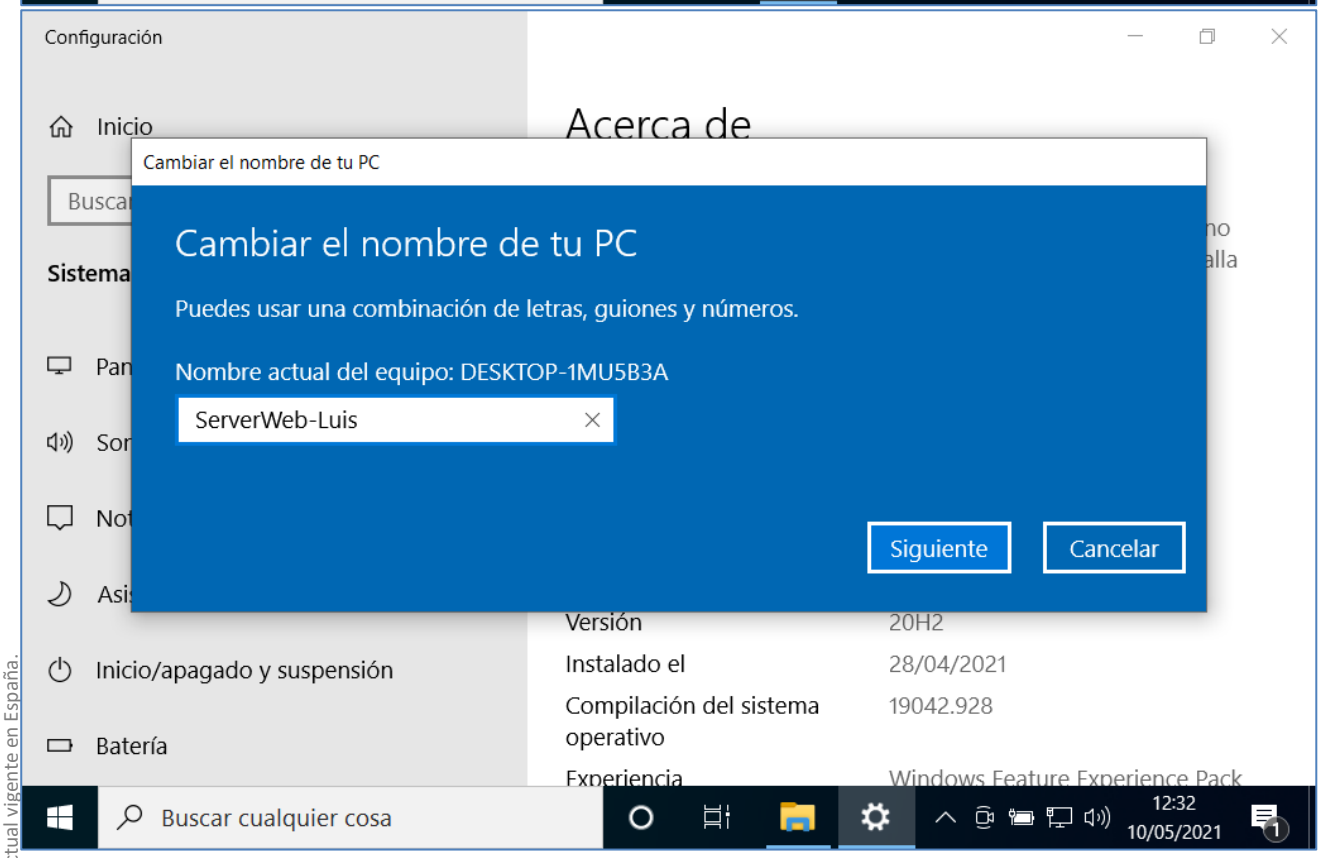


Y en protocolo versión 4 (TCP/IPv4) seleccionamos también Propiedades:

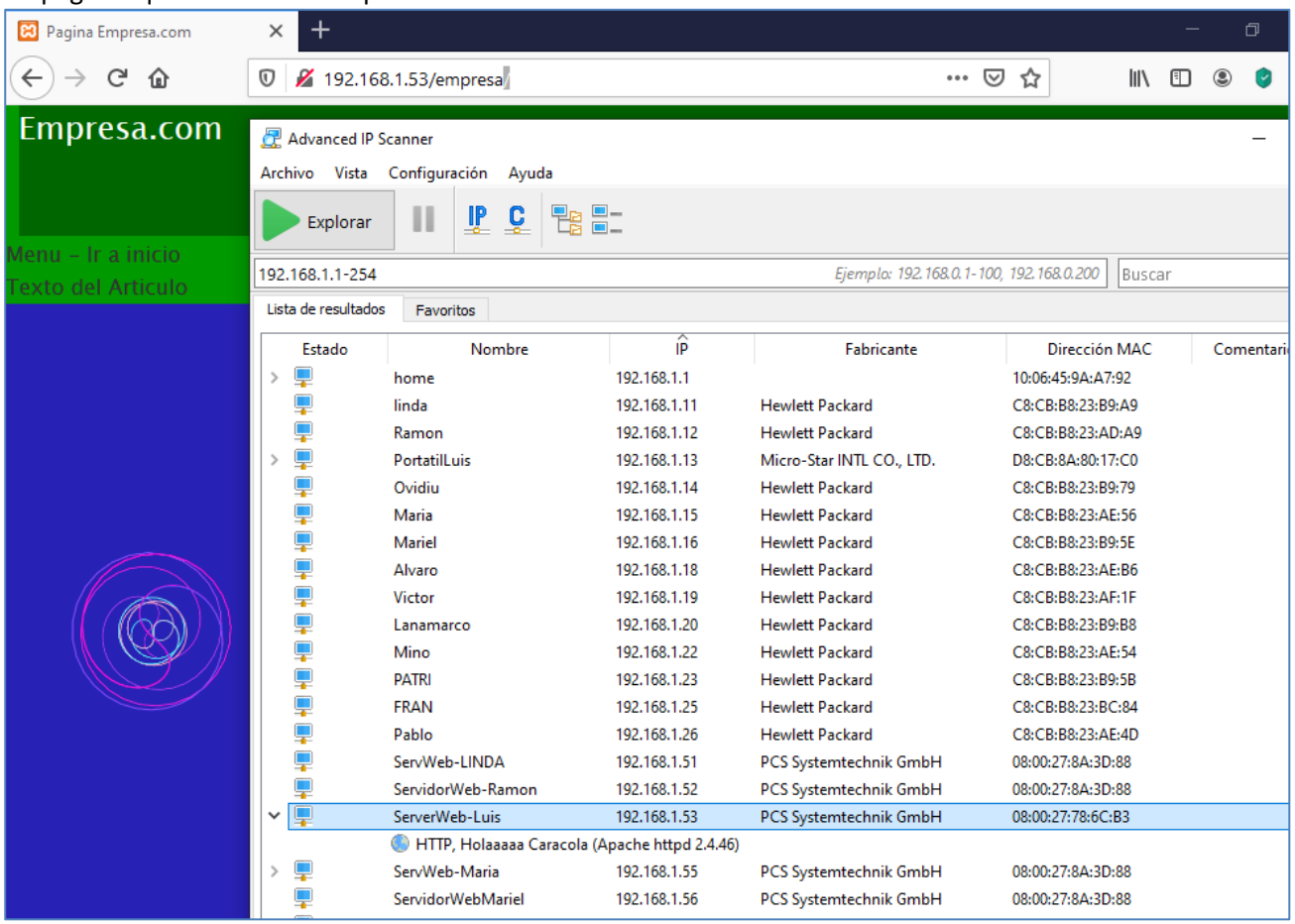


Cambiamos el nombre del equipo de la máquina virtual, pulsando con el botón derecho sobre Este equipo:

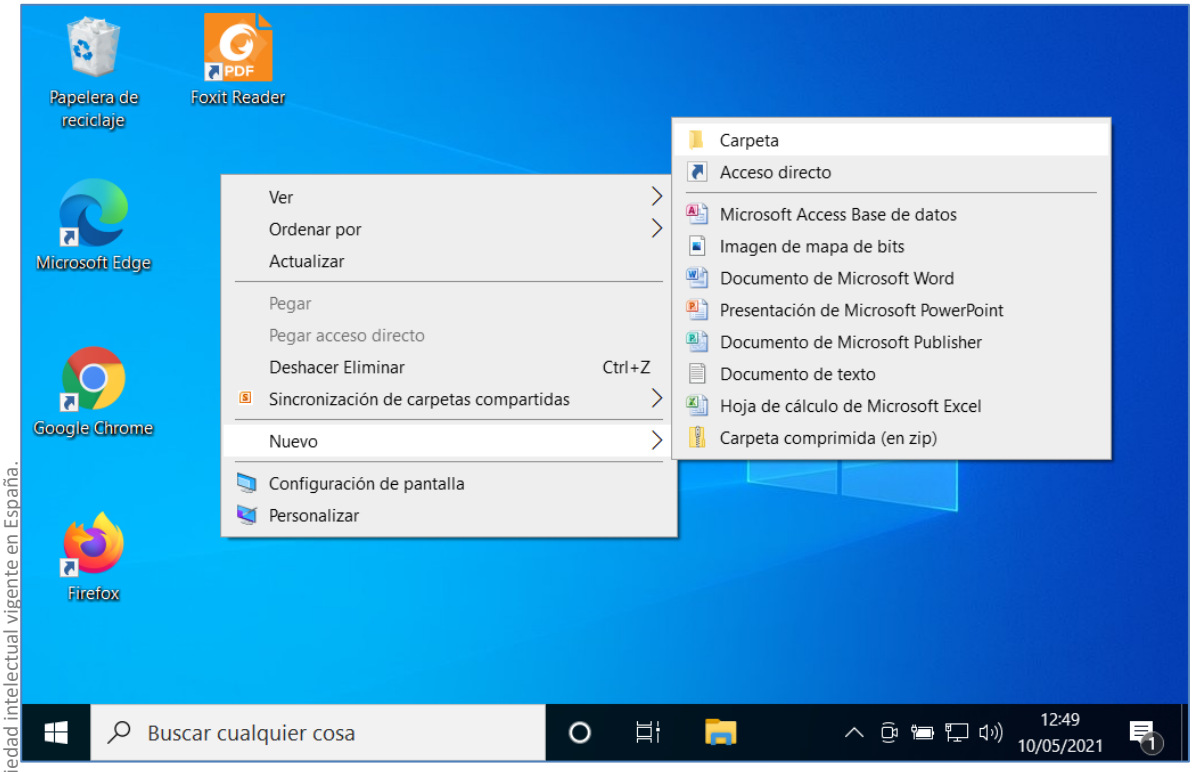


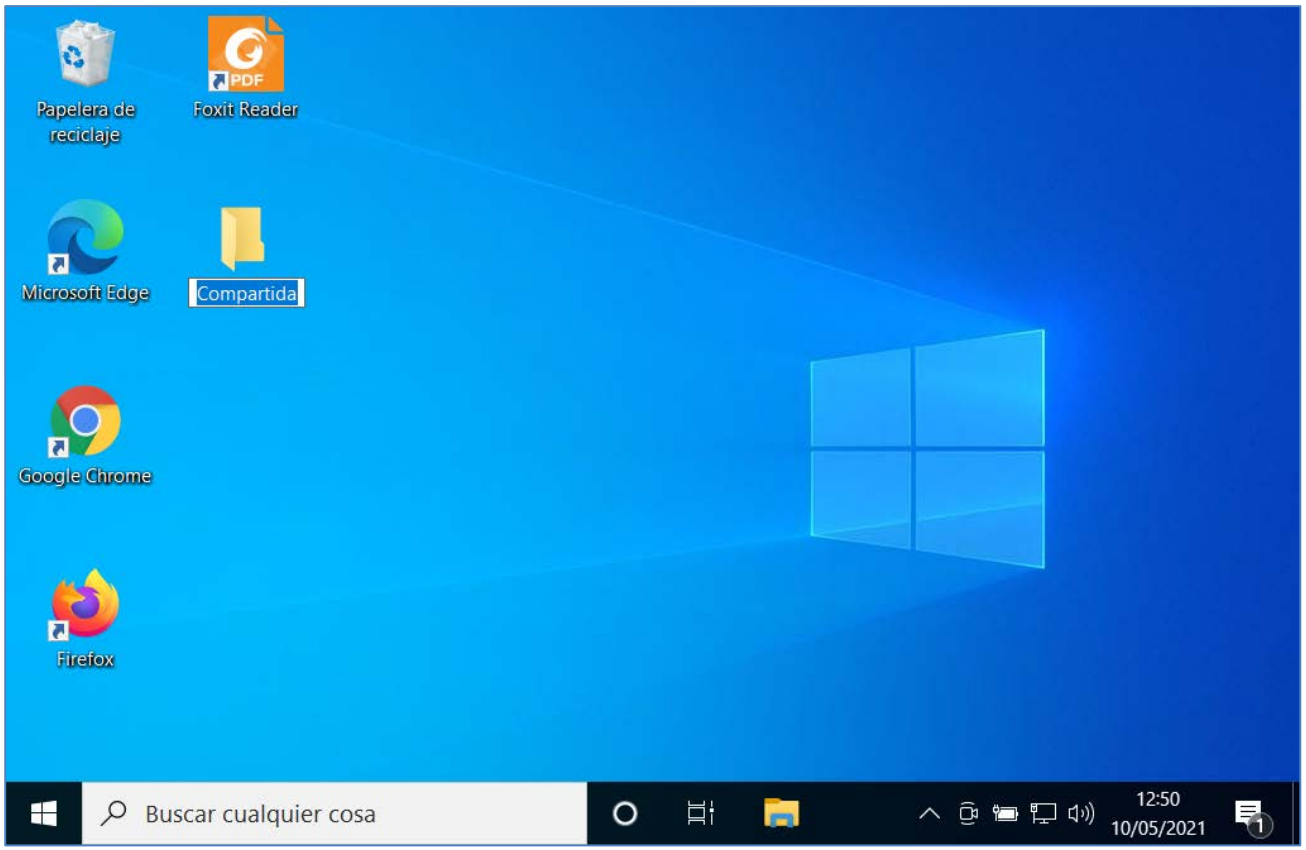


Y ahora si accedemos a IP de cualquiera de las máquinas virtuales de nuestra red por un navegador veremos las páginas que hicimos en los primeros días del curso:

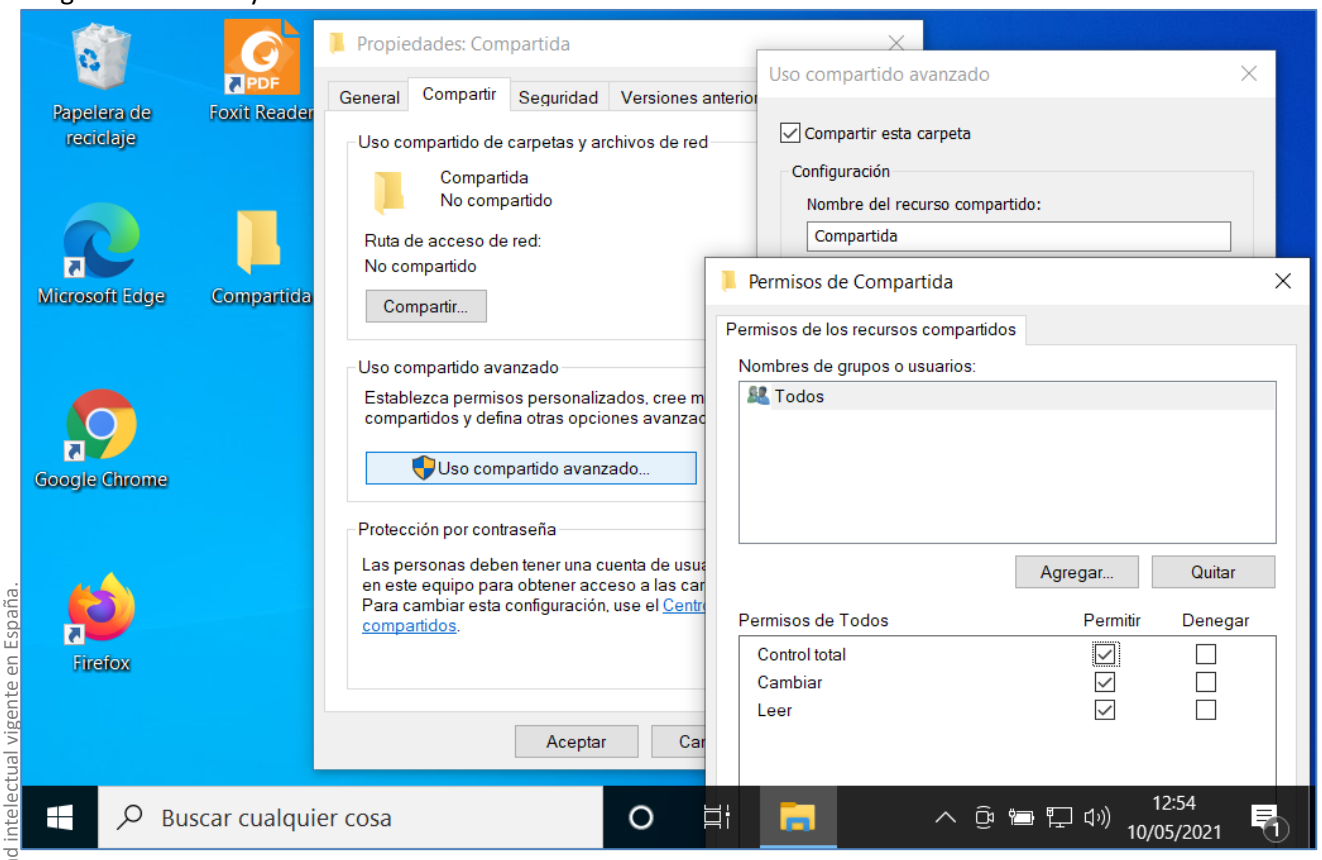


También podemos compartir elementos de las máquinas virtuales con otros usuarios de la red. En este caso Compartimos una carpeta en el escritorio de la máquina virtual:

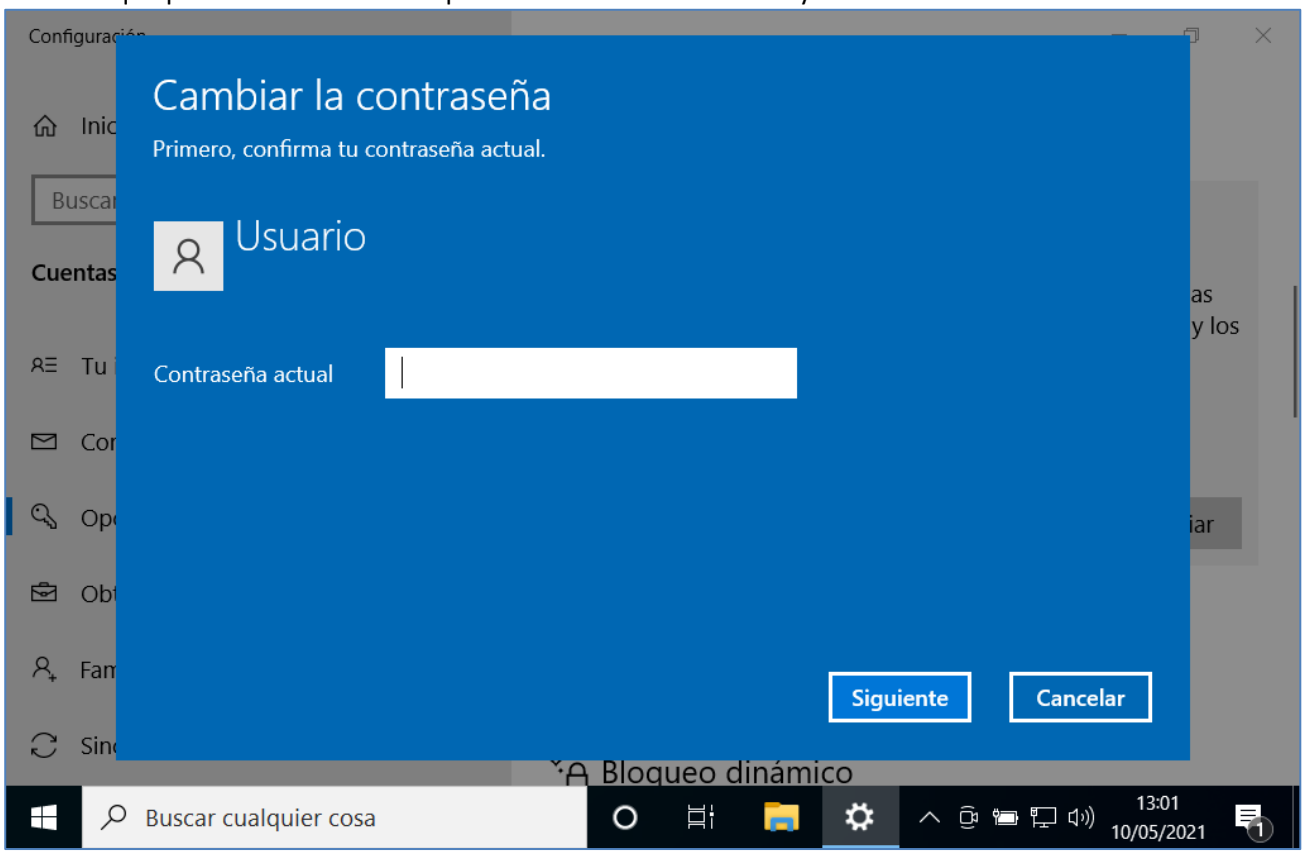




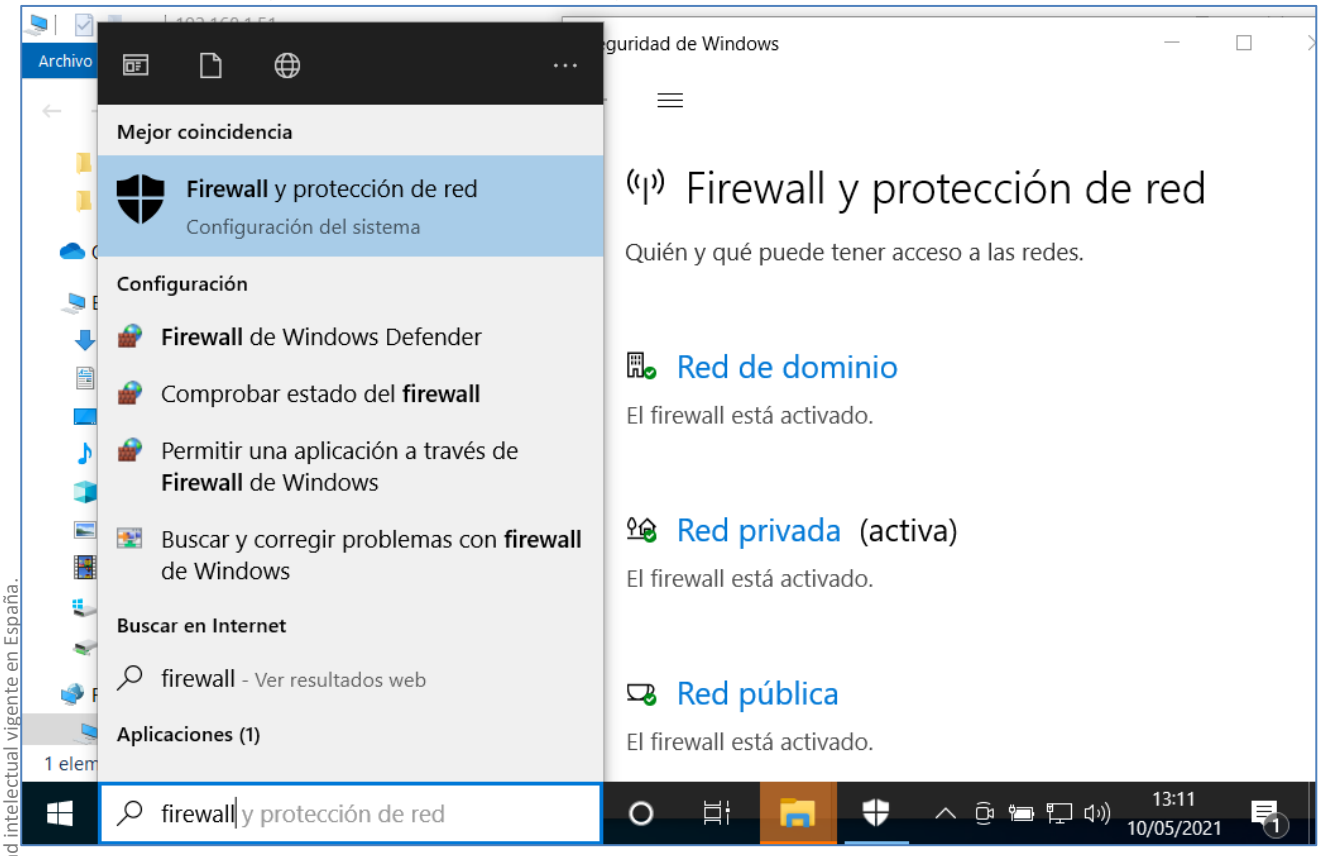
Botón derecho Carpeta en la Carpeta, Luego hacemos clic en la pestaña Compartir.
Luego en Uso compartido avanzado…
Luego en Permisos y marcamos Permitir control Total a Todos.

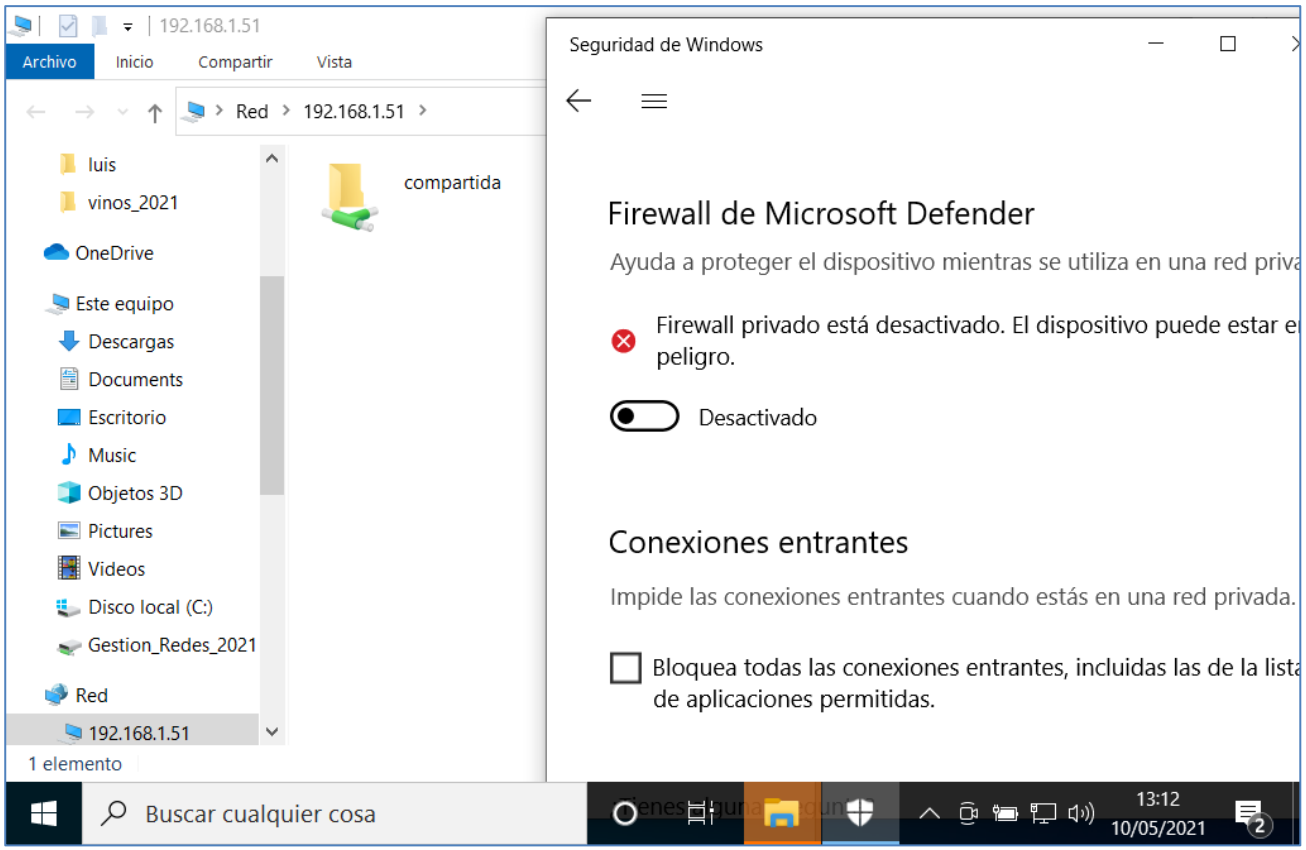


Para poder compartir elementos de uno a otro equipo debemos identificarnos y para poder hacerlo tenemos que ponerle contraseña. Le ponemos contraseña 123456 y el nombre de usuario es **Usuario**:



Quitamos el firewall (NO HACER EN CASA!!!!!!!!!!!)

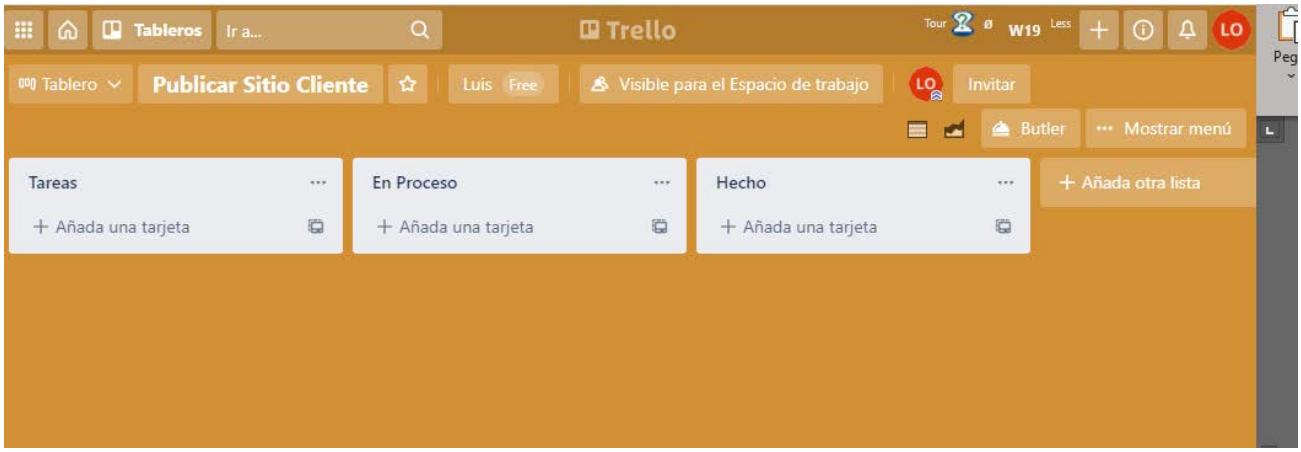




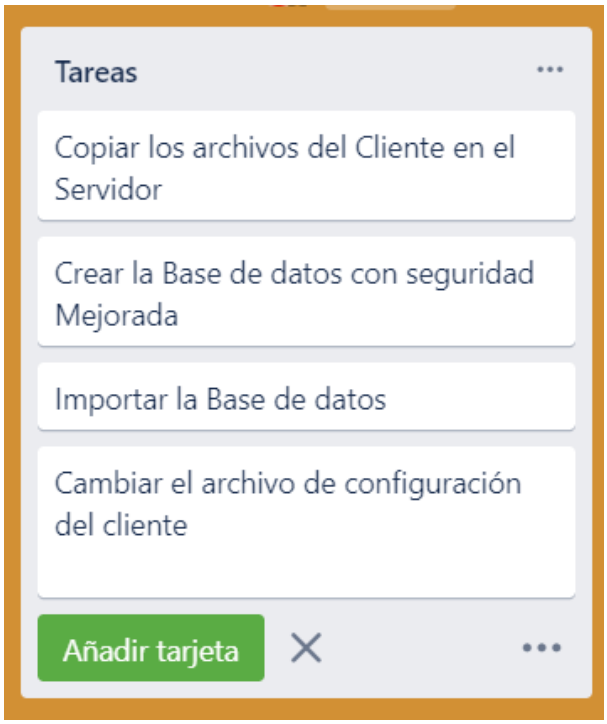
Publicar Sitio Cliente

Con trello creamos el tablero:

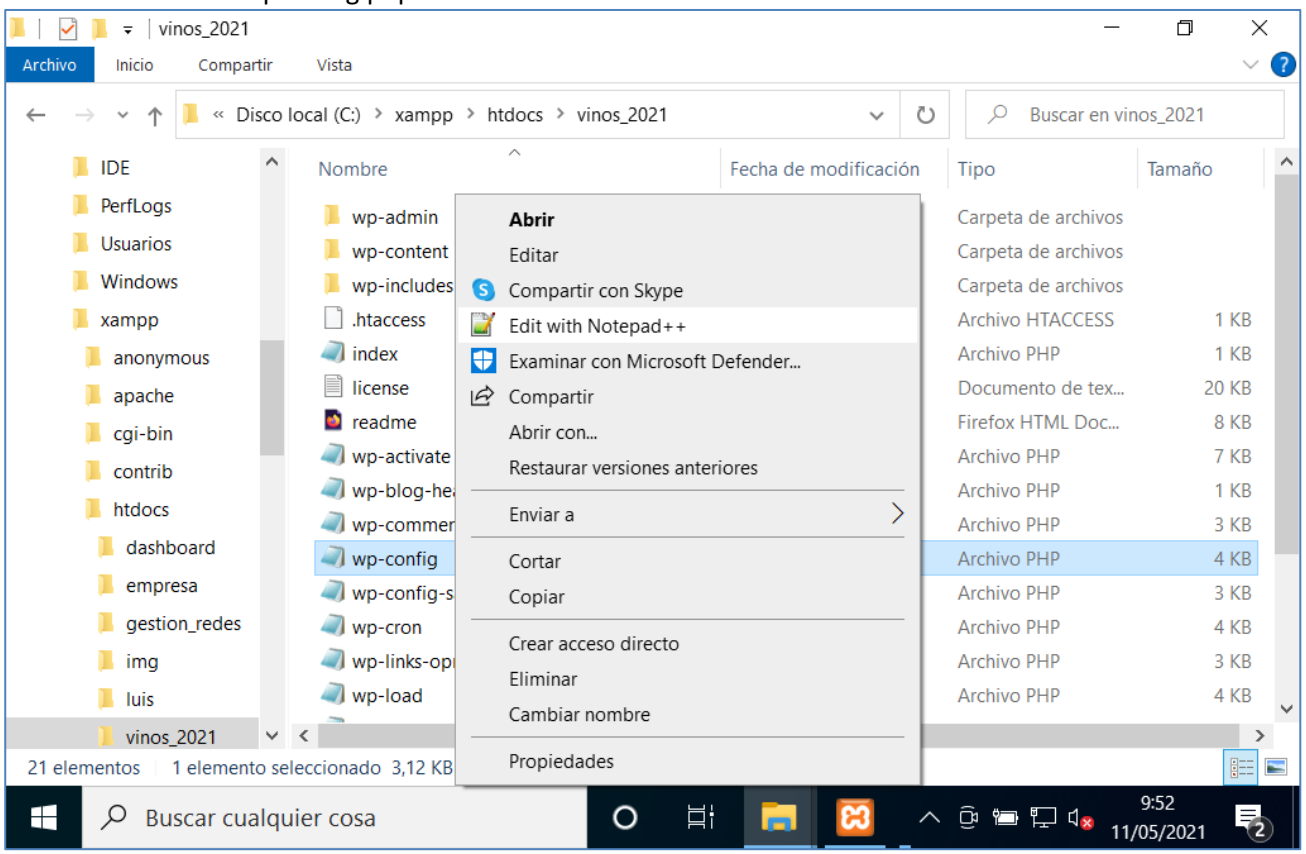
Creamos las 3 Listas:



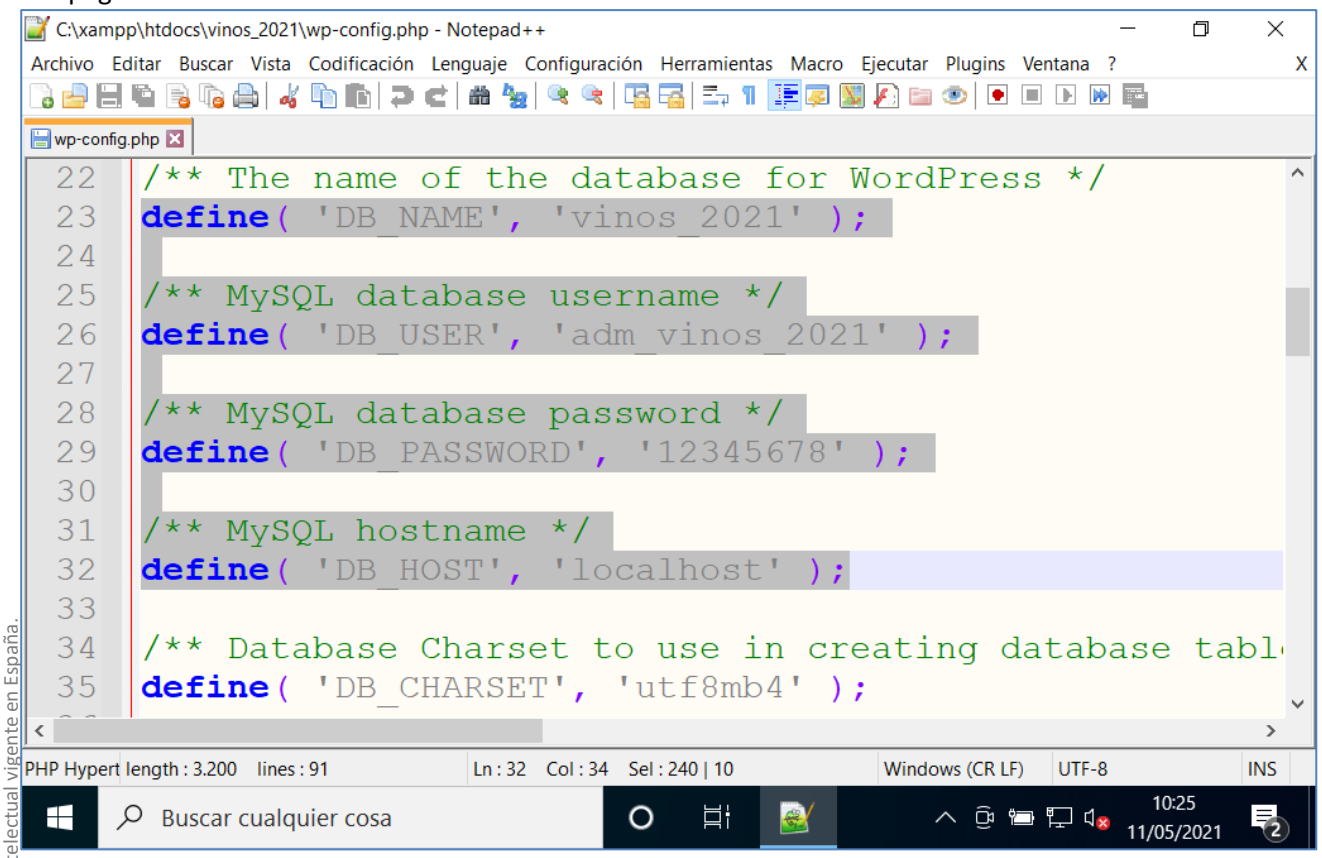
Creamos las tareas:



Editamos el archivo wp-config.php:



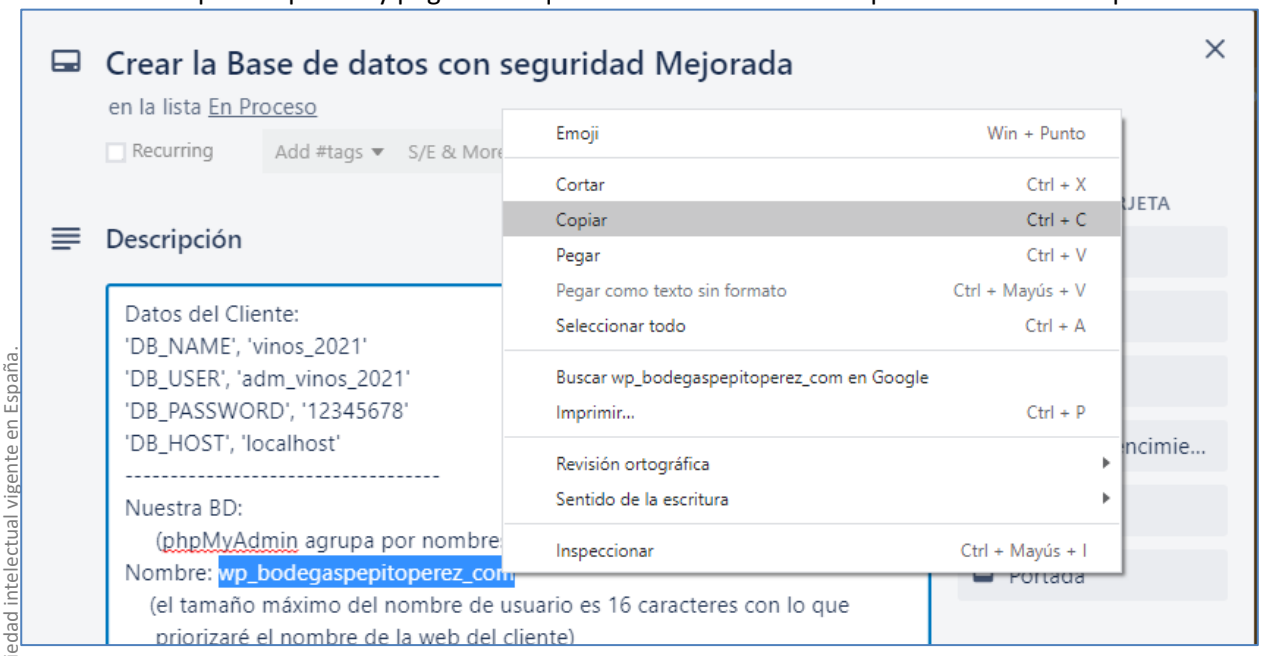
Y lo pegamos en la tarea de trello los datos de la base de datos:



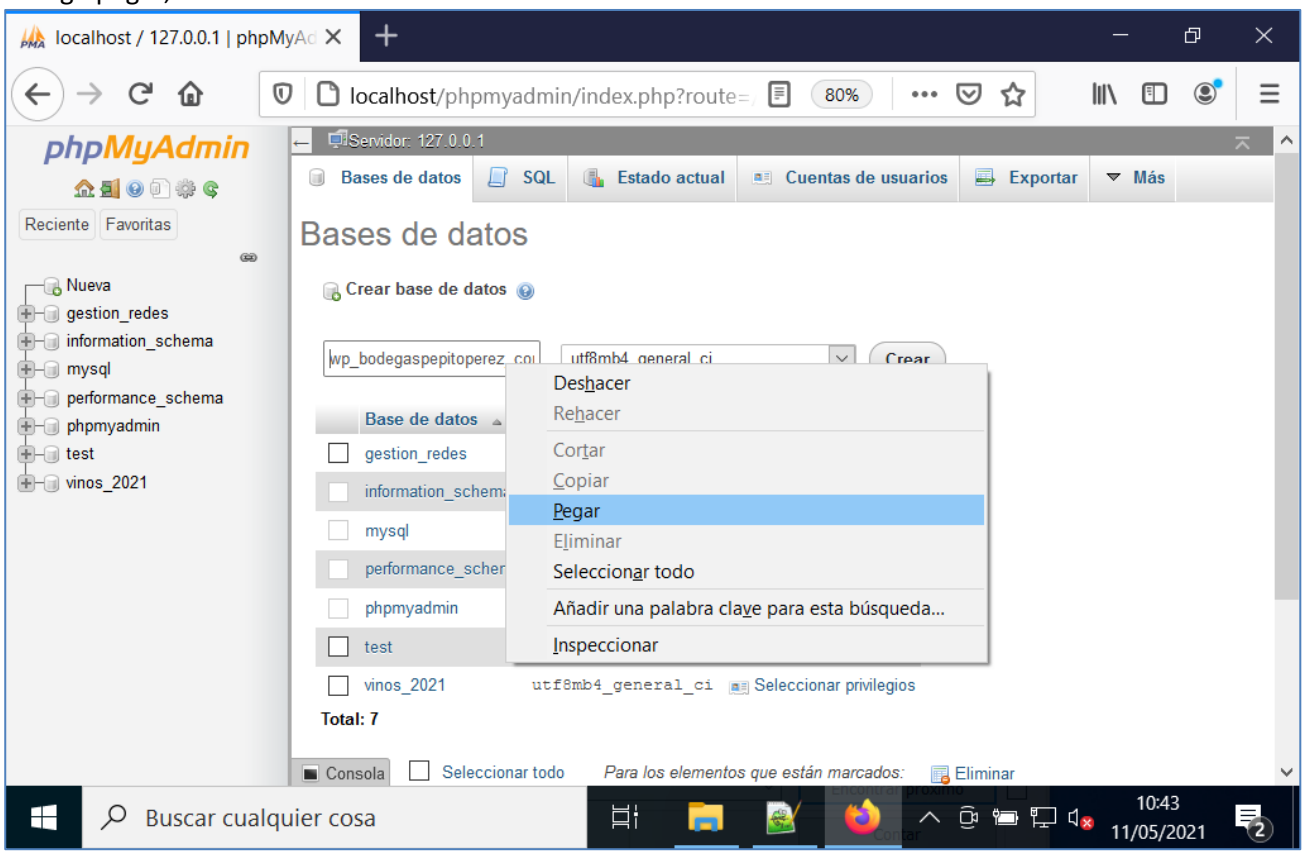
Modificamos la tarea para incluir los nombres que queramos darle a la BD:

Creamos la base de datos, para lo cual nos vamos a PhpMyAdmin, pulsando en el botón Admin de XAMPP:

Creamos la BD pero copiando y pegando lo que hemos escrito en trello para evitar meter la pata:

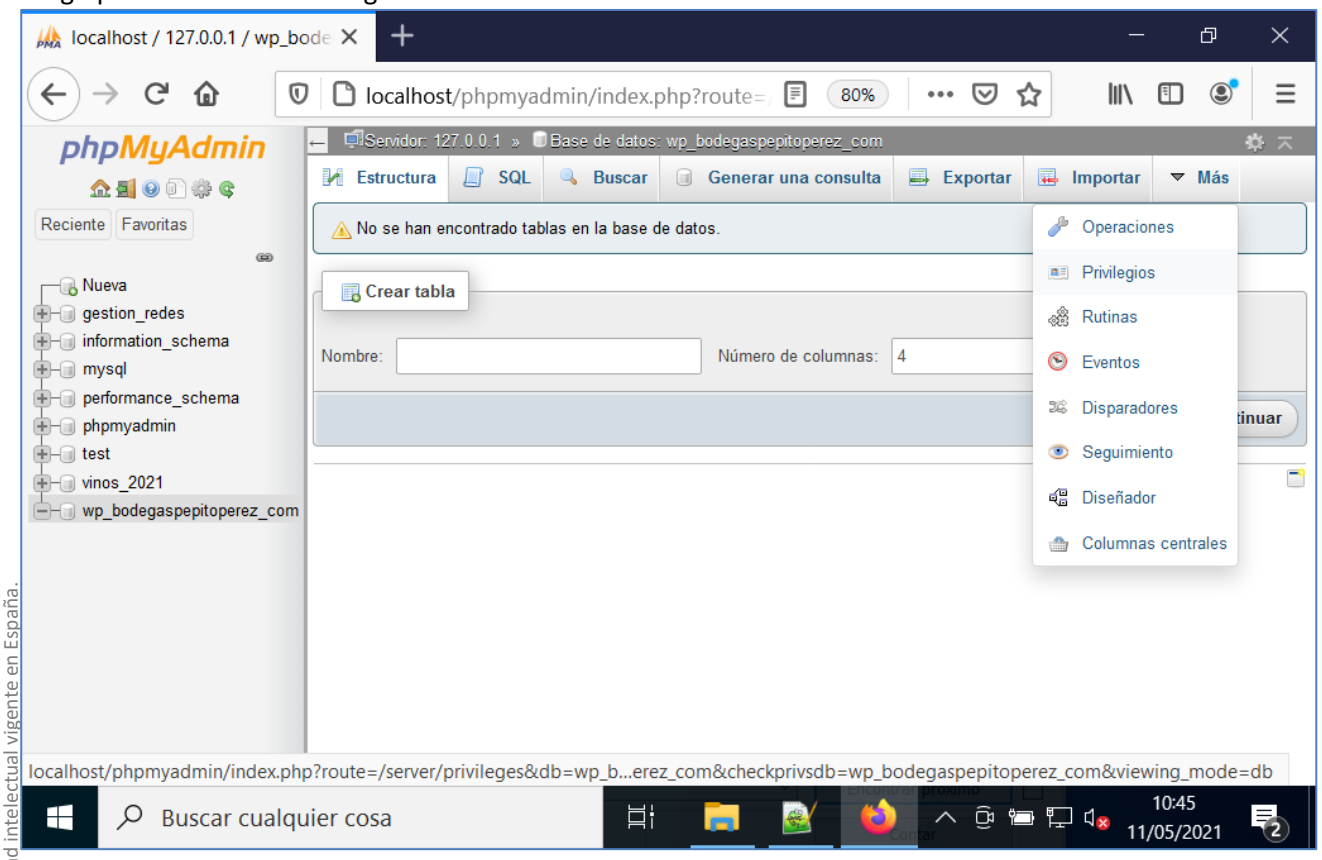


Y luego pegar, en Bases de datos:

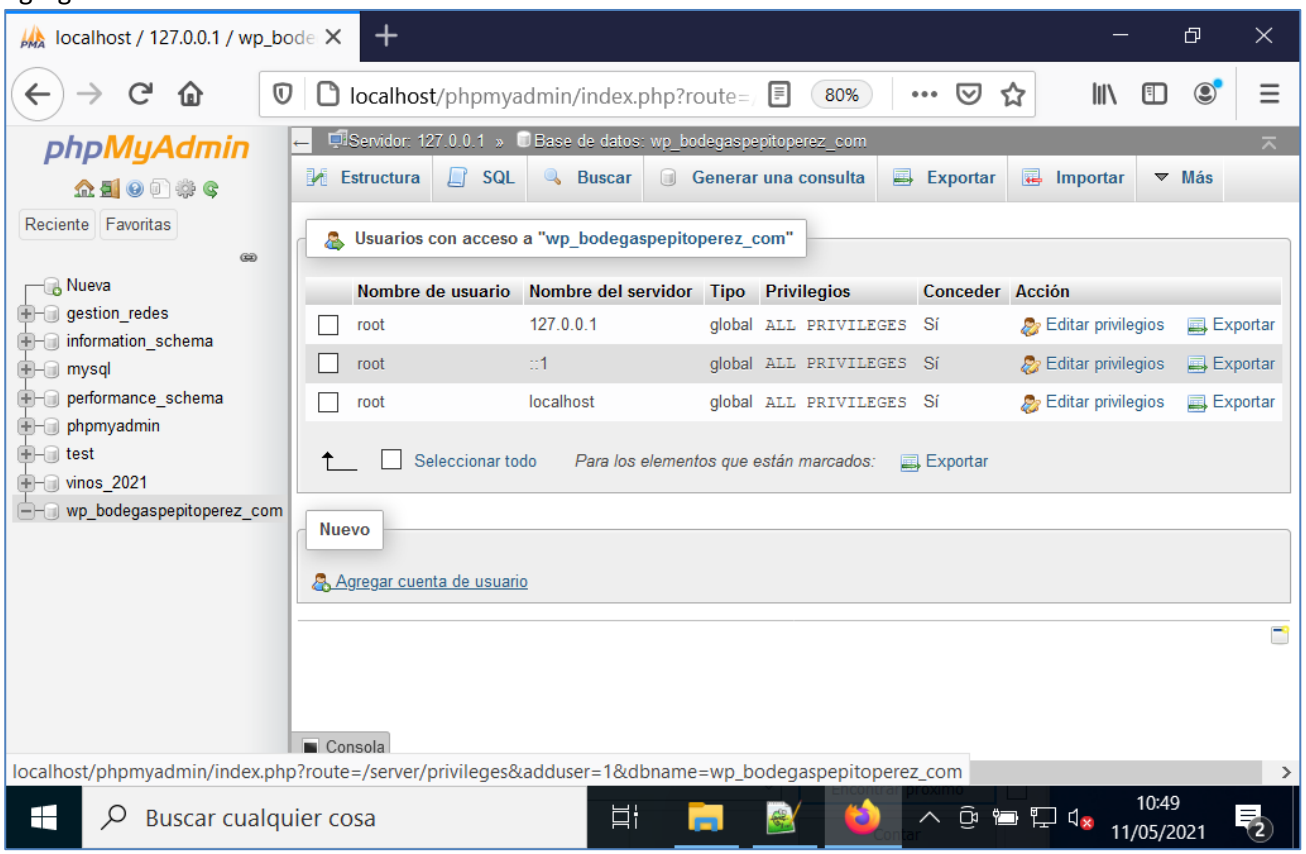


Y pulsamos sobre **crear**.

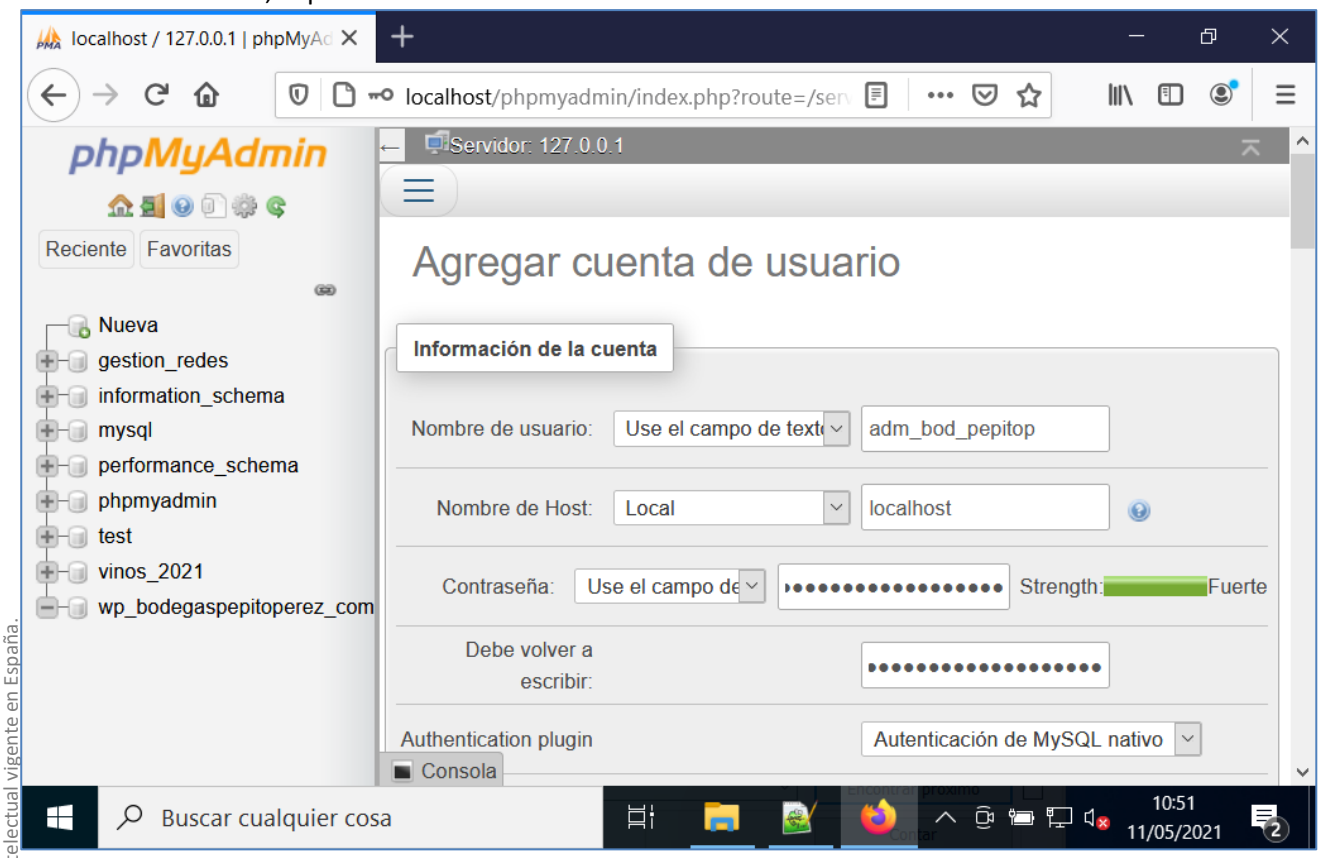
Luego pulsamos sobre Privilegios:



Agregar cuenta de Usuario:

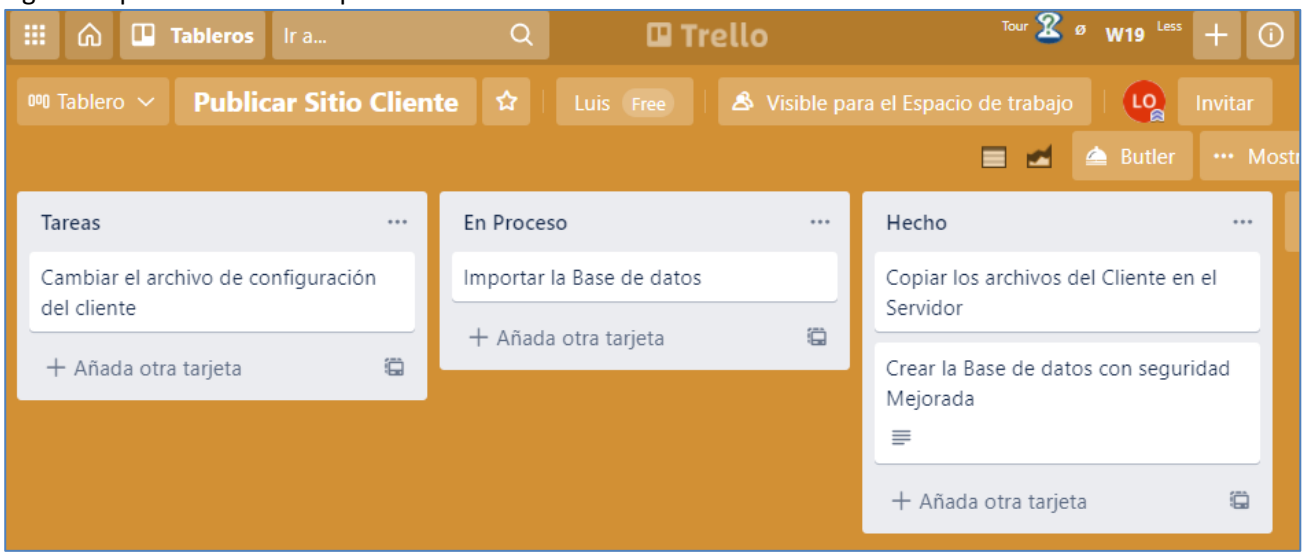


Y metemos los datos, copiándolos de trello:

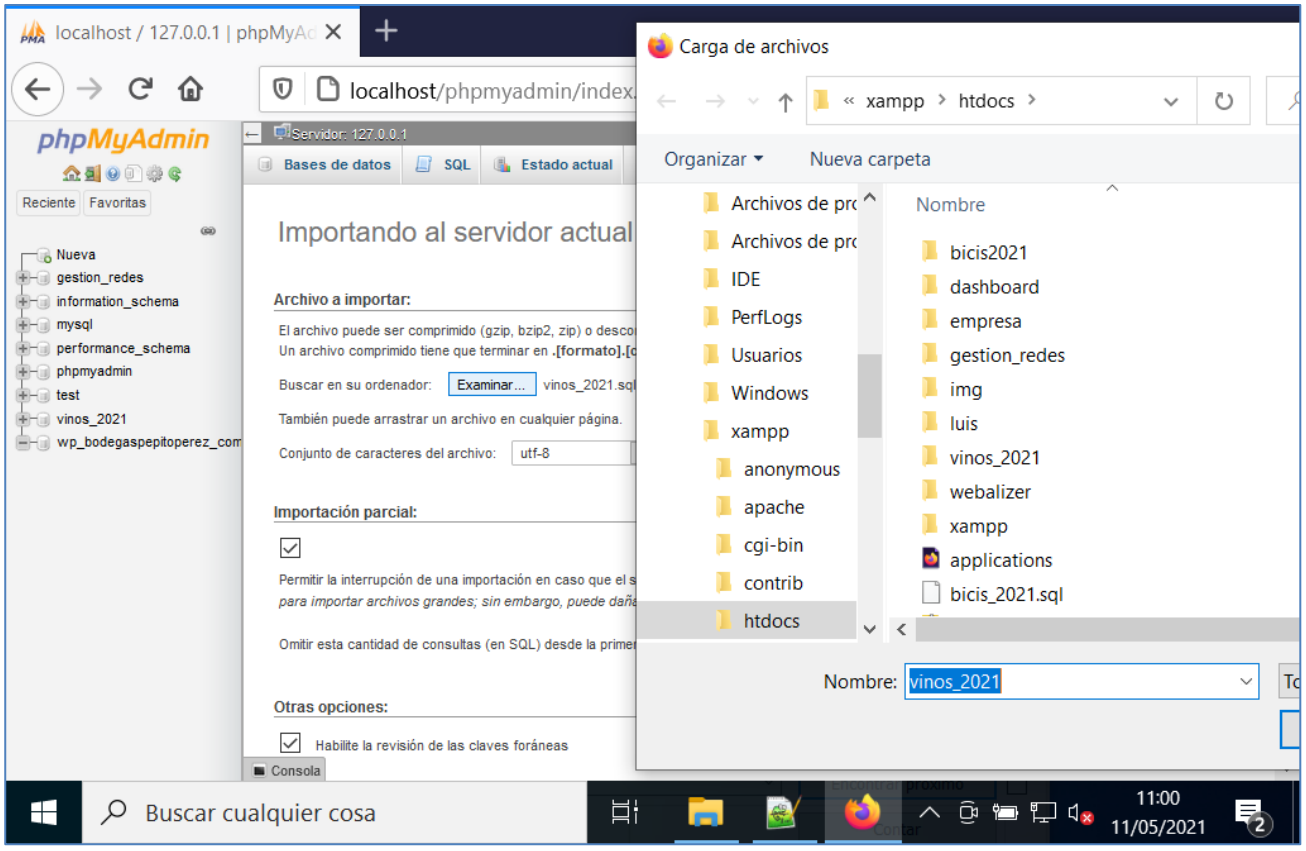


Luego continuar

Siguiente paso del Trello: Importar la Base de datos:

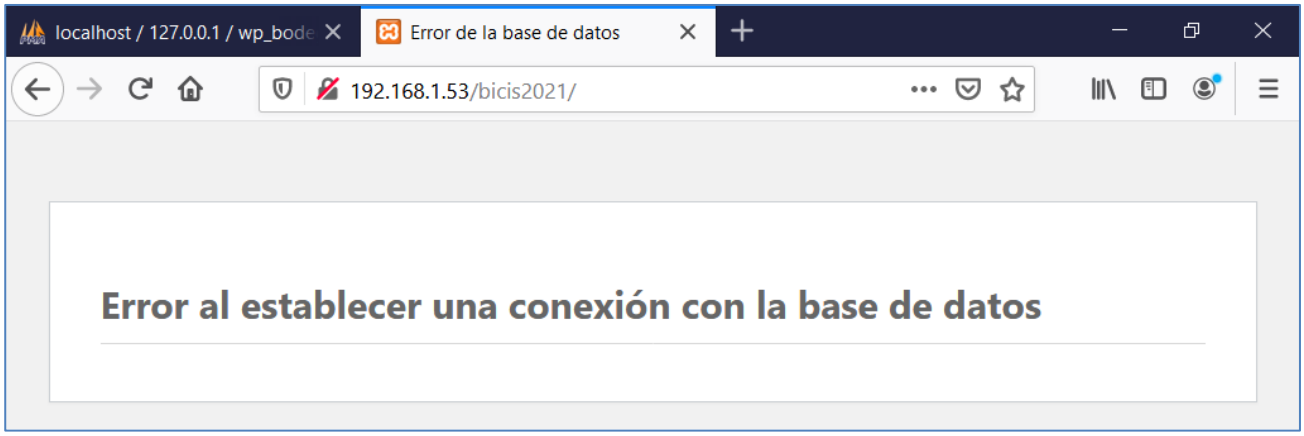


Buscamos el archivo SQL: vinos_2021.sql

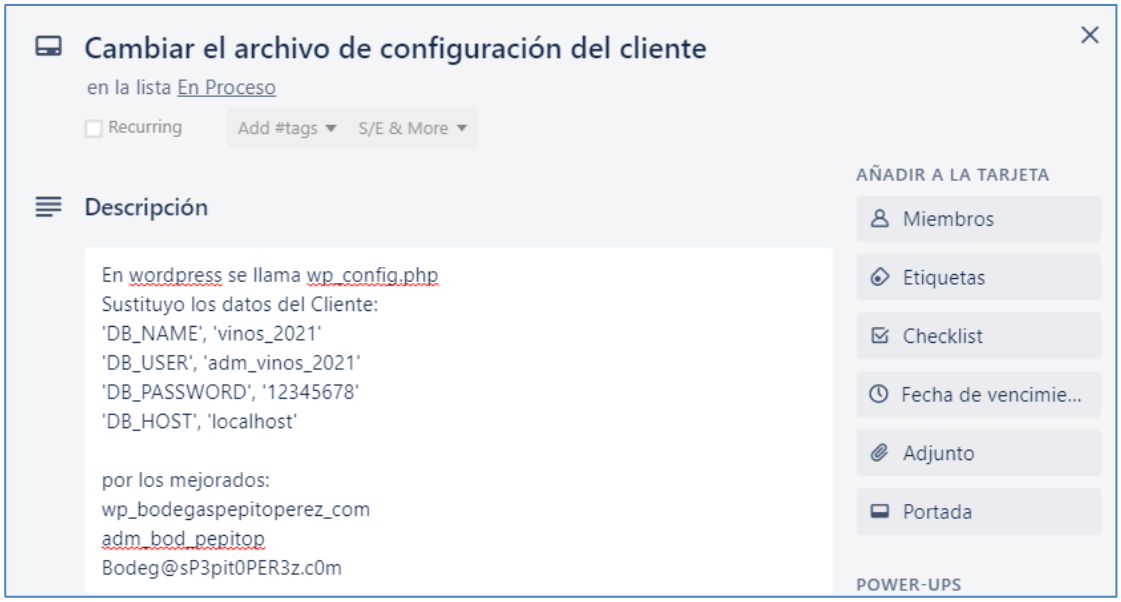


Pulsamos sobre **Continuar**

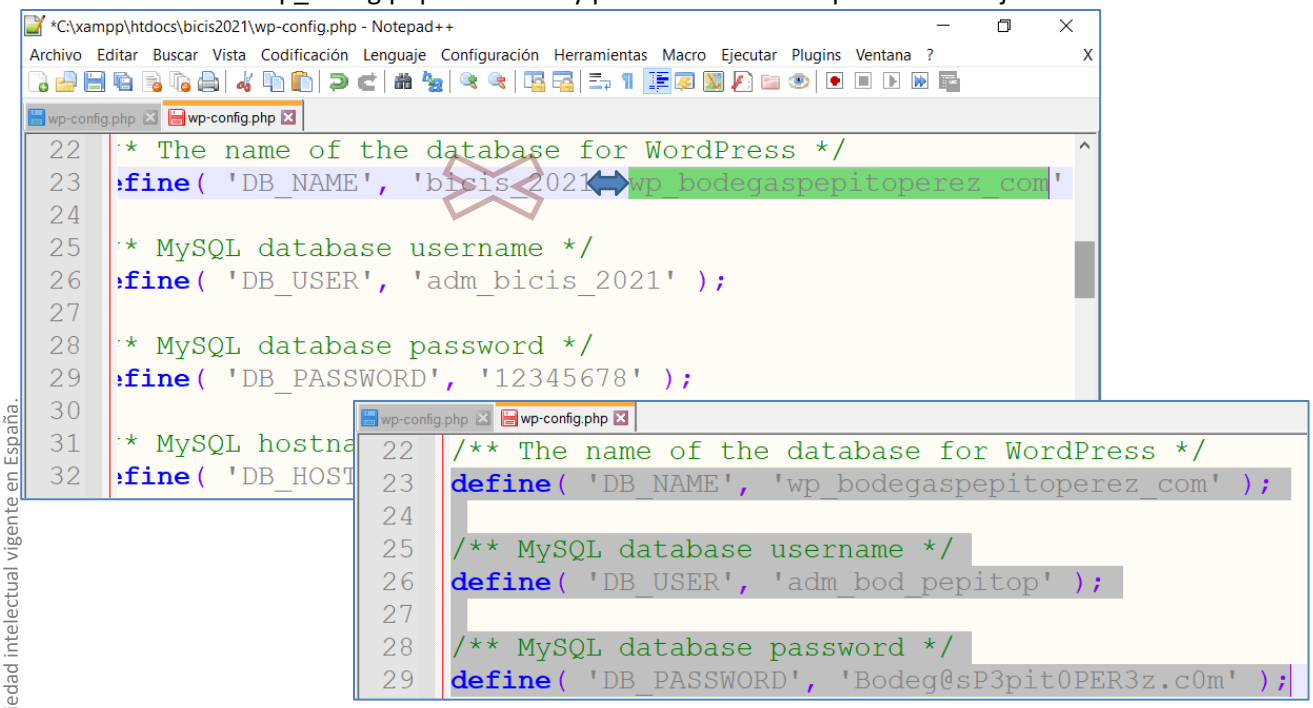
Y ya tenemos restaurada la base de datos, ahora el sitio nos dirá que está desconectado de la base de datos:



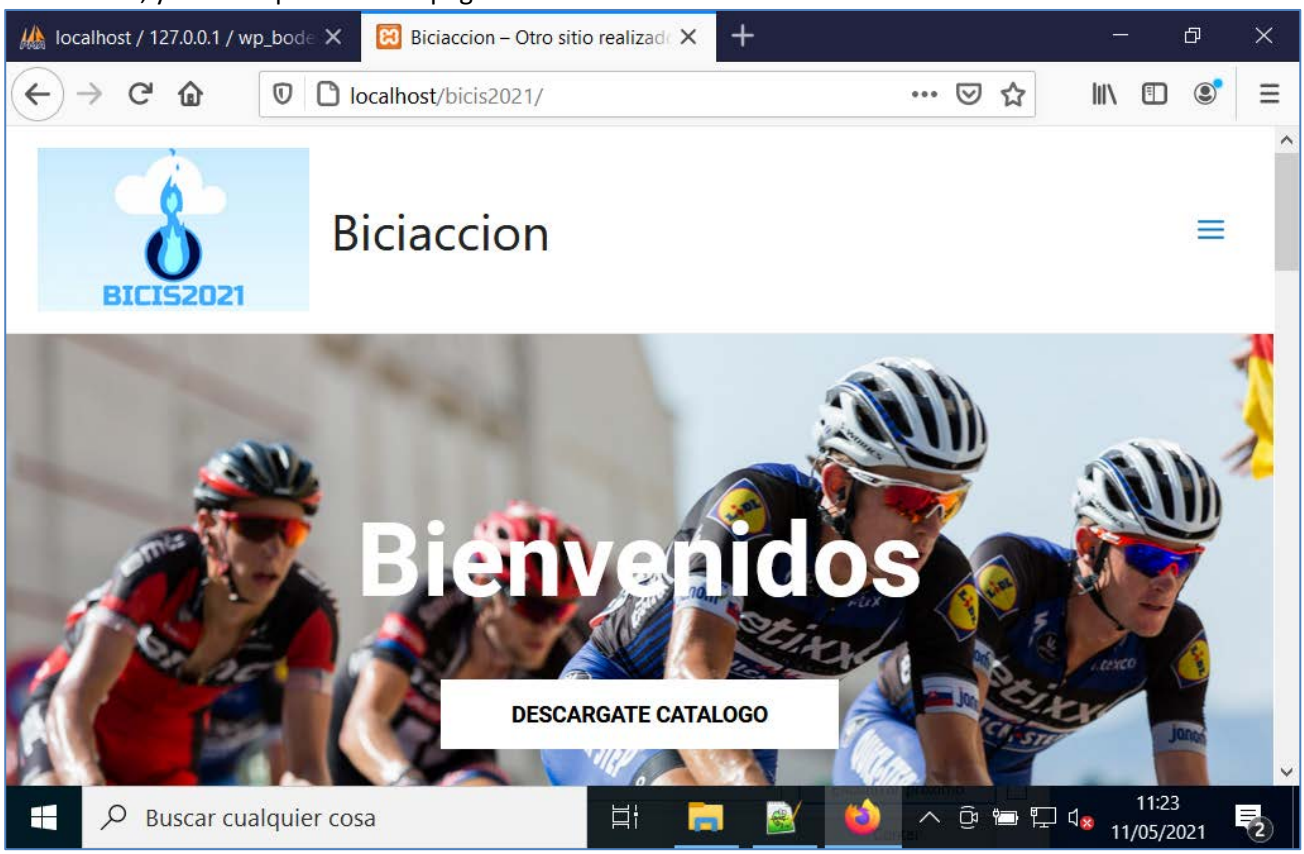
Porque tenemos que ponerle los datos mejorados con los que hemos creado la BD



Editamos el archivo wp_config.php del cliente y ponemos los datos que hemos mejorado:



Guardamos, y si ahora probamos la página debería funcionar:



4. Medios de transmisión inalámbricos

4.1. Características de la transmisión no guiada

Un medio de transmisión inalámbrico es aquel que no emplea ningún cable (no – alambre) para transmitir la información.
También se les denomina medios de transmisión no guiados, ya que la información no va guiada o encapsulada en un cable.
Se trata del otro gran grupo de medios de transmisión (además de los medios de transmisión guiados) que se emplea en la actualidad para transmitir datos, televisión, telefonía, etc., y cualquier tipo de información o servicio de telecomunicaciones.
En los medios de transmisión inalámbricos se emplea el aire como medio de transmisión y pueden ser de dos tipos:

- Medios de transmisión por **radiofrecuencias**:
  Es aquel en la que se emplean señales electromagnéticas y es preciso para ello emplear antenas.
- Medios de transmisión por **infrarrojos**:
  Es aquel que emplean luz óptica para transmitir (pero usando el aire y no un cable como la fibra óptica). Para ello deberán emplearse en sus extremos fotoemisores y fotodetectores.

Dentro de cada una de ellas existirán diferentes implementaciones que veremos a continuación.
La transmisión no guiada se caracteriza por transmitir la información empleando como medio de transmisión el aire, el mar o el vacío.
No emplea ningún elemento físico (como un cable) para 'guiar y encapsular' la información a transmitir.
De los medios de transmisión anteriormente descritos (aire, mar o vacío), el más empleado para transmitir datos es el aire.
Por el aire podemos transmitir ondas electromagnéticas (transmisiones radio) o luz óptica (transmisión por infrarrojos).
La más habitual es la transmisión radioeléctrica, ya que es una tecnología que admite numerosas implementaciones tanto a corta, media y larga distancia.
En cambio, la transmisión por infrarrojos (por su naturaleza) se emplea para distancias cortas y para determinadas aplicaciones comerciales.
Veremos a continuación las características de transmisión de cada una de ellas.

Transmisión radioeléctrica:
En este tipo de transmisión se emplean señales de radio para transmitir la información.
Están basadas en las ondas electromagnéticas. En ellas existe un elemento que radia energía (una antena emisora) y otra que recibe o capta esa energía radiada (una antena receptora).
Las antenas son por tanto dispositivos que radian y capturan ondas electromagnéticas y son capaces de traducirlas a señales de voltaje.
El proceso de transmisión de la onda electromagnética es sencillo:
Una carga eléctrica en movimiento genera un campo magnético y un campo eléctrico. La antena es un dispositivo en el que se producen corrientes eléctricas (por diferencia de voltajes) y como consecuencia radian estos campos magnéticos y eléctricos que serán proporcionales a la intensidad de la corriente eléctrica.
Estas ondas electromagnéticas (suma de eléctrica y magnética) en teoría se propagan hasta el infinito aunque el aire introduce atenuación.
Cuando estas ondas electromagnéticas llegan a otro dispositivo que está conectado a un circuito eléctrico (antena receptora) producirá una fuerza electromotriz que obliga a los electrones del dispositivo a moverse generando una corriente que será proporcional a la intensidad y frecuencia de la señal electromagnética radiada.
Así es como se produce la transmisión por señales electromagnéticas.

Una de las características de las ondas electromagnéticas es que su potencial es inversamente proporcional al cubo de la distancia recorrida por el aire ($E \alpha (1 / d^3)$. Esto quiere decir que su energía se pierde por la distancia según esa fórmula.
Estas ondas se caracterizan también porque pueden 'traspasar' los obstáculos (edificios, montañas, bosques, etc.) sin problema, aunque con ello sufra atenuación.
Esta atenuación aumenta cuanto mayor es la frecuencia de la onda de radio. De hecho, a altas frecuencias la lluvia y el agua pueden absorber dichas ondas electromagnéticas.

Transmisión por infrarrojos:
En este tipo de transmisión se emplean señales ópticas para transmitir la información.
Como medio de transmisión se emplea el aire, y en los extremos se instalan equipos fotoemisores de luz óptica y equipos fotodetectores de luz óptica.
La señal óptica que se transmite se emite a una determinada longitud de onda (un equivalente a la frecuencia en las ondas electromagnéticas).
Una característica de este tipo de transmisión es que ambos extremos (fotoemisor y fotodetector) deben tener visibilidad directa, es decir, deben estar alineados y sin obstáculos para que la transmisión pueda efectuarse.
Este tipo de transmisión se emplea para transmitir a altas velocidades, pero en distancias cortas y siempre con visibilidad.
Un ejemplo de este tipo de transmisión es el del mando a distancia del televisor.

4.2. Frecuencias de transmisión inalámbricas

Como se ha descrito anteriormente, las ondas electromagnéticas se emiten y se propagan a diferentes frecuencias.
Así se clasifican las ondas electromagnéticas, en función de la frecuencia en la que trabajan y dónde se han establecido.
Podemos verlo en la siguiente tabla:

Frecuencia	Tipo de onda de:	Banda
3 – 30 Khz	Muy baja frecuencia	VLF
30 – 300 Khz	Baja frecuencia	LF
300 – 3000 Khz	Media frecuencia	MF
3 – 30 Mhz	Alta frecuencia	HF
30 – 300 Mhz	Muy alta frecuencia	VHF
300 – 3000 Mhz	Ultra frecuencia	UHF
3 – 30 Ghz	Super alta frecuencia	SHF
30 – 300 Ghz	Extra alta frecuencia	EHF

Todo el conjunto de frecuencias forman lo que se denomina espectro radioeléctrico, que está regulado por instituciones y organismos gubernamentales e internacionales.
Cada servicio de telecomunicación (radio comercial, televisión terrestre, datos por satélite, etc.) se transmite en un tipo de frecuencia determinada, ya que cada banda de frecuencia tiene determinadas características que la hace adecuada para transmitir un tipo de servicio de telecomunicación u otro.
Veremos a continuación y con más detalle los servicios de telecomunicaciones que utilizan cada banda de frecuencias.

- Banda **VLF**:
  Esta banda de frecuencias es la que se corresponde con las ondas de radio con frecuencias entre 3 y 30 Khz y corresponde con longitudes de onda entre 100 km y 10 km.
  Estas ondas se propagan por la superficie de la tierra con muy baja atenuación y por ello se puede realizar enlaces de grandes distancias.
  Se emplea para servicios geofísicos, radioayudas, comunicación submarina, etc.
  Presenta como gran inconveniente el escaso ancho de banda (apenas 30 Khz) y que las antenas necesarias deben ser muy grandes. Todo esto provoca que el sistema sea ineficiente.
- Banda **LF**:
  Esta banda de frecuencias es la que se corresponde con las ondas de radio con frecuencias entre 30 y 300 Khz y corresponde con longitudes de onda entre 10 km y 1 km.
  Estas ondas se propagan por tener una baja atenuación que le permite realizar enlaces de grandes distancias.
  Es la banda habitual para las comunicaciones marítimas y aéreas y determinados servicios meteorológicos.
  También se usa en determinados servicios de radiodifusión como la radio AM que trabaja en la banda 148,5 y 283,5 kHz.
  También en esta banda de frecuencias existe una sub-banda que comprende desde 135.7 a 137.8 kHz que se ha destinado para radioaficionados.
  Su principal inconveniente es un escaso ancho de banda (del orden de khz) y como gran ventaja es su largo alcance para la transmisión.
- Banda **MF**:
  Esta banda de frecuencias es la que se corresponde con las ondas de radio con frecuencias entre 300 y 3000 Khz y con longitudes de onda entre 1 km y 100 m.
  A menudo se conoce esta banda como la banda media. Estas ondas se propagan siguiendo la curvatura de la tierra y reflejándose en la ionosfera.
  Su atenuación es baja y pueden alcanzarse largas distancias, sobre todo por la noche que desaparece la capa D de la ionosfera (absorbe fuertemente las ondas de estas frecuencias) y con ello se alcanzan mayores distancias.
  En esta banda se distribuye el servicio de radiodifusión AM (frecuencias desde 535 a 1705 kHz) y también en esta banda está una sub-banda para los radioaficionados cuyas frecuencias van desde los 800 Khz hasta los 2000 Khz.
  También determinados servicios de radioayuda como los radiofaros usan frecuencias de esta banda.
- Banda **HF**:
  Esta banda de frecuencias es la que se corresponde con las ondas de radio con frecuencias entre 3 y 30 Mhz y con longitudes de onda entre 100 m y 10 m.
  Estas ondas se propagan por el rebote de las ondas en las diferentes capas de la atmósfera (troposfera, ionosfera, etc.) alcanzándose mayores distancias por la noche que por el día.
  Es un tipo de onda fuertemente sensible a variaciones climáticas, de ruido, de temperatura, etc.
  Existen determinadas sub-bandas para radioaficionados y para comunicaciones militares.
  Esta banda fue una de las primeras utilizadas para servicios de telecomunicaciones cuando aparecieron las primeras transmisiones por radio.

- Banda **VHF**:
  Esta banda de frecuencias es la que se corresponde con las ondas de radio con frecuencia entre 30 y 300 Mhz y con longitudes de onda entre 10 y 1 m.
  Esta es una banda muy utilizada por muchos servicios de telecomunicaciones sobre todo de radiodifusión.
  En esta banda se encuentra el servicio de FM (87,5 hasta los 108 Mhz), la radio digital DAB (en la banda de los 173 a los 205 Mhz), muchos canales de televisión (canales del 2 al 14 aunque hoy día ya en desaparición por la TDT) y comunicaciones aéreas (108 a 136,97 Mhz) entre otros.
  En esta banda también hay determinadas frecuencias asignadas para los servicios de emergencias y servicios de uso civil como radio-taxis, etc.
  En estas frecuencias las ondas se transmiten por la superficie de la tierra (de ahí el empleo de estaciones emisoras y receptoras en montañas y puntos estratégicos) aunque a medida que se sube en frecuencia para adquiriendo importancia la propagación aérea.
- Banda **UHF**:
  Esta banda de frecuencias es la que se corresponde con las ondas de radio con frecuencias entre 300 y 3000 Mhz y con longitudes de onda entre 100 y 10 cm.
  Esta es una de las bandas más utilizadas comercialmente por numerosos servicios de radiodifusión.
  En esta banda se encuentra el servicio de televisión TDT (frecuencias desde el 475 Mhz hasta los 862 Mhz), los nuevos servicios de telefonía móvil (alrededor de los 900 Mhz), identificación RFID (desde los 860 hasta los 960 Mhz) entre otros.
  Es la banda también que usa el horno-microondas para calentar (alrededor de los 2 Ghz), de los sistemas GPS, del servicio de Bluetooth, etc.
  En estas frecuencias las ondas se transmiten por la superficie de la tierra aunque sufren fuertes atenuaciones por los efectos climáticos y ello implica que el alcance sea reducido y por ello deban emplearse reemisores.
- Banda **SHF**:
  Esta banda de frecuencias es la que se corresponde con las ondas de radio con frecuencias entre 3 y 30 Ghz y con longitudes de onda entre 10 y 1 cm.
  Esta es una de las bandas también ampliamente utilizadas por numerosos servicios de telecomunicaciones.
  En esta banda se encuentran los servicios de radiodifusión por satélite de radio y televisión, las comunicaciones por microondas, servicios de astronomía, redes inalámbricas de datos de alta velocidad (Wimax), servicios de radar, etc.
  En esta banda, la señal se atenúa mucho con la distancia y cualquier obstáculo o fenómeno climatológico afecta a la señal. En cambio, como gran ventaja que se obtiene es su gran ancho de banda (del orden de Mhz y Ghz).
  Otra de las características de este tipo de comunicaciones es que precisa de visibilidad directa para poder realizar la transmisión.
- Banda **EHF**:
  Esta banda de frecuencias es la que se corresponde con las ondas de radio con frecuencias entre 30 y 300 Ghz y con longitudes de onda entre 1000 y 100 mm.
  Dado que su longitud de onda es del orden de mm a esta banda también se le conoce como banda de las milimétricas.
  En esta banda las ondas sufren una fuerte atenuación con las distancias y obstáculos que hacen que sólo se pueda emplear para determinados servicios (pero no de radiodifusión) como comunicaciones por microondas, teledetección, radioastronomía y servicios de transmisión experimentales.
  En esta banda también se encuentran numerosos servicios de comunicaciones militares.
  Otra de las características de este tipo de comunicaciones, al igual que la banda SHF, es que precisa de visibilidad directa para poder realizar la transmisión.

Transmisión por infrarrojos:

Como ya se ha descrito anteriormente otro gran grupo de transmisiones inalámbricas son las transmisiones por infrarrojos.

En el caso de transmisiones por infrarrojos no hablamos de frecuencias, sino de longitudes de onda (λ) y se mide en metros.

Existe una relación entre la longitud de onda y la frecuencia dada por la siguiente fórmula:

$$\lambda = \frac{c}{f}$$

siendo c la velocidad de la luz (3 x 10^8 m/seg) y f la frecuencia medida en Hz.

Al igual que las frecuencias, existe lo que se denomina un espectro de longitud de onda de forma que en cada longitud de onda se emite un determinado servicio.

En este caso no se habla de banda de frecuencias sino de ventanas de longitud de onda.

Así estas ventanas están relacionadas con las bandas de frecuencias por la fórmula anterior.

La transmisión por infrarrojos se caracteriza por transmitir en la banda de infrarrojos cuya ventana va desde 0,7 a los 100 µm.

En la radiación infrarroja generalmente se emite calor por lo que a veces se usa para detección de cuerpos.

Esta ventana de las infrarrojas es usada por sistemas de comunicaciones para transmitir información, empleando un diodo led o láser que emite onda de luz que representa información codificada. En el receptor se emplean fotodetectores que captan están luz óptica y la decodifican.

La transmisión por infrarrojas sufre desde hace años numerosas investigaciones para su utilización para comunicaciones de datos a corto alcance. Una de ellas es su utilización para comunicar equipos (red LAN) cercanos entre sí (a pocos metros).

No obstante su gran competidor ha sido el nuevo estándar Wifi que permite alcanzar grandes velocidades de transferencia y a diferencia de las transmisión infrarroja no precisa de visibilidad directa.

4.3. Antenas

Una antena es un dispositivo (generalmente metálico) capaz de emitir y captar señales radioeléctricas.

En esencia una antena no es más que un transductor o conversor que traduce señales eléctricas en señales de radio (antena emisora) u ondas de radio en señales eléctricas (antena receptora).

En base lo anterior, existen dos tipos de antenas.

- Antena emisora.
- Antena receptora.

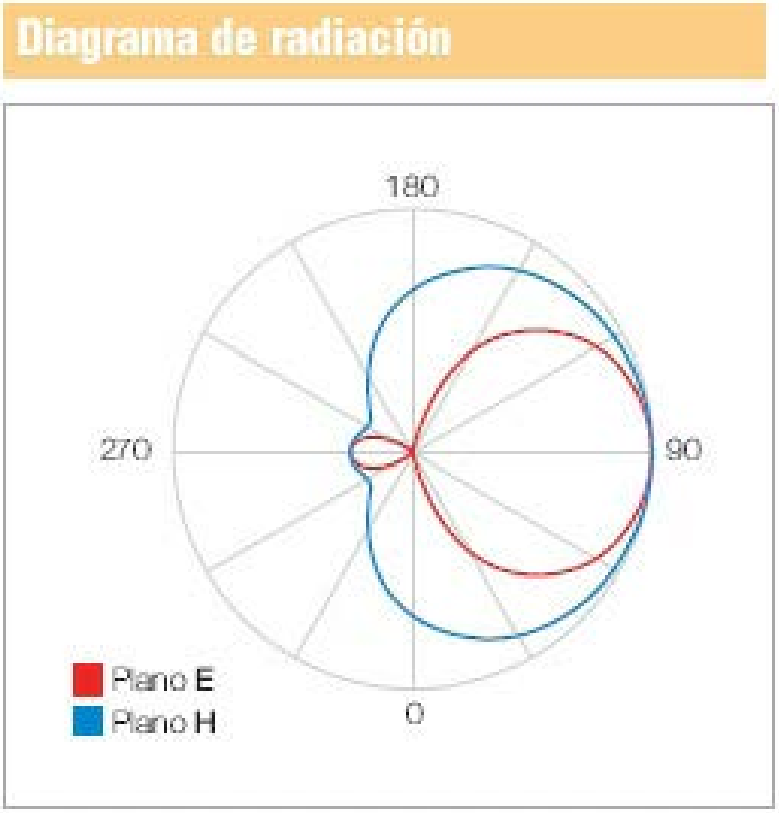
Es habitual que existan antenas capaces de emitir y captar señales radioeléctricas.

Las antenas deben siempre estar ubicadas en espacios libres para poder emitir y recibir señales sin presencia de obstáculos (por ello se ubican generalmente en las cubiertas de los edificios).

Como ya se ha visto anteriormente hay muchos tipos de ondas radioeléctricas, cada una trabajando en una banda de frecuencias de trabajo y con unas características propias.
Es por ello que existen numerosos tipos de antenas, cada una adaptada a una banda de trabajo, ya que en definitiva la antena debe estar adaptada a la señal de radio que debe emitir o recibir.
Por ello, una antena de UHF sólo es capaz de emitir y recibir señales de radio que viajan en esa banda de frecuencias, y por ello esta antena no será capaz de emitir o recibir señales de otras frecuencias o bandas, como por ejemplo de la banda SHF.
Independientemente del tipo de antena, todas ellas presentan una serie de parámetros que son comunes y que caracterizan las prestaciones del dispositivo.
Veremos a continuación los parámetros más relevantes que caracterizan a una antena (emisora o receptora).

Ganancia de una antena:
Una antena que emite su señal en todas direcciones por igual es una antena isotrópica (balón de futbol). Su diagrama de radiación es una esfera perfecta. Por convenio decimos que tiene ganancia 0 dB.
Las antenas reales nunca son isotrópicas, siempre envían más señal en una dirección que en otra.
Definimos entonces la ganancia como la relación existente entre la señal entregada por una antena con respecto a la entrega por una antena de isotrópica (antena dipolo elemental).
Es una magnitud que se mide en decibelios (dB).
Siempre se buscan antenas con mayor ganancia.
También se tiene que tener en cuenta que la ganancia suele variar con la frecuencia, presentando la antena ganancias diferentes a distintas frecuencias dentro de la banda de trabajo.
Este vídeo explica el funcionamiento de una antena (es un poco "espeso") https://youtu.be/WrTw61sxNH8

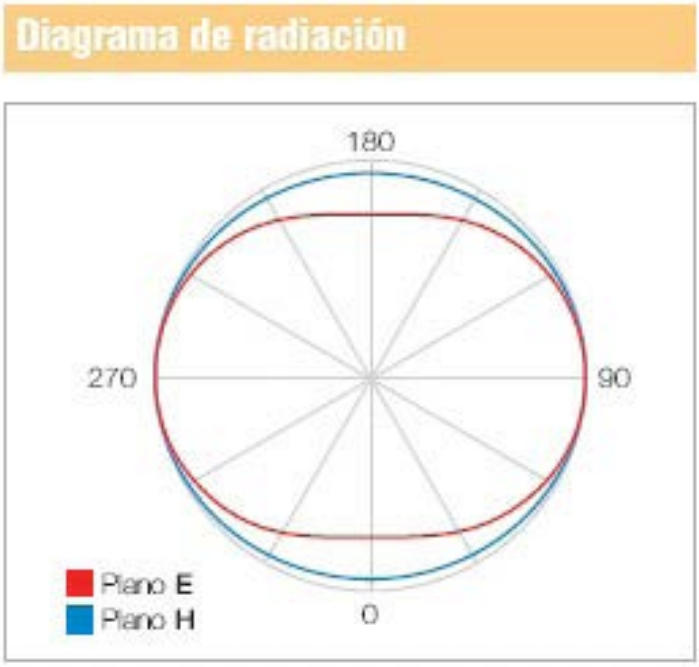
Diagrama de radiación de una antena:
Es una representación gráfica de una antena receptora o emisora en el eje vertical y horizontal que indica en qué direcciones (medida en grados) la antena tiene mayor ganancia para emitir o recibir.



En base a lo anterior, las antenas admiten una primera clasificación:

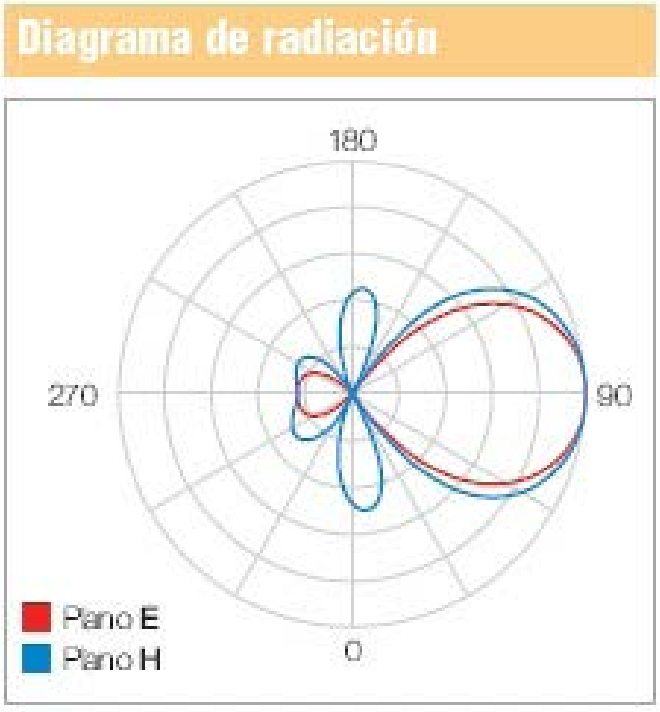
Antenas omnidireccionales:

Son aquellas capaces de emitir y recibir en todas las direcciones. Su diagrama de radiación tendrá un aspecto como la siguiente.



Antenas direccionales o directivas:

Son aquellas que emiten o reciben en una determinada dirección. Su diagrama de radiación tendrá un aspecto como la siguiente. (plano H-horizontal y plano E-vertical)



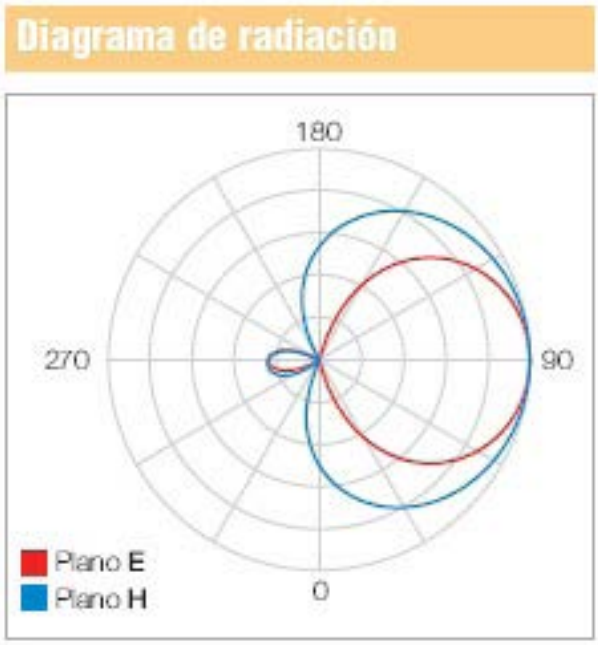
Analizando el diagrama de radiación de una antena podemos determinar varios parámetros de la antena:

- Si es directiva o no y en qué ángulos presenta esa directividad.
- La ganancia de la antena:
  Con el valor máximo del lóbulo principal medido en dB.
- La relación delante/detrás:
  Es un parámetro que veremos a continuación y que representa la relación entre la ganancia del lóbulo principal con respecto a la del lóbulo secundario.

Todas estas magnitudes son esenciales para la elección de una antena en función del servicio de telecomunicaciones que se quiera transmitir (radio, televisión, datos, etc).

Directividad

Indica la capacidad de una antena en emitir y recibir en una determinada dirección.
Se obtiene del análisis del diagrama de radiación.
Para ellos debemos observar el lóbulo principal y su valor máximo y 'grosor' nos indica el valor de ganancia y su directividad en grados en el plano horizontal y vertical respectivamente.
Para algunos servicios de telecomunicación, será necesarios utilizar antenas más o menos directivas (por ejemplo en las de televisión TDT) y en otras no (por ejemplo las de radio).



Relación delante/atrás

Es la relación o cociente entre la ganancia que presenta el lóbulo principal con respecto al segundo lóbulo con mayor ganancia.
Está relacionado con la directividad. Cuanto mayor sea la relación más directiva es la antena.
Esto se debe a que la antena, aunque emita o reciba en una dirección principal, también emite o recibe en otras direcciones (generalmente por detrás de la dirección principal) y que afectan a la ganancia de la antena para la señal deseada.

Ancho de banda

Indica el rango de frecuencias en el que trabaja la antena.
Así encontramos antenas que trabajan en la banda de UHF, en la banda de VHF, en la banda de LF, etc.

ROE

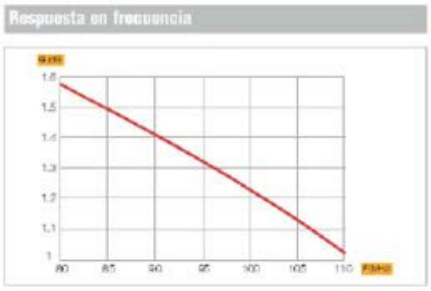
Es un parámetro que indica el valor de adaptación de la antena con respecto a la impedancia al sistema que está conectado a ella.

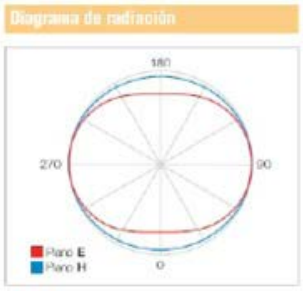
Es un parámetro adimensional pero que indica la probabilidad de la antena de generar ondas estacionarias (ondas espurias) que afectan a la ganancia y prestaciones de la antena con respecto a la señal deseada a emitir o recibir.
El fabricante de una antena proporciona siempre las características de dicha antena. Analizando dichas especificaciones podemos obtener todos los parámetros anteriormente descritos.

Veamos un **ejemplo**.
Dada la siguiente antena y su hoja de especificaciones dada por el fabricante.
Se pide que:

- ⇨ Indica si es una antena directiva o omnidireccional.
- ⇨ La ganancia de la antena.
- ⇨ La ganancia a la frecuencia de 100 Mhz.

Referencias			1201
Banda			FM
Ganancia		dB	1
Relación D/A			0
Longitud		mm	500
Carga al viento	800 N/m²	N	27
	1100 N/m²		37





Solución:
Del análisis de los datos anteriores podemos responder a las cuestiones que nos plantea.

- ⇨ Podemos observar del diagrama de radiación que la antena emite o recibe en todas las direcciones (no existe un lóbulo principal), luego la antena es **omnidireccional**.
- ⇨ La ganancia de la antena la proporciona el propio fabricante, es decir, **G = 1 dB**.
- ⇨ La antena proporciona una ganancia variable con la frecuencia en la banda de trabajo (todas las antenas tienen estas características).
  De la respuesta en frecuencia de la antena podemos observar que a la frecuencia de f=100 Mhz la antena presenta una ganancia de 1,25 dB que es el dato que nos piden.

Vemos que efectivamente la antena trabaja en la banda de FM comercial ya que su ganancia comprende desde la frecuencia de los 80 Mhz hasta los 110 Mhz que engloba a la banda de FM (87,5 Mhz a los 108 Mhz).

A continuación, vamos a ver diferentes tipos de antenas junto con las características principales que la definen y para qué tipo de servicio se emplean.
Como ya se ha descrito anteriormente, la antena debe adaptase a la señal que emite o recibe y son diferentes en su fabricación y sus parámetros dependiendo de la frecuencia en la que trabaja.
Aunque la variedad de antenas es muy amplia aquí resaltaremos algunas de las más utilizadas destacando las siguientes:

- Antena de FM.
- Antena de UHF.
- Antena parabólica.
- Antena de Wifi.

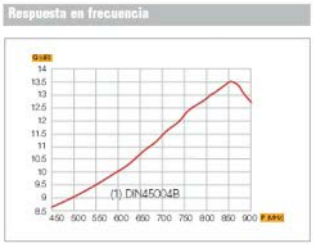
Las vemos a continuación con más detalle.

Antena de FM:
Se trata de un tipo de antena capaz de trabajar en la banda de FM comercial, es decir, desde la frecuencia 87,5 Mhz hasta los 108 Mhz.
Suelen ser antenas circulares con un diagrama de radiación omnidireccional.
En la siguiente imagen podemos ver un ejemplo de dicha antena y sus parámetros.

Antena de UHF:
Se trata de un tipo de antena capaz de trabajar en la banda de UHF comercial, es decir, desde la frecuencia 470 Mhz hasta los 862 Mhz.
Corresponde a los canales 21 a 69 del espectro radioeléctrico y en ellos se transmite la señal de televisión terrestre (TDT).
Por tanto dicha antena está preparada para recibir señales de televisión comerciales.
Son las antenas típicas de los edificios para la recepción de la televisión convencional.
Se caracterizan por ser antenas de tipo yagi, es decir, son un conjunto de dipolos dispuestos de forma paralela (cuantos más dipolos mayor ganancia) y son directivas para obtener mayor ganancia. Es por ello que deben estar alineados con respecto al reemisor o repetidor de televisión.
Por tanto su diagrama de radiación presenta un lóbulo principal que indica en qué ángulos la antena presenta mayor ganancia.
En la siguiente imagen podemos ver un ejemplo de antena de UHF junto con las especificaciones dadas por el fabricante.

Referencias			1121
Canal			21-69
Ganancia		dB	12
Relación D/A			26
Longitud		mm	1180
Carga al viento	800 N/m²	N	73
	1100 N/m²		100.3

Presión de viento	N/m²	800	1100
Velocidad de viento	Km/h	130	150



En este tipo de antena es importante la ganancia que presenta y su directividad ya que en entornos de difícil recepción o de señales muy débiles, es preciso tener antenas de gran ganancia y alta directividad.
También dichas antenas ya que cubre una banda de frecuencias amplia (desde la 470 Mhz hasta los 862 Mhz) presentan una respuesta en frecuencia que se debe tener en cuenta para determinados canales de televisión.
El mercado ofrece un amplio abanico para este tipo de antenas cada uno adecuado para un tipo de ubicación (edificios, campings, etc.) y en función de los niveles de recepción existente en la ubicación.

Antena parabólica:
Se trata de un tipo de antena capaz de captar las señales procedentes de los satélites.
Estas señales trabajan en el rango de las frecuencias de los Ghz (alrededor de los 10 y 11 Ghz) y son señales muy débiles por lo que este tipo de antena lo forma un reflector parabólico (es la propia parábola en sí) y un conversor LNB.
El objetivo de la parábola es capturar estas débiles señales y focalizarlas hacia un punto: el foco de la antena donde se encuentra el conversor LNB.
El conversor LNB no es más que un conversor de frecuencias que baja las frecuencias de los 10 Ghz a la frecuencia de FI (alrededor de los 1 y 2 Ghz) que es la señal que se distribuye.
Aunque las antenas parabólicas pueden usarse para numerosos servicios es muy habitual usarlas para la recepción de los canales de radio y televisión comerciales y por ello se instalan en numerosos edificios.
Uno de los parámetros básicos de una antena parabólica es su diámetro ya que a mayor diámetro mayor ganancia presenta, o lo que es lo mismo, es capaz de captar señales más débiles o de mayor lejanía.
Por eso para entornos ruidosos se emplean parabólicas de mayor tamaño.
En la siguiente imagen podemos ver un ejemplo de antena parabólica junto con las especificaciones dadas por el fabricante.

MODELO		PO 064	PO 081	DPO 105*
Referencia		86064	86081	86105
Diámetro	cm	51 x 57	73 x 80	91 x 100
Distancia focal	cm	32,7	46,8	58,3
Reflector tipo		Offset		
Material		Acero electrozincado		
Recubrimiento		Poliéster		
Tipo de fijación		Suelo / Pared / Mástil		Mástil
Ø mástil	mm	30 ÷ 60	30 ÷ 60	30 ÷ 60
Elevación	º	17 ÷ 55	17 ÷ 55	- 5 ÷ 82
Ángulo Offset	º	19		
Azimut	º	180		
Fijación LNB Ø	mm	25 ÷ 40		
Frecuencia	GHz	10 ÷ 12,75		
Ganancia (11,7 Ghz)	dB	35	38	39,2
Rendimiento	%	>60		
Ángulo de apertura (- 3 dB)	º	2,8	2,4	2,1
Relación F/D		0,64		
Carga al viento		Operacional: hasta 100 km/h Supervivencia: hasta 130 km/h		
Dimensiones embalaje	mm	610 x 610 x 110	830 x 840 x 120	1020 x 1000 x 120
Peso	Kg	5	9	10

Como ya se ha comentado anteriormente, lo más importante a destacar es su diámetro (proporciona ganancia) y la ganancia del conversor LNB (que es quien finalmente amplifica la señal antes de su distribución).
Existen dos tipos de parabólicas:

- Las de foco centrado:
  El foco está centrado en el centro de la parábola y con ello presenta un sombra que baja la ganancia y eficiencia de la antena. Está en desuso.
- Las de offset:
  El foco está desplazado con objeto de no crear 'sombras' y con ello se mejora la ganancia y la eficiencia de la antena. Son las usadas actualmente.

Antena Wifi:
Wifi se entiende como una tecnología capaz de emitir y recibir en una banda de frecuencias del espectro radioeléctrico que no está regulado, es decir, está libre.
Esta banda es usada por numerosos particulares, organizaciones y empresas para transmitir información (generalmente datos) y no tener que abonar las tasas por uso del espectro radioeléctrico.
Actualmente, es un tipo de tecnología muy madura en la cual numerosos dispositivos son compatibles para transmitir en esta banda: ordenadores, smartphones, tablets, etc.
La banda Wifi comprende las frecuencias de los 2,4 Ghz aunque existen también la banda de los 5 Ghz.
Existen numerosos estándares para la interoperabilidad en esta banda definidas en la normas 802.11 a) b) c) g) y n) entre otras.
Las antenas que operan en esta banda deben estar adaptadas a estas frecuencias y hay en el mercado una amplia gama de antenas Wifi.
En la siguiente imagen podemos ver un ejemplo de una antena Wifi.

Este tipo de antena se caracteriza por estar formada generalmente por un dipolo de tipo omnidireccional (emite en todas las direcciones).
El ejemplo más claro son las antenas de los router Wifi para las redes locales domésticas.
Pero también existen antenas Wifi directivas para enlaces de datos a largas distancias.
Este tipo de antenas presenta una tipología diferente a la anterior ya que se busca mayor ganancia y directividad (son antenas directivas y no omnidireccionales).

Veamos un **ejemplo**.
Se quiere realizar un radioenlace en la frecuencia de los 2,4 Ghz (banda Wifi) y para ello se emplea dos antenas: una en emisión y otra en recepción cuya banda de trabajo cubre los 2,4 Ghz.
Sabiendo que la ganancia de la antena de emisión es de 14 dB y que la atenuación que introduce el trayecto con una distancia de 2 Km es de 35 dB, se pide calcular la ganancia mínima que debe tener la antena receptora para poder demodular la señal recibida, sabiendo que para ello el nivel mínimo de señal recibida debe ser de 24 dBµV y que la señal emitida (antes de ser radiada) es de 30 dBµV.
Para resolver el problema dibuje un croquis del radioenlace.
Solución:
En base a los datos que nos aporta, realizamos en primer lugar el esquema de la transmisión:

En base al esquema anterior podemos establecer la siguiente ecuación:

$$Nivel_{señal\ emitida} + G_{antena\ emisora} - Atenuación_{trayecto} + G_{antena\ receptora} = Nivel_{señal\ recibida}$$

En la ecuación anterior podemos ver que las ganancias de ambas antenas suman tensión a la señal emitida y el trayecto resta tensión a la señal emitida. Sustituimos valores:

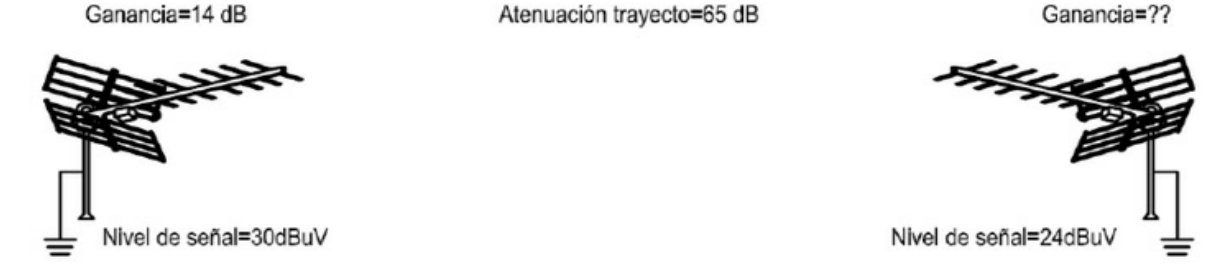
$$30\ dB\mu V + 14\ dB - 35\ dB + G_{antena\ receptora} = 24\ dB\mu V$$

Despejando el valor de ganancia de la antena receptora nos da el resultado solicitado:

$$G_{antena\ receptora} = 15\ dB$$

Se trata de un valor mínimo de ganancia para la antena.

Veamos otro **ejemplo**.
Partiendo de los mismos datos del ejemplo anterior, ahora se quiere realizar el radioenlace para una distancia de 5 km por lo que ahora la atenuación introducida por el trayecto es de 65 dB. Con los mismos parámetros anteriores de nivel de señal y ganancia de antena emisora, calcula la ganancia mínima necesaria para la antena receptora para que pueda demodularse la señal recibida.
Calcula asimismo el tamaño que deben tener las antenas (emisoras y receptoras) sabiendo que para que puedan funcionar su longitud debe ser al menos la mitad de la longitud de onda de la frecuencia en la que trabaja.
Solución:
Realizamos de nuevo el esquema de la transmisión:



Establecemos de nuevo la fórmula de ganancias y atenuaciones del radioenlace:

$$Nivel_{señal\ emitida} + G_{antena\ emisora} - Atenuación_{trayecto} + G_{antena\ receptora} = Nivel_{señal\ recibida}$$

Sustituyendo valores donde en este caso la atenuación del trayecto es mayor (mayor distancia) obtenemos:

$$30\ dB\mu V + 14\ dB - 65\ dB + G_{antena\ receptora} = 24\ dB\mu V$$

Despejando el valor de ganancia de la antena receptora nos da el resultado solicitado:

$$G_{antena\ receptora} = 45\ dB$$

Es decir, se necesita una antena de mayor ganancia para poder demodular la señal recibida. Como en el caso anterior se trata de un valor mínimo de ganancia de antena receptora.

Para calcular la longitud de la antena, aplicamos la relación que enlaza la longitud de onda con la frecuencia, es decir:

$$\lambda = \frac{c}{f}$$

Con lo que sabiendo que c= 3 x 10^8 m/seg y f= 2,4 Ghz se obtiene que:

$$\lambda = \frac{3\ x\ 10^8}{2{,}4\ x\ 10^9} = 0{,}125\ \text{m}\ =\ 12{,}5\ \text{cm}$$

Luego la longitud de la antena debe ser λ / 2, es decir:

Longitud antena = **6, 2 cm**

Observamos que esta es la longitud que normalmente suelen tener las antenas Wifi.

4.4. Microondas terrestres y por satélite

Anteriormente se ha visto el espectro radioeléctrico y cómo se divide en bandas de frecuencias donde en cada una de ellas se transmite uno u otro servicio de telecomunicaciones.

No obstante, en este espectro radioeléctrico se habla de tres regiones:

Región	Frecuencias
Banda de las microondas	Desde los 2 Ghz hasta los 40 Ghz
Banda de las ondas de radio	Desde los 30 Mhz hasta 1 Ghz.
Banda de los infrarrojos	Desde los 3 x 1011 a los 400 Thz

Estas bandas tienen especial importancia, puesto que en ellas es donde se concentran la mayoría de las transmisiones de datos para los diferentes servicios de telecomunicaciones que se emplean en la actualidad.

Entraremos ahora con más detalle en las características de cada una de ellas y qué servicios emplean estas frecuencias para las transmisiones.

La banda de las microondas, como se ha comentado anteriormente, comprende aquellas frecuencias que van desde los 2 Ghz hasta los 40 Ghz.

Se trata de una banda en la que se emplean antenas muy direccionales y se emplean para servicios de comunicaciones terrestres y por satélite.

Esta banda es importante porque es empleada para transmitir datos a alta velocidad (la tecnología Wifi está en esta banda de frecuencias).

Existen dos tipos:

- Microondas terrestres.
- Microondas por satélite.

Aunque ambas emplean las mismas frecuencias, su implementación es diferente y son adecuadas uno u otro en función del servicio que se quiere transmitir.

Microondas terrestres:
Se suelen emplear para transmitir servicios de televisión, telefonía y datos a largo alcance.
Emplean antenas parabólicas las cuales deben tener visibilidad directa para la conexión. Se pueden alcanzar grandes distancias con el empleo de conexiones intermedias punto a punto entre antenas parabólicas.
La gran ventaja es su rápida implementación con respecto a implementar dicha conexión con cualquiera de los medios de transmisión guiados, que precisan tirar el cable.
Su principal inconveniente son las pérdidas por el aire, cuya atenuación aumenta con el cuadrado de la distancia frente a una atenuación logarítmica con los medios guiados como el cable coaxial y par trenzado, es decir, su atenuación viene dada por la siguiente expresión.

$$\text{Atenuación espacio libre (dB)} = 10 \times \log \left(\frac{4\pi d}{\lambda}\right)^2$$

Siendo d la distancia en metros que separa el enlace.
Además, esta atenuación es mayor en condiciones climatológicas adversas como por ejemplo lluvia.

Microondas por satélite:
También se emplean para transmitir televisión, telefonía y datos a largo alcance pero empleando los satélites como repetidores.
El satélite recibe la señal, la amplifica y la retransmite de nuevo a la tierra. Para ello usan las antenas terrestres (que deben ser parabólicas) y el satélite deben estar perfectamente alineados y ello obliga al satélite a ser geoestacionario.
El rango de frecuencias para la recepción del satélite debe ser diferente del rango al que este emite, para que no haya interferencias entre las señales que ascienden y las que descienden.
Debido a que la señal tarda un pequeño intervalo de tiempo desde que sale del emisor en la Tierra hasta que es devuelta al receptor o receptores, ha de tenerse cuidado con el control de errores y de flujo de la señal.
Se emplean mucho para redes privadas de datos (VSAT).

4.5. Enlace punto a punto por satélite

Un enlace punto a punto por satélite no es más que una conexión inalámbrica en la cual una antena en la tierra (generalmente una parabólica) se conecta con un satélite (geoestacionario) para establecer un enlace y transmitir información (generalmente datos aunque también puede ser telefonía, radio, etc).
Como en toda comunicación satelital que se ha descrito anteriormente, antena y satélite deben estar perfectamente alineados para poder realizar la conexión.
El diámetro de la antena parabólica dependerá en gran medida de la frecuencia de la portadora que se empleará para transmitir la información, la distancia al satélite y las condiciones de propagación.
Así, si la distancia antena-satélite es mayor o si las condiciones atmosférica son muy adversas (introduce mayor atenuación) se necesitarán parabólicas de mayor tamaño para garantizar los niveles de señal suficiente para establecer la conexión.

4.6. Multidifusión por satélite

Las comunicaciones vía satélite permiten establecer comunicaciones entre diversos puntos de la tierra (generalmente muy alejados entre sí) empleando como repetidor un satélite.
La gran ventaja del uso de satélite es su gran cobertura, es decir, permite llegar a una amplia zona de la tierra y a zonas remotas que no podrían ser alcanzadas bajo otro sistema.
El repetidor, como se ha descrito, es el satélite, que actuaría como hub, mientras que los emisores y receptores sería antenas parabólicas situadas en diversos puntos de la tierra.
Esto es lo que formaría una red VSAT.
Este tipo de redes VSAT son cada día más empleadas por numerosas empresas que quieren establecer redes de datos propias a nivel mundial. Aunque su coste hoy día sigue siendo alto, es asumible para grandes empresas.
La ventaja de una estación terrestre de VSAT sobre una conexión de red terrestre típica, es que las VSAT no están limitadas por el alcance de un sistema cableado. Una estación terrestre de VSAT puede instalarse en

cualquier parte, sólo requiere ser vista por el satélite. Existe otro tipo de ventajas relacionadas con el bajo costo de operación, la mayor facilidad de expansión de la red y sobre todo, como se ha indicado antes, la instalación en lugares donde es difícil llegar con instalaciones de cable.

4.7. Radio

La radio se caracteriza por ser un medio de transmisión no guiado basado en la propagación de ondas radioeléctricas.
Las ondas radioeléctricas son campos de energía eléctrica y magnética capaces de transmitirse y representar información.
A través de estas ondas de radio podemos distribuir numerosos servicios de telecomunicaciones como radio comercial, televisión, transmisión de datos, señalización aérea y marítima, etc.
La principal característica y ventaja de la radio es su movilidad, es decir, a diferencia de un sistema cableado permite al usuario disponer de equipos portátiles y no con ello pierde la conectividad con el sistema.
La radio ha experimentado en los últimos años un fuerte avance en sus comunicaciones al ser uno de los medios más empleados para transmisión de datos.

4.8. Infrarrojos

Las comunicaciones por infrarrojos se caracterizan por transmitir datos empleando la banda de infrarrojos del espectro.
Basa su funcionamiento en impulsos ópticos que hoy día permiten altas tasas binarias de transmisión.
Como medio de transmisión se emplea el aire y en los extremos se instalan equipos fotoemisores de luz óptica y equipos fotodetectores de luz óptica.
La señal óptica que se transmite se emite a una determinada longitud de onda (un equivalente a la frecuencia en las ondas electromagnéticas).
Una característica de este tipo de transmisión es que ambos extremos (fotoemisor y fotodetector) deben tener visibilidad directa, es decir, deben estar alineados y sin obstáculos para que la transmisión pueda efectuarse.
Se emplea para transmitir a altas velocidades pero en distancias cortas y siempre con visibilidad.
Hoy día hay numerosas líneas de investigación acerca de cómo usar esta tecnología para transmitir datos a corta distancia (por ejemplo una LAN) y con alta tasa de transmisión.

4.9. Formas de propagación inalámbrica

Las ondas de radio admiten varias formas de propagación:

- Propagación por ondas de superficie.
- Propagación troposférica.
- Propagación ionosférica.
- Propagación por visibilidad directa.

Cada una de ellas tiene unas características que la hacen adecuada para la transmisión de un tipo u otro de servicio de telecomunicación.
Veamos a continuación y con más detalle cada una de ellas.

Propagación por ondas de superficie:
Es aquel tipo de propagación donde las ondas radioeléctricas viajan a través de la superficie de la tierra siguiendo su curvatura.
Alcanzan grandes distancias (incluso a nivel mundial) y pueden transmitirse incluso sobre la superficie del agua.
La distancia alcanzada depende de la potencia de señal con que se emite, de forma que a más potencia mayor alcance.
El problema es que requiere antenas de gran tamaño.

Propagación troposférica:
Es aquel tipo de propagación donde la onda de radio se refleja en la capa de la troposfera de la atmósfera y rebota de nuevo hacia la tierra permitiendo alcanzar grandes distancias.

También permite la transmisión directa entre emisor y receptor siempre que exista visibilidad directa.
En el caso de que no existiera esta visibilidad directa (por la curvatura de la tierra) se podría alcanzar el enlace gracias a la reflexión en la troposfera.

Propagación inosférica:
Es aquel tipo de propagación donde las ondas radioeléctricas son radiadas hacia la capa de la ionosfera de la atmósfera, se reflejan en ella y vuelven hacia la tierra permitiendo alcanzar largas distancias.
Por la noche, y debido a que parte de la capa de la ionosfera desaparece, la reflexión se produce a una cota superior alcanzándose con ello mayores distancias.

Propagación por visibilidad directa:
En esta propagación existe una visibilidad directa entre antena emisora y receptora mediante la cual se puede establecer el enlace.
Debido a la curvatura de la tierra y a la presencia de obstáculos, dichas antenas deben estar situadas en zonas altas y estar enfrentadas entre sí.
Este tipo de propagación es muy empleada para transmisiones punto a punto como repetidores de televisión, enlaces de datos, etc.

5. Control de enlace de datos

5.1. Funciones del control de enlace de datos

El nivel de enlace de datos es el nivel que corresponde con la capa 2 del modelo OSI y/o modelo TCP/IP.
Es por tanto un nivel que está por encima del nivel físico (no trata la información bit a bit) pero aún no llega a realizar las funciones de las capas superiores como enrutado, asignación de calidad de servicio, etc.
Como todos los niveles o capas del modelo introduce una cabecera a la información que recibe de los niveles superiores (cabecera del nivel de enlace) que incluye información de este nivel para que después pueda ser decodificado en el nivel 2 en el otro extremo.
En el siguiente esquema se observa su ubicación en la torre de protocolos del modelo OSI.

El nivel de control de datos como ya se ha descrito anteriormente se corresponde con el nivel 2 del modelo OSI.
Su función principal es realizar una conexión fiable de la información que se transmite entre un nodo y otro adyacente. Es por ello que añade sobre lo que realiza el nivel físico (capa inmediatamente inferior) un control de flujo y de errores para conseguir esta transmisión fiable.
Para conseguir esa conexión fiable en esta capa se realizan las siguientes funciones:

- **Tramado**:
  En este nivel el flujo de bits se agrupa en unidades denominadas tramas. Esta capa se encarga de transmitir, manejar y gestionar tramas que no es más que un grupo de bits.
- **Direccionamiento físico**:
  El nivel de enlace de datos añade una cabecera a la trama donde se especifica la dirección física del emisor y del receptor.
- **Control de flujo**:
  En este nivel se regula la velocidad de transmisión, es decir, adecúa la velocidad la tasa de transferencia en función de la capacidad de recepción del receptor. Para ello implementa buffer de entrada y de salida en los nodos emisor y receptor.
  Con ello se evita el desbordamiento del receptor.
- **Control de errores**:
  En este nivel se añaden funciones de detección y control de errores de las tramas que llegan defectuosas, que no llegan o que llegan duplicadas.
  La corrección de tramas defectuosas se realiza mediante la retransmisión de la trama.
  Es con esta funcionalidad lo que hace que en este nivel se consigue que la transmisión de la información sea fiable nodo a nodo.

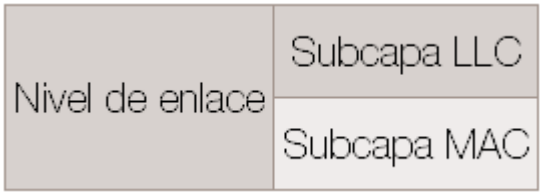
Con el nivel de enlace de datos, lo que se consigue en definitiva es enmascarar las errores de transmisión que puede crearse o deberse al medio de transmisión empleado (cableado, infrarrojos, inalámbrico, etc).

5.2. Tipos de protocolos

El nivel de enlace de datos se puede subdividir a su vez en dos subcapas:

- Subcapa **MAC**:
  Es la capa más inferior y cuyas funciones son más cercanas al nivel físico (a nivel hardware) que a nivel lógico.
- Subcapa **LLC**:
  Es la capa más superior y asignadas funciones de carácter más lógico (a nivel software) que a nivel físico.

La suma de las funciones de ambas subcapas aglutina las funciones que le corresponden al nivel de enlace de datos.
En la siguiente tabla se puede observar la subdivisión del nivel de enlace de datos en estas dos subcapas.



Veremos a continuación con más detalle las funciones que realiza cada subcapa.

Subcapa MAC:
Se trata de la subcapa más inferior del nivel de enlace de datos y se corresponde con las siglas de subnivel de *control de acceso al medio* (Medium Access Control).
Tiene asignadas las funciones más cercanas a nivel físico del enlace de transmisión (sin ser las propias de la capa de nivel físico) entre la que destacan las siguientes:

- Controlar el **acceso** al medio:
  El medio de transmisión es compartido y en esta capa se regula el acceso al medio bien sea CSMA/CD, Token-ring, token-bus, etc.
- Realizar el **tramado**:
  Es decir, agrupar el flujo de bits en tramas que es la unidad de información que gestiona el nivel de enlace de datos.
- **Direccionamiento físico**:
  Se encarga de incluir la dirección física del emisor y del receptor
- Detectar los **errores** de la transmisión y notificarlo al subnivel LLC.

Subcapa LLC:
Se trata de la subcapa más superior del nivel de enlace de datos y se corresponde con las siglas de subnivel de *control lógico del enlace* (Link Logic Control).
Tiene asignadas las funciones más cercanas a nivel de red (sin ser las propias de la capa de nivel de red) entre la que destaca las siguientes:

- Realizar el **interfaz** entre el subnivel MAC y el nivel de red.
- Realizar **encapsulado** de los paquetes de nivel superior y añadir la cabecera del nivel de enlace de datos.
- Controlar la **comunicación** de nodo a nodo.
- Realiza el control de **errores** tras la detección de ellos por el nivel MAC.

La detección del error la realiza el nivel MAC con redundancia cíclica y la corrección del error la realiza el LLC con la retransmisión de la trama.
Como se ha comentado anteriormente, el subnivel MAC realiza la detección de errores.

Técnica de bit de paridad

Una de las técnicas de detección de errores más empleados es la técnica de bit de paridad.
Esta técnica consiste en añadir un bit de control a la trama de bits, de forma que si el número de bits puesto a 1 de la trama es par el bit de paridad es un 0. Si es impar el número de bits puesto a 1, el bit de paridad es puesto a 1.
Con esta técnica se asegura la integridad de la trama, ya que el receptor cuando recibe la trama lo primero que realiza es contar el número de bits puesto a 1 y comprueba si coincide con el bit de paridad.
Si coincide, da por válido la trama y lo pasa a los niveles superiores. En caso contrario, notifica a subnivel LLC que la trama recibida es errónea para que proceda a su corrección, que como se ha descrito anteriormente, es mediante la retransmisión de la trama.
¿Qué pasa si el error se produce en el bit de paridad?
En este caso, ya no podemos utilizar este 'chivato' para comprobar si la trama es correcta o no ya que también el bit de paridad puede sufrir alteración en la transmisión.
¿Y qué ocurre si hay un conjunto de errores en los bits de la trama (no uno sino varios) que haga que el número de bits puesto a 1 sea par o impar y coincida con el bit de paridad pero que en el fondo es un cúmulo de errores?
En este último caso tampoco funcionaría el bit de paridad, ya que con ello no podríamos discriminar las tramas correctas de las erróneas.
Por todo ello, hay nuevas técnicas de control de errores a nivel de enlace de datos más complejas que solucionan estos problemas.
Uno de ellos es la técnica de redundancia cíclica (CRC) que veremos a continuación.

Técnica de redundancia cíclica (CRC):

Esta técnica de redundancia cíclica (CRC) es un método de detección de errores que consiste en añadir al final de la trama de información una serie de bits (habitualmente 2 o 4 bits) que actuarán como bits de control para la detección de errores por parte del receptor.
Para ello emplea un algoritmo que consiste en tratar el flujo de bits a enviar por el emisor como si fuera un polinomio al cual se le aplica una operación matemática polinomial con un patrón (conocido por emisor y receptor) y el resultado es lo que realmente se transmite junto con un patrón residual.
Así por **ejemplo** si la trama a enviar es el flujo de bits siguientes:

1 0 0 1 1 0

Esta técnica lo considera como un polinomio de grado Nº de bits -1, es decir:

$$1 \times X^5 + 0 \times X^4 + 0 \times X^3 + 1 \times X^2 + 1 \times X^1 + 0 \times X^0 = X^5 + X^2 + X$$

A este polinomio se le denomina polinomio del mensaje M(x).
Por otro lado, tenemos un polinomio de grado k que actuará como polinomio generador G(x) y que es conocido por emisor y receptor y que actuará como polinomio patrón para aplicar el algoritmo del CRC.
Por ejemplo, podemos tener un polinomio patrón G(x) de grado 2 como el siguiente:

$$G(x) = x^2 + 1$$

La esencia del algoritmo consiste en dividir el mensaje M(x) por el código patrón G(x) y adicionar el resto obtenido al mensaje M(x) y que actuará como bits de control. Esto lo realiza el emisor antes de enviar la trama.
En el receptor recibe la trama enviada (que como sabemos incluye el mensaje original y los bits de control) y lo que hace es dividir dicho mensaje por el patrón. Si en la división sale un resto esto indica que ha habido un error en la transmisión.
Para calcular la redundancia (bits de control) se deben seguir los siguientes pasos:

1. A la trama del mensaje M(x) se debe añadir tantos ceros por su extremo menos significativos como grado sea el polinomio generador G(x).
2. Al flujo de bits obtenidos se le debe aplicar la división por el polinomio generador G(x) empleando la división en módulo 2.
3. Al resto obtenido aplicar la resta en módulo 2 y el resultado obtenido adicionar dichos bits por el extremo menos significativo a la trama a enviar. Esto último es la trama que se debe enviar.

El algoritmo implica un coste computacional para realizar las operaciones polinomiales descritas, pero a cambio, se obtiene eficiencia en la detección de errores, ya que es un algoritmo robusto.
En primer lugar describimos cómo realizar la división en módulo 2.
Esta división corresponde a un OR exclusivo, es decir no hay términos de acarreo ni para la suma ni para la resta. Su tabla de verdad es la siguiente:

A	B	A (XOR) B
0	0	0
0	1	1
1	0	1
1	1	0

La división se realiza en binario, con la excepción de que la resta se efectúa en módulo 2.

Ejemplo:
Dado el siguiente mensaje M(x) formado por bits **0 1 1 0 1 0** y el patrón G(x) con los bits **1 0**, calcular la trama que se enviaría al receptor si como detección de errores aplicamos la técnica de CRC.
Solución:
En primer lugar debemos pasar el flujo de bits que nos indica en polinomios, ya que en CRC tratamos polinomios para aplicar el algoritmo. Así obtenemos:

$$M(x) = 0 \times X^5 + 1 \times X^4 + 1 \times X^3 + 0 \times X^2 + 1 \times X^1 + 0 \times X^0 = X^4 + X^3 + X$$

$$G(x) = 1 \times X^1 + 0 \times X^0 = X$$

Ahora debemos aplicar el algoritmo anteriormente descrito paso por paso.

1. Añadimos al mensaje M(x) tantos ceros como grado sea el polinomio generador G(x) en este caso 1 cero. Nos queda entonces:

   T(x)= **0 1 1 0 1 0 0**

2. Aplicamos al resultado anterior la división por el polinomio generador G(x) aplicando división en módulo 2.

```
    0 1 1 0 1 0 0
    1 0
 ------------
    1 1 1
    1 0
 ------------
    0 1 0
 1 0
 ------------
 0 0 1
 1 0
 -----------
 0 0 0
 1 0
 ------------
 1 1 0
 1 0
```

----

0 0 Resto R(x).

Luego la trama a enviar será el mensaje original M(x) al cual debemos de añadir el resto obtenido, es decir, R(x).

Luego la trama a enviar será: **T(x) a transmitir = 0 1 1 0 1 0 0 0 0**

Vemos por tanto que dicha trama transmitida tiene dos bits de CRC (**0 0**).

Estos dos bits son lo que empleará el receptor para la detección de errores una vez recibida la trama.

5.3. Método de control de línea

Antes de poder enviar una trama a otro nodo, el nivel de control de enlace de datos debe comprobar que el medio de transmisión (que es compartido) está preparado para transmitir.

El que está preparado para transmitir depende de varios factores:

- Que no esté ocupado por otra transmisión.
- Que el receptor al que va dirigido la trama esté listo para su recepción.

Ambas comprobaciones debe realizarlo el nivel de enlace de datos antes de poder transmitir la trama y para ello se establece un mecanismo o control de línea.

Existen dos métodos de control de línea:

- Sondeo y reconocimiento.
- Sondeo y selección.

Sondeo y reconocimiento:

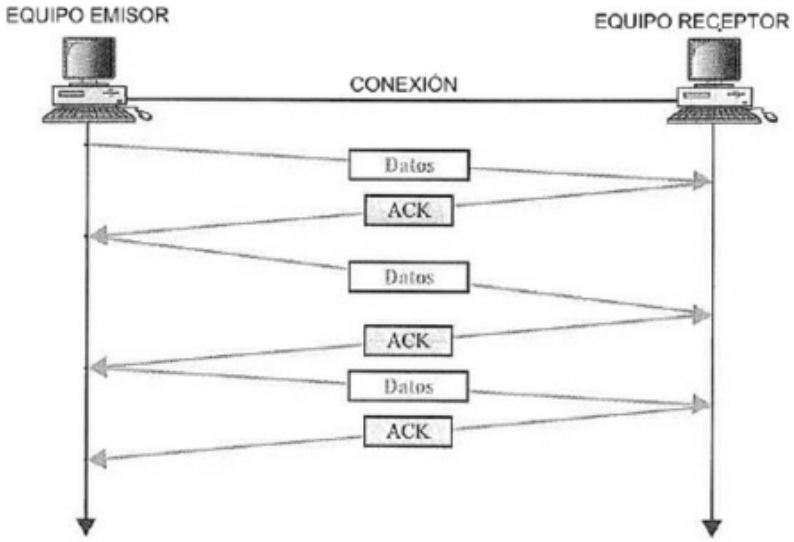
Esta técnica de control de línea, también denominada ENQ/ACK, se emplea sólo cuando el medio no es compartido y lo único que se comprueba es que el receptor está preparado para recibir datos.

El canal de transmisión sólo se usa para transmitir datos de un nodo a otro sin que haya otro nodo o aplicación que pueda usar el mismo canal.

Esta técnica emplea un procedimiento que es el siguiente:

- El emisor transmite en primer lugar una trama de solicitud de inicio de transmisión ENQ (*Petición, consulta*) esperando con ello una trama de confirmación ACK (*Acuse de recibo*) por parte del receptor que está preparado para recibir datos.
- En caso de que el receptor esté preparado enviará una trama ACK al emisor. En caso contrario enviará una trama de rechazo NAK *(Acuse de recibo negativo)* .
- Si el emisor no recibe ninguna trama de respuesta del receptor, supone que dicha trama ENQ se ha perdido y la retransmite. Realiza hasta tres intentos y si no se recibe ACK desestima la transmisión
- En caso de recibir ACK por parte del receptor se inicia la transmisión de información.
- La comunicación se termina cuando el emisor envía al receptor la trama de EOT que indica final de transmisión.

En el siguiente esquema puede verse cómo se sigue la secuencia de tramas en esta técnica de sondeo y reconocimiento.



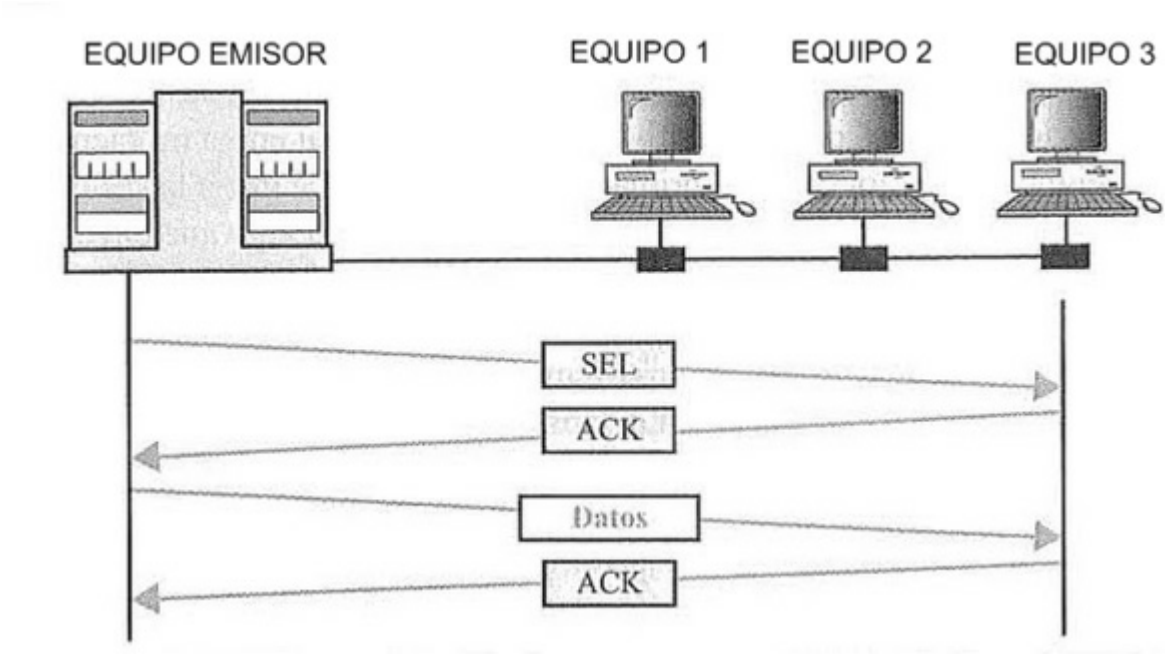
El principal inconveniente de esta técnica es que sólo es válida para enlaces dedicados, es decir, el medio no puede ser compartido por varias transmisiones.
Aun así es una técnica ampliamente utilizada por su simplicidad y rapidez de establecimiento de la conexión.

Sondeo y selección:
Esta técnica de control de línea se emplea sólo cuando el medio es compartido entre varios nodos.
En este caso siempre existe un nodo principal y primario por el cual pasan todos los datos y varios nodos secundarios. Se trata de un enlace multipunto.
En este caso, antes de enviar cualquier dato, no sólo hay que determinar si el receptor está preparado para recibir datos, sino que además hay que seleccionar el receptor que debe recibir el dato (es el proceso de selección). Este proceso de selección lo realiza el nodo primario.
Es el nodo primario quien actúa como receptor, pregunta a los nodos secundarios si quieren transmitir algo (proceso de sondeo) y en caso afirmativo, le da el control del medio de transmisión.
Por tanto en este método de control de línea existen dos procesos:

- Proceso de sondeo.
- Proceso de selección.

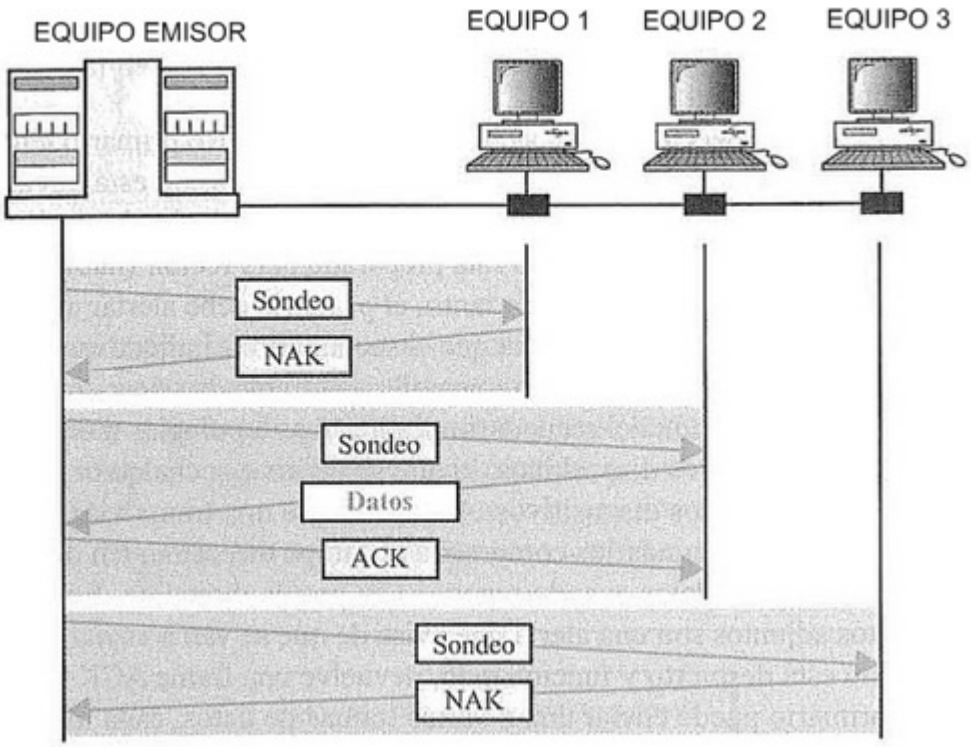
Proceso de selección:

En este proceso es el nodo primario el que va a actuar como emisor y por tanto debe preguntar a los nodos secundarios (que van a ser los receptores) si están preparados para recibir los datos.
El canal siempre está disponible, por lo que sólo hay que asegurarse si lo está el nodo receptor.
Para ello, envía una trama SEL con el campo de dirección destino al que va dirigido el mensaje. Esta trama le llega a todos los nodos secundarios o posibles receptores, pero sólo el nodo secundario que tiene esa dirección como dirección de red lo reconoce y envía una trama de ACK al nodo primario. Éste último recibe el ACK y comienza el envío de la información a ese nodo.
En la siguiente imagen podemos ver la secuencia de tramas.

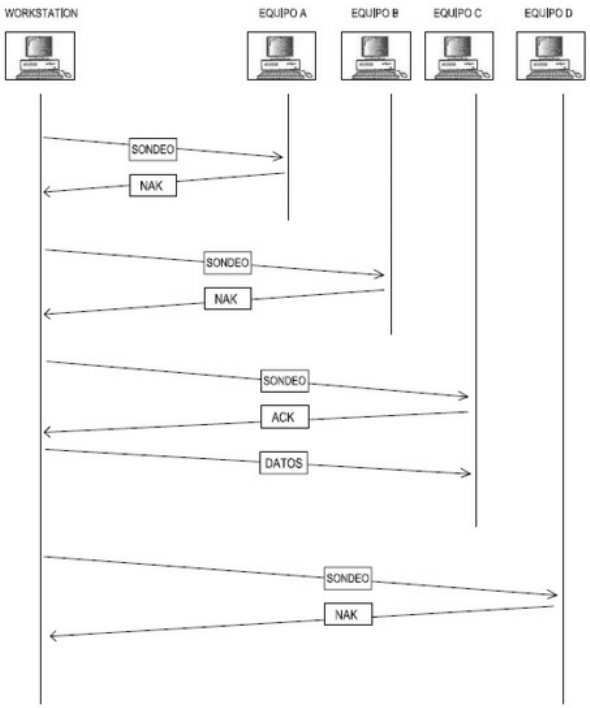


Proceso de sondeo:

En este proceso es el nodo primario el que va a actuar como receptor y por tanto debe preguntar a los nodos secundarios (que van a ser los posibles emisores) si quieren enviar algo.
Para ello envía una trama de petición de envío a todos los nodos secundarios. Esta trama se realiza por orden a cada dispositivo. En el caso en el que el nodo secundario no tenga nada que enviar responde con una trama NAK. En cambio si tiene algo que enviar responde con las tramas de datos que quiere enviar.
En la siguiente imagen podemos ver la secuencia de tramas.



Veamos un **ejemplo**:
Supongamos una red con un Workstation –o Estación de trabajo- A que quiere enviar datos al equipo C y donde existen además los equipos B, D y E que comparten el mismo canal de transmisión.
Si se emplea como método de control de línea el método de sondeo/selección, dibuja la secuencia de tramas que se produce entre los equipos emisor y los receptores.



Solución:
En este caso el método de sondeo/selección antes de enviar datos al receptor debe seleccionarlo y esperar a que responda con un ACK que está listo para recibir.
Aquellos que no sean el destinatario enviará un NAK de rechazo de transmisión.
La secuencia de tramas que se produce será la siguiente:
En primer lugar, el emisor WorkStation A enviará una trama de petición de inicio de transmisión con la dirección física del receptor al que va dirigido.
Esta petición lo realiza de forma secuencial a los equipos A, B, C, y D.
El equipo A, al recibir esta petición y ver que no es su dirección, rechaza la solicitud enviando al emisor una trama NAK. Ocurre lo mismo con el equipo B y D.
Sólo el equipo B que observa la dirección y que está preparado para recibir datos, acepta la petición y envía un ACK. Entonces al recibir el emisor este ACK empieza a enviarle las tramas de información.
Cuando termina de enviarle las tramas de información el emisor enviará al equipo C una trama de fin de conexión EOT.

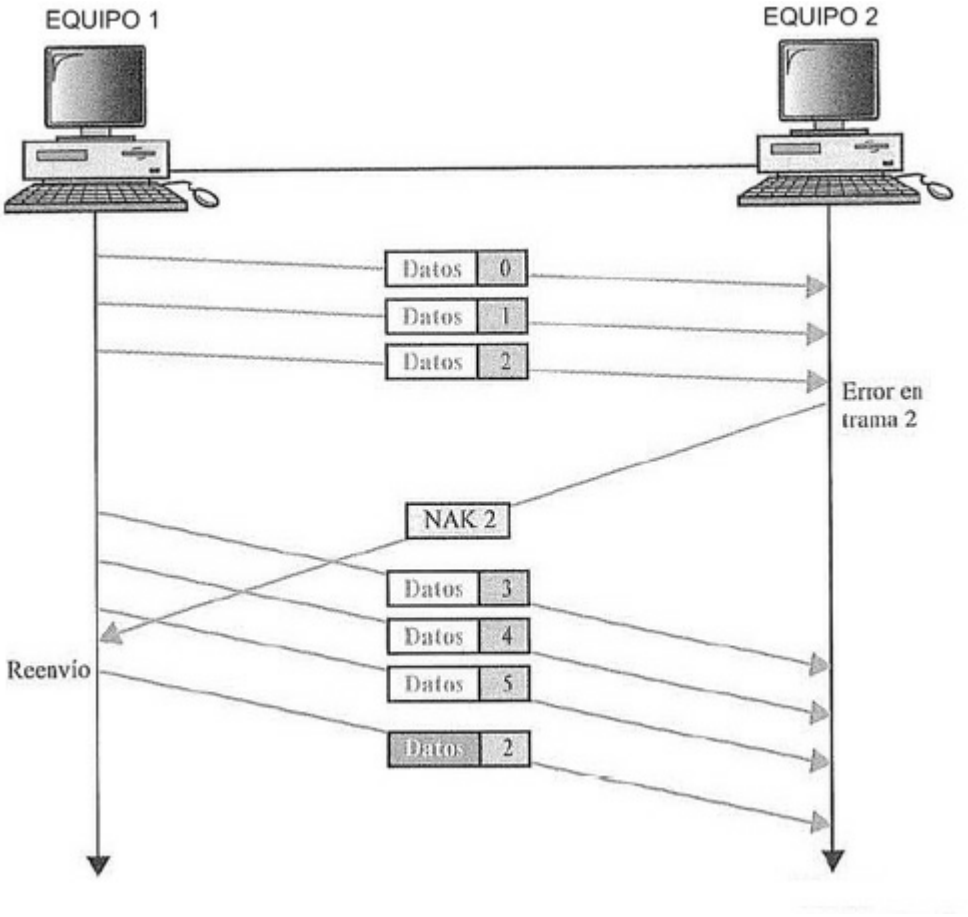
5.4. Tratamiento de errores

Como se ya ha visto anteriormente, el nivel de enlace de datos realiza una detección de errores, la cual se encarga el subnivel MAC y una corrección de errores que se encarga el subnivel LLC.
La técnica de corrección de errores empleada es la retransmisión de nuevo de la trama, es decir, si la trama recibida es errónea se solicita de nuevo su retransmisión.
Pero esta petición de retransmisión de trama errónea puede implementarse de varias formas:

- Petición automática de retransmisión (ARQ).
- Parada y espera con ARQ.
- Ventana deslizante con ARQ.

Vemos a continuación cómo funciona cada uno de estos mecanismos con más detalle.

Petición automática de retransmisiones (ARQ):
Es el método de corrección de errores basado en la retransmisión más sencilla.
En ella, el emisor va enviando tramas al receptor y, éste último cuando detecta una trama errónea, le envía al emisor una trama NAK junto con el número de trama errónea.
Cuando el emisor recibe el NAK con este número, retransmite la trama errónea.
En la siguiente imagen se puede comprobar el funcionamiento de este mecanismo.



Parada y espera con ARQ:

En este método, el emisor envía tramas al receptor, aunque no envía la siguiente hasta no haber recibido la confirmación de trama recibida por parte del receptor. Es decir, hay una parada y espera por parte del emisor que no envía nueva trama hasta recibir la confirmación por parte del receptor.

El procedimiento es sencillo: el emisor envía una trama numerada por 0 y 1 (alternativamente para evitar duplicidad) y espera el ACK del receptor que indicará la siguiente trama a recibir. Es decir, si ha enviado la trama con número 0 y ha llegado correctamente, el receptor enviará un ACK 1 que indica que espera recibir la trama 1 ya que la trama 0 le ha llegado correctamente.

Sólo cuando ha llegado el ACK envía la siguiente trama el emisor.

En caso de que la trama recibida sea errónea, el receptor envía un NAK y cuando lo recibe el emisor retransmite la última trama enviada.

Este mecanismo incorpora un temporizador, de forma que si el emisor en un tiempo preestablecido no recibe un NAK o un ACK de la última trama enviada, entiende que no ha llegado y retransmite de nuevo la última trama enviada.

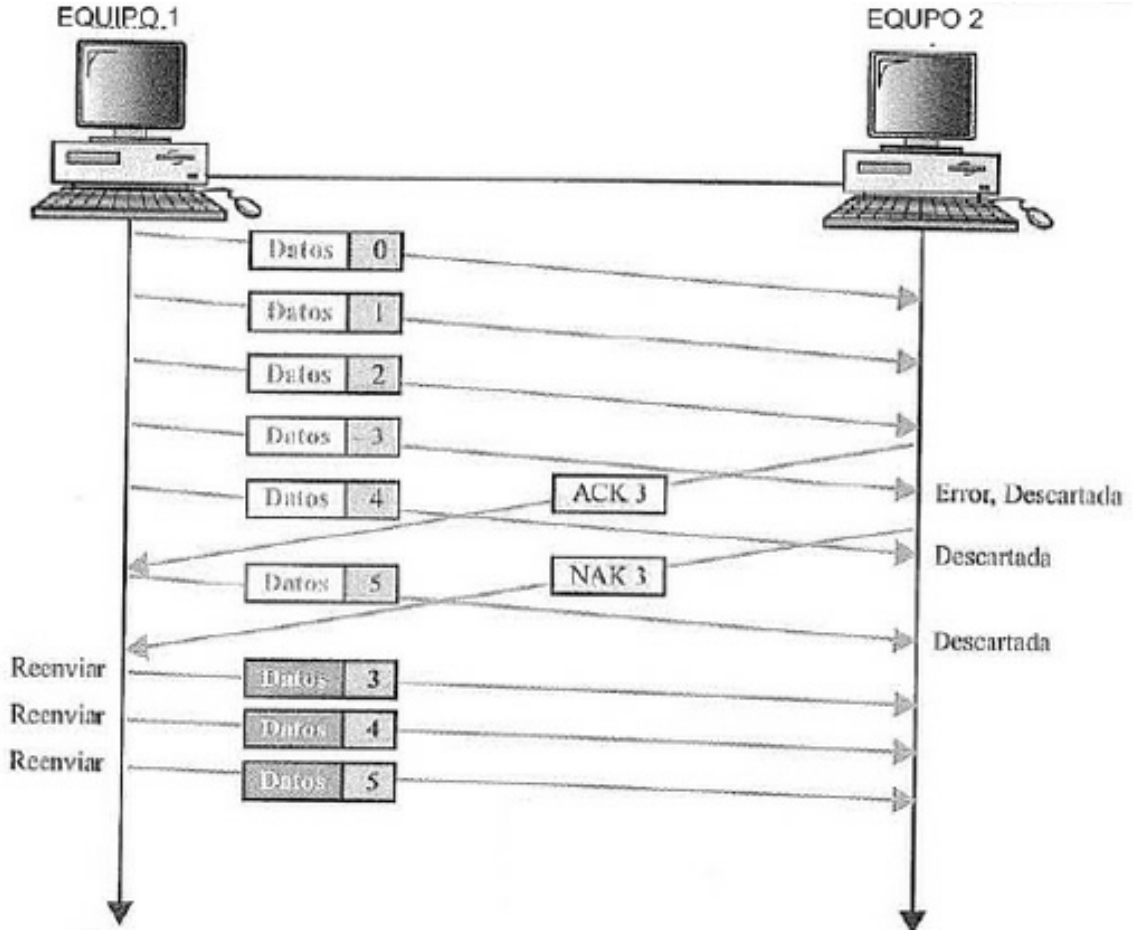
Ventana deslizante con ARQ:

El mecanismo de parada y espera con ARQ tiene el siguiente problema: es un mecanismo lento ya que no puede enviar nuevas tramas hasta recibir el ACK de la última trama enviada. Esto ralentiza el proceso de transmisión.

Esto se soluciona con el mecanismo de ventana deslizante con ARQ.

Es este mecanismo el emisor envía tramas de forma numerada y sin esperar confirmación por parte del receptor. Cuando la trama es recibida correctamente el receptor, envía un ACK junto con el número de la trama siguiente a recibir. El emisor al recibir este ACK da por válido todas las tramas enviadas anteriormente.

En el caso de que la trama recibida sea errónea, el receptor envía un NAK junto con el número de la trama errónea. El emisor al recibirlo envía dicha trama y todas las siguientes enviadas a continuación ya que entiende que la transmisión ha podido fallar y sean erróneas todas las tramas siguientes.
El sistema se llama ventana deslizante, porque existe una 'ventana' de tramas que se envía sin esperar confirmación y esto hace conseguir velocidad en la transmisión.
En la siguiente imagen podemos el funcionamiento de este mecanismo.

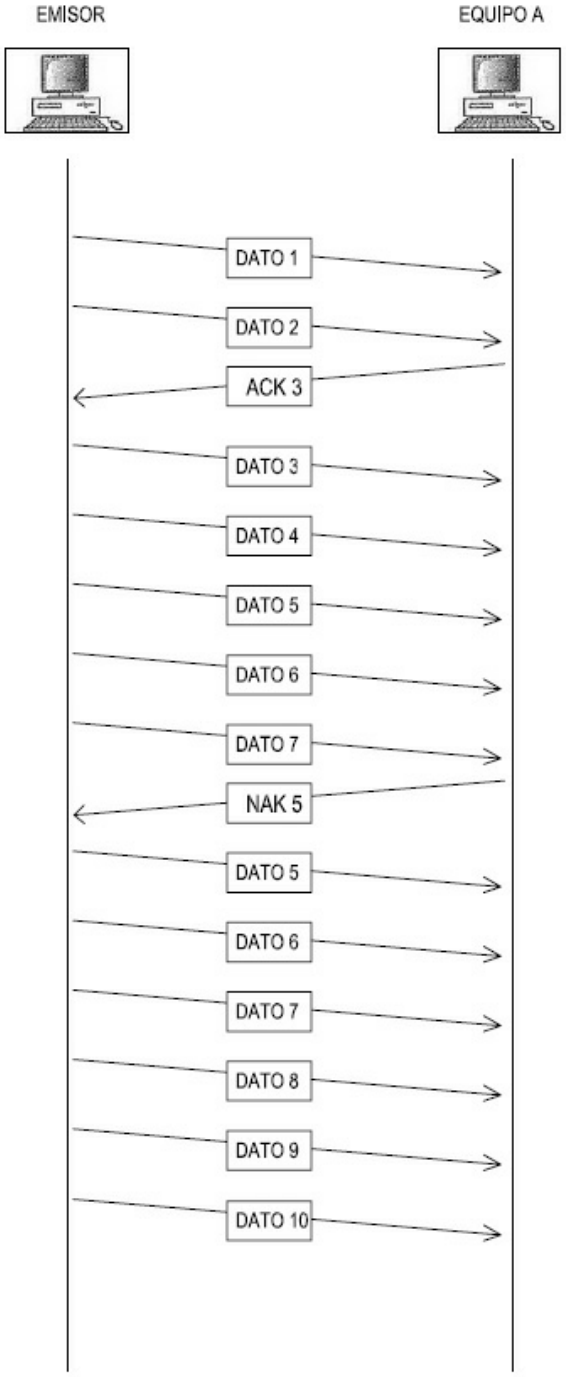


Este mecanismo de ventana deslizante con ARQ admite dos variantes:

- Vuelta atrás con n ARQ.
- Rechazo selectivo con ARQ.

Vuelta atrás con n ARQ:

Es el mecanismo anteriormente descrito.
En este caso el emisor envía tramas numeradas sin esperar confirmación. Cuando recibe un ACK numerado, entiende que se han recibido correctamente todas las tramas con un número anterior a la indicada en el ACK que es la siguiente que se espera recibir.



En el caso de recibir un NAK, se indica el número de trama errónea y entonces el emisor envía dicha trama y todas las siguientes.

Este método se denomina n ARQ, porque es el número de tramas que se envía desde la NAK recibida, es decir, si se recibe un NAK 3, y n es 4, se retransmite la trama 3 y las 3 tramas siguientes, es decir, la trama 4, 5 y 6. En total se retransmiten 4 tramas.

Rechazo selectivo con ARQ:

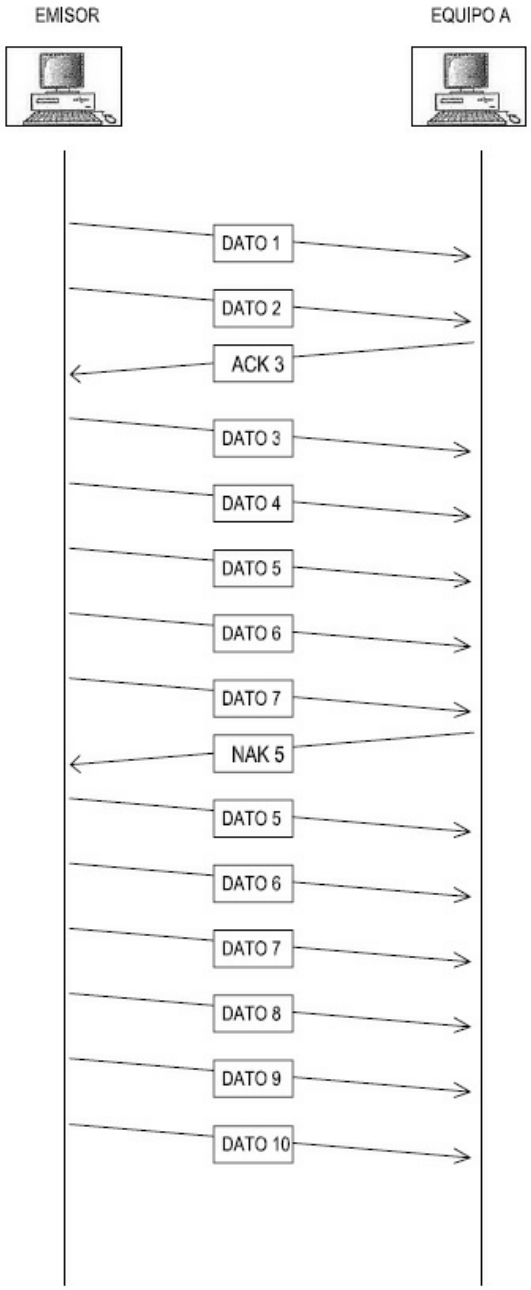
En este método, a diferencia del anterior, el receptor envía un ACK de la trama recibida correctamente y no de la siguiente esperada.

En el caso de trama errónea, el NAK la indica para que el emisor sólo la envíe y no todas las siguientes. De esta forma se logra más eficiencia ya que no se reenvía n tramas siguientes.

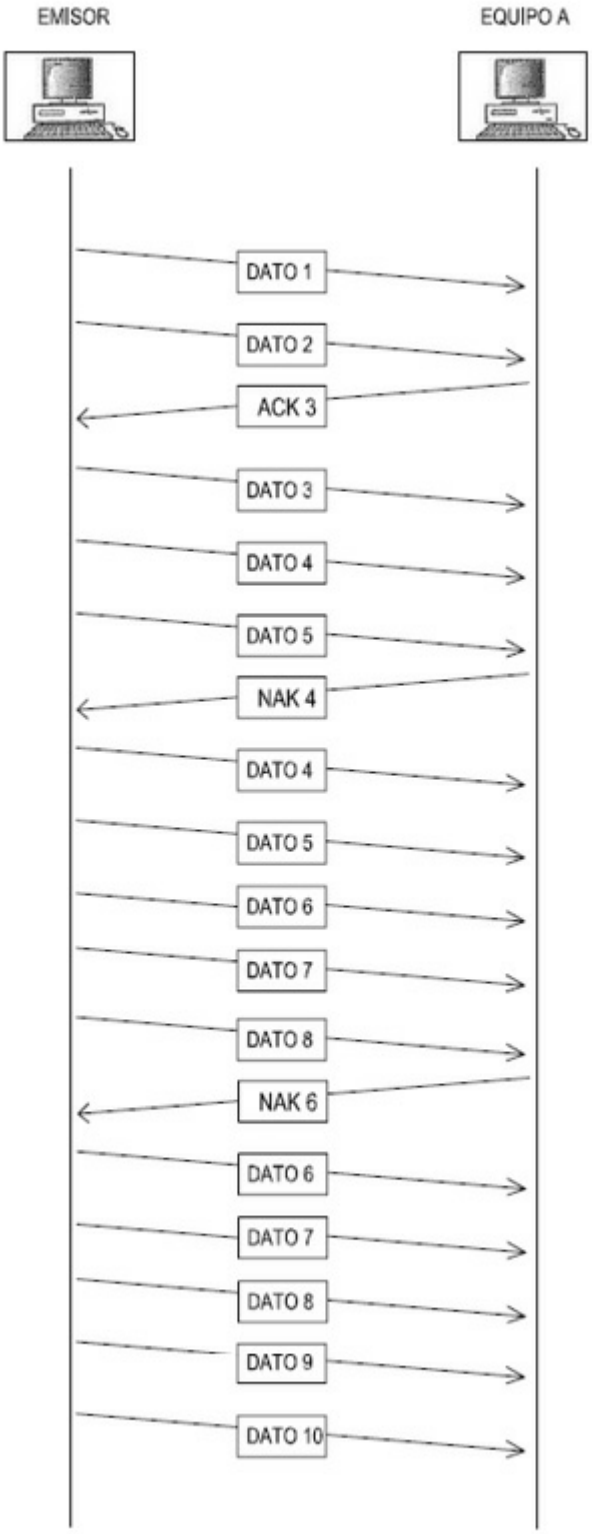
No obstante, este método contempla la implementación de un buffer en el emisor y receptor que sean capaces de almacenar un número determinado de tramas, por si falla alguna en la transmisión, el emisor la tenga almacenada en el buffer y pueda transmitirla.
En el caso del receptor, un determinado número de tramas recibidas deben estar almacenadas temporalmente para que si fallase una y necesita retransmisión, el receptor pueda reordenarlas junto con las recibidas correctamente.

Ejemplo:
Supongamos un enlace de transmisión entre dos nodos adyancentes A y B donde como método de control y corrección de errores se emplea Vuelta atrás con 5 ARQ. Dibuja la secuencia de tramas que se transmite donde durante la transmisión de la trama 7 el emisor recibe un NAK 5.

Solución:
En este caso, la ventana de transmisión n es 5, es decir, en el caso de que el emisor reciba un NAK deberá enviar la trama indicada y las 4 siguientes (en total 5 que es la ventana de transmisión).
Dibujamos la secuencia de tramas del enlace.
En este caso, el emisor empieza a enviar tramas sin esperar confirmación por parte del receptor. Al recibir el ACK 3 indica que las tramas 1 y 2 han llegado correctamente y espera la trama 3.
Durante la transmisión de la trama 7, el emisor recibe un NAK 5 que le indica que no se ha recibido la trama 5 y por tanto debe retransmitirla junto con las 4 siguientes, es decir, la trama 5, trama 6, trama 7, trama 8 y trama 9.
Una vez retransmitidas todas esas tramas, continúa con la transmisión de tramas y en caso reanuda la transmisión con las tramas 10, 11, etc.
En este caso, al ser la ventana n=5, permite ganar velocidad en la transmisión, aunque si se pierde alguna trama, baja su eficiencia al tener que reenviar un número alto de tramas.



Veamos otro **ejemplo**.
Supongamos el mismo enlace de transmisión descrito anteriormente pero en este caso la ventana de transmisión es n=3. Dibuja la secuencia de tramas donde en este caso se produce una pérdida de la trama 4 y de la trama 6 durante la transmisión.
Solución:
En este caso, con una ventana de transmisión más pequeña conseguiremos más eficiencia que el anterior, al tener que retransmitir menos tramas.
No obstante, en este caso, tenemos más errores en la transmisión.
Dibujamos la secuencia de tramas del enlace.



En este caso, el emisor empieza a enviar tramas sin esperar confirmación por parte del receptor. Al recibir el ACK 3 indica que la trama 1 y 2 han llegado correctamente y espera la trama 3.
Durante la transmisión de la trama 5, el emisor recibe un NAK 4 que le indica que no se ha recibido la trama 4 y por tanto debe retransmitirla junto con las 2 siguientes, es decir, la trama 5 y trama 6.
Una vez retransmitidas todas esas tramas, continúa con la transmisión de tramas y en este caso reanuda la transmisión con las tramas 7, 8, etc.
Durante la transmisión de la trama 8, de nuevo el emisor recibe un NAK 6 que indica que no se ha recibido la trama 6. Es por ello que debe retransmitir dicha trama y las dos siguientes, es decir, la trama 7 y la trama 8.
Una vez retransmitidas todas esas tramas, continúa con la transmisión de las tramas.

5.5. Control de flujo

Otra de las funciones básicas que realiza el nivel de enlace de datos es el control de flujo.

El control de flujo es un conjunto de técnicas que permite al emisor saber cuántas tramas puede enviar consecutivamente, sin esperar confirmación por parte del receptor y no provocar el desbordamiento de éste último.

Con esto se evita que, debido a la capacidad de recepción de tramas por parte del receptor y de su limitación de memoria, no pueda absorber la velocidad de llegada de tramas por parte del emisor y debe indicarle que baje o 'regule' la velocidad de emisión de tramas.

Esto se debe a que en la recepción se debe realizar una detección y control de errores, además de otras funciones como desentramado y por tanto es una operación más lenta que puede desbordar el buffer de entrada de las tramas.

Hay dos implementaciones para el control de flujo:

- Parada y espera.
- Ventana deslizante.

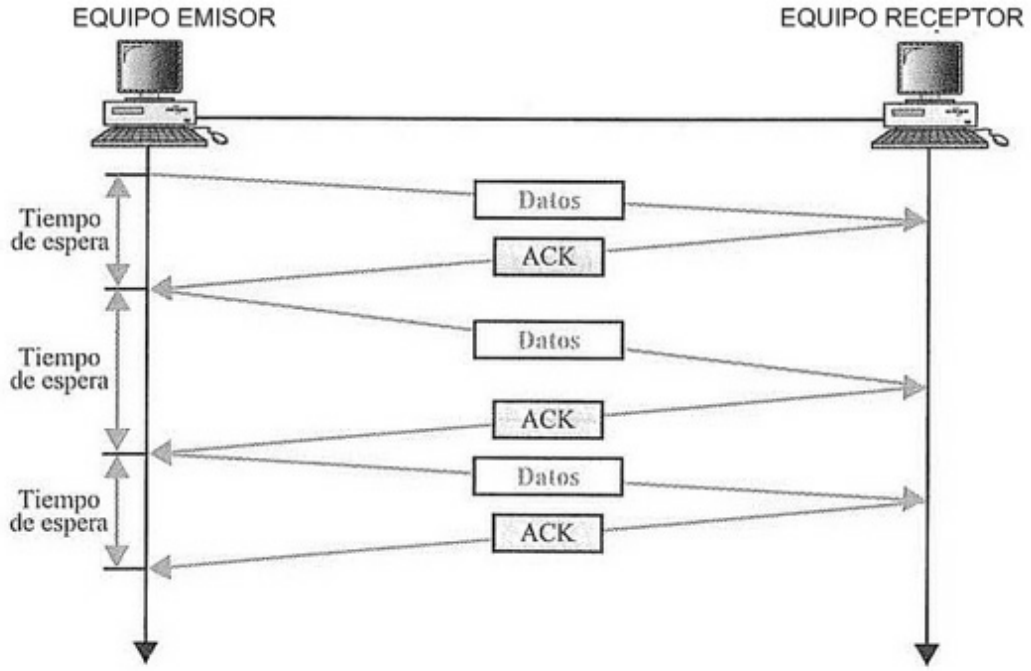
Parada y espera:

En este método de control de flujo, el emisor envía una trama y espera la confirmación de recepción de dicha trama.

No enviará la trama siguiente hasta recibir el ACK de la trama enviada o el NAK en cuyo caso retransmitirá de nuevo la trama.

Este sistema se caracteriza por su sencillez ya que cada trama enviada es reconocida y validada antes de enviar la siguiente. El inconveniente es su baja eficiencia debido a su lentitud.

En la siguiente imagen podemos ver un ejemplo de funcionamiento de este mecanismo de control de flujo.



Ventana deslizante:

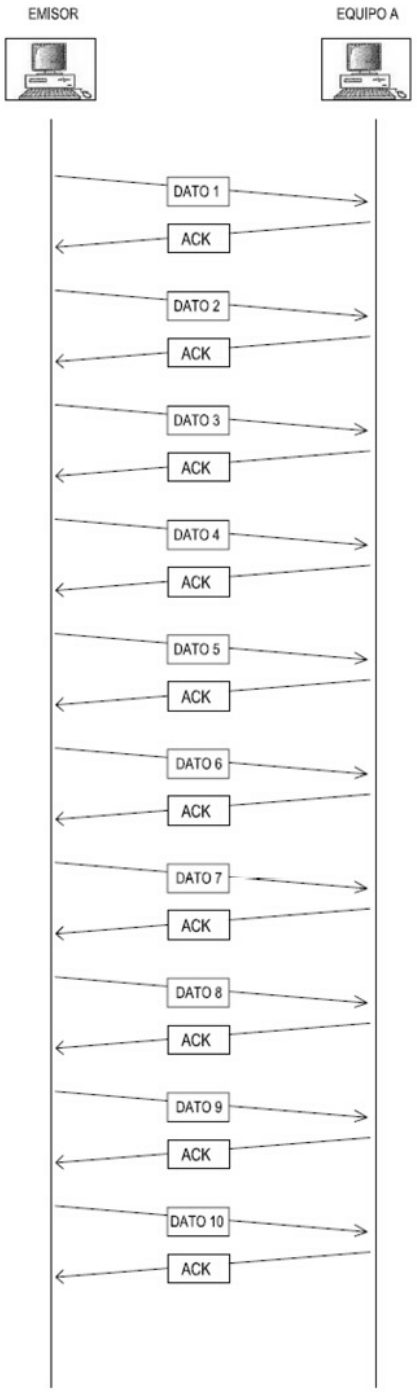
En este método de control de flujo, el emisor puede enviar varias tramas sin tener que esperar la validación de ellas.

Cuando recibe un ACK, éste va junto con el número de trama siguiente que espera recibir el receptor, validando la entrega correcta de las tramas anteriores.

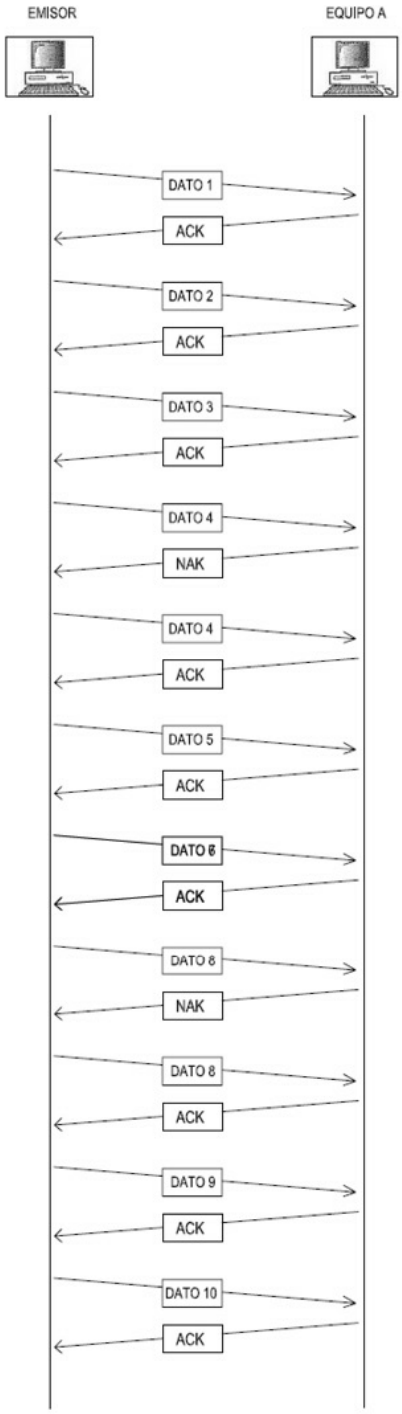
La ventana proporciona un límite superior en el cual se indica el número máximo de tramas que se puede enviar sin esperar la confirmación por parte del receptor. Es como si fuera un buffer que se va llenando de tramas a enviar y se va vaciando según se vayan transmitiendo las tramas (en el lado del emisor).

En el lado del receptor actúa también como buffer que se va llenando según las tramas que va recibiendo y se va vaciando según van siendo validadas hasta el tope máximo de la ventana.
En la parte de recepción, al principio de la transmisión la ventana está vacía y se va llenando a medida que va recibiendo tramas. Se va reduciendo a medida de que va validando las tramas y en ese caso toma nuevas tramas nuevas recibidas hasta llenar la ventana de recepción.
Este sistema aunque es más complejo que el de parada y espera por su implementación es más eficiente ya que aumenta la velocidad efectiva de la transmisión.

Ejemplo:
Supongamos dos equipos que se conectan a través de un enlace de datos donde se aplica un control de flujo basado en la parada y espera.
Si se envían en total 10 tramas desde el equipo emisor A al equipo receptor B, donde el tiempo de transmisión de la trama es de 1 mseg y el tiempo de espera al ACK o NAK es de 2 mseg, calcula el tiempo que tardaría el sistema en realizar la transmisión completa.
Realiza también la secuencia de tramas de la transmisión.
Supón que no se pierde ninguna trama enviada.
Solución:
En este caso, el método de parada y espera exige que no se pueda enviar una nueva trama hasta recibir el ACK o el NAK de la trama enviada.
Dado que todas las tramas enviadas son recibidas correctamente, la secuencia de tramas de la conexión es la siguiente:
Como se envían 10 tramas y se espera la confirmación de cada una de ellas, al no haber retransmisión, el retardo producido por envío de trama y espera de confirmación ACK será de:
Retardo por trama = Tiempo envío trama + Tiempo espera ACK =
= 1 mseg + 2 mseg = 3 mseg.
Como se envían 10 tramas, el retardo total de la transmisión (tiempo de transmisión) será de:
Tiempo de transmisión = 10 x Retardo por trama = 30 mseg.
Podemos observar que la mayor parte del retardo de la transmisión se produce por el tiempo de espera del ACK, que incluye el propio tiempo de transmisión del ACK y de las operaciones de validación por parte del receptor.



Veamos otro **ejemplo**.
Supongamos el mismo sistema o esquema que el anterior ejemplo, es decir, se envían 10 tramas entre dos nodos adyacente con el método de control de flujo. Los tiempos de transmisión son los mismos.
En este caso se produce dos NAK: un NAK 4 y un NAK 8.
Dibuja de nuevo la secuencia de las tramas y calcula de nuevo el tiempo o retardo total de la transmisión.
Solución:
En este caso, se produce la retransmisión de la trama 4 y 8, por lo que el emisor ya no enviará 10 tramas sino 12.
La secuencia de tramas que se produce entre emisor y receptor es la dibujada en el siguiente esquema.



En este caso, el retardo de transmisión por trama recibida correctamente no ha variado:
Retardo por trama = Tiempo envío trama + Tiempo espera ACK =
= 1 mseg + 2 mseg = 3 mseg.
Pero en el caso de que haya retransmisión el retardo por trama será de:
Retardo por retransmisión = Tiempo envío trama + Tiempo espera ACK +
+ Tiempo envío trama + Tiempo espera ACK =
= 1 mseg + 2 mseg + 1 mseg + 2 mseg = 6 mseg.
En nuestro caso se han producido 8 tramas recibidas correctamente y 2 retransmisiones, por lo que el tiempo total (o retardo) de transmisión será de:
Tiempo de transmisión = 8 x Retardo por trama + 2 x Retardo retransmisión
= 8 x 3mseg + 2 x 6 mseg = 36 mseg.
–La capa de enlace de datos es la capa del nivel 2 del modelo OSI encargado de la transmisión fiable de la información entre un nodo y nodo adyacente.
–Para ello implementa métodos de detección y corrección de errores a nivel de trama que es la unidad mínima de información que maneja.
–Dicha capa se subdivide en dos subcapas: la capa MAC más próxima a la capa física y la capa LLC más próxima a la capa de red.
–Son numerosos los métodos de control de línea que trabajan en esta capa como el método de sondeo y selección, el método de ventana deslizante, petición automática de retransmisiones, etc.
–También en esta capa se implementan los métodos de detección de errores como el método del bit de paridad y los métodos CRC.

6. Protocolos

6.1. Protocolos de interconexión de redes. Protocolo IP

El protocolo IP es un protocolo que trabaja a nivel tres del modelo OSI o del modelo TCP/IP.
Se trata de un protocolo basado en datagramas sin conexión y no fiable, es decir, se encarga de enrutar los paquetes de origen a destino buscando la ruta más óptima pero no asegura que el paquete llegue libre de errores ni asegura su recepción. Delega en capas superiores (por ejemplo la capa de transporte) quien deba realizar la detección y corrección de errores.
El protocolo IP 'trocea' la información en paquetes a los que añada la cabecera IP y forman lo que se denomina Datagrama. Estos datagramas se tratan de forma independiente por lo que datagramas del mismo mensaje pueden ser enrutados por rutas diferentes para llegar al mismo destino. Obviamente pueden llegar desordenados y serán las capas superiores las que deban ordenarlos adecuadamente.
La cabecera del datagrama presenta un formato bien definido según el protocolo IP que incluye una serie de campos cuyas funciones se van a describir a continuación.

CABECERA IP

Versión	Longitud Cabecera	Tipo de servicio	Longitud Total
Identificación		Indicadores	Desplazamiento
TTL	Protocolo	Checksum	
Dirección IP origen			
Dirección IP destino			
Opciones			

Versión:
En este campo se define la versión IP del protocolo, es decir, la versión IPv4 que se representa con el valor binario 0110.
Longitud de la cabecera:
Este campo define la longitud de la cabecera como múltiplo de cuatro bytes. Dado que el campo es de 4 bits, la longitud máxima será de $(2^4 -1) \times 4$ bytes= $15 \times 4 = 60$ bytes.
Tipo de servicio:
En este campo se especifica mediante bits o también llamados flags el tratamiento que debe llevar la red en la transmisión del datagrama, es decir, si son datagramas que deban ser priorizados como por ejemplo de tráfico de vídeo o de voz. En la práctica no es tenida en cuenta en la red ya que el tratamiento de los paquetes se gestiona desde capas superiores.
Longitud total:
En este campo se define la longitud total del datagrama IP en bytes. Dado que tiene 16 bits, la longitud máxima será de 2^{16}= 65.536 bytes.
Identificación:
Este campo se utiliza junto con el desplazamiento del fragmento, cuando el datagrama es fragmentado para indicar el número que ocupa en la secuencia la fragmentación.
Indicadores:
Este campo se define mediante flags o bits si el datagrama en cuestión es un fragmento de un datagrama mayor, o si es el primero, el último, etc.

Desplazamiento del fragmento:
En este campo se define el puntero que muestra el desplazamiento del datagrama cuando se produce la fragmentación del mensaje. La posición exacta del fragmento en el paquete IP original
Tiempo de vida (TTL):
En este campo se define el número de saltos (en nodos) que puede dar el datagrama antes de ser descartado. Esto es porque a veces un datagrama por diversas circunstancias o incluso errores en la dirección IP destino no llega a su destino y está constantemente circulando por la red sin rumbo. Pasado un número determinado de saltos o nodos especificados en este campo, si el datagrama no ha llegado al destino automáticamente se elimina de la red.
Protocolo:
En este campo se define el tipo de protocolo de la capa de transporte en la que se encuentra encapsulado el datagrama. Indica la capa de red en el host de destino, para que el Protocolo este paquete pertenece a, es decir, el siguiente nivel. Por ejemplo número de protocolo de ICMP es 1, TCP es 6 y UDP es 17
Suma de comprobación de la cabecera:
Es un checksum que verifica la integridad de la cabecera. Este campo se usa para mantener valor de la suma de todo el cabezal que se utiliza a continuación para comprobar si el paquete es recibido sin error
Dirección IP de origen:
En ella se especifica la dirección IP del que parte el datagrama.
Dirección IP de destino:
En ella se especifica la dirección IP a la que debe ser dirigido el datagrama.
Opciones:
En ella se especifican funcionalidades añadidas que el emisor considere que debe saber el receptor al que va dirigido el datagrama.

6.1.1. Internet y sus organizaciones

Internet no es más que un conjunto de redes interconectadas todas entre sí.
Su ámbito es global, es decir mundial ya que interconecta redes de cualquier parte del mundo y para ello emplea el protocolo TCP/IP.
Su origen se remonta a los años 1960, cuando en plena Guerra Fría entre USA y URSS el Departamento de Defensa americano ordenó una despliegue descentralizado de su Agencia de Inteligencia Militar para evitar que la caída de una de sus sedes (por un ataque enemigo) dejara descabezado el mando militar.
En base a ello, se crearon diferentes sedes militares repartidas espacialmente en diversas partes de los EEUU, pero que debían de estar intercomunicadas entre sí y para ello los investigadores idearon el protocolo TCP/IP, con el cual surgió Arpanet como germen de Internet.
Esta red luego se extendió al ámbito de las investigación en las universidades americanas, hasta que en los años 1990 dio el salto al gran mercado comercial hasta nuestros días
Desde su creación y hasta nuestros días (sobre todo en los últimos lustros), no ha parado de crecer y sobre ella se han implementado numerosos servicios y aplicaciones que lo hace una herramienta esencial en todos los ámbitos de nuestra sociedad: empresarial, económico, social, financiero, industrial, educativo, etc.
Aunque Internet no es propiedad de ninguna organización, empresa o país si en cambio tiene una serie de organismos que se encarga de su gestión para su correcto funcionamiento.
Entre ellos los más destacados son los siguientes:
IETF:
Se trata del cuerpo de ingenieros de Internet y que se dedican a la investigación y al desarrollo de nuevos protocolos y servicios sobre Internet.
ICANN:
Es el organismo encargado de la numeración y asignación IP en Internet.
RIPE:
Es el organismo que asigna grupos de direcciones a los operadores de telecomunicaciones.
NIC
Es el organismo en España dependiente de la entidad Red.es encargada de la gestión de los dominios en Internet.

6.1.2. Direccionamiento IPv4 e IPv6. Creación de subredes

Cualquier equipo o máquina conectado a una red que usa el protocolo TCP/IP debe ser identificado en ella mediante una dirección IP.

Una IP no es más que un número que identifica de manera única a un dispositivo conectado a la red de forma que para dirigirnos a ellas debemos de indicar su IP.

Es como la dirección postal de un lugar al que, si queremos enviar un mensaje, debemos indicar su dirección postal para que dicho mensaje llegue a su destino.

Una IP está asociada a un interfaz de red, por lo que si un dispositivo tiene varios interfaces de red, por ejemplo, varias tarjetas de red, tendrá una IP por cada tarjeta de red instalada.

El dispositivo podrá conectarse a la red de forma cableada o inalámbrica, pero en cualquier caso, es indiferente en cuanto que debe tener una dirección IP.

Formato Dirección IP:

Una dirección IP consta de cuatro octetos (3 bits) separados por puntos. Es lo que se conoce por notación por puntos.

Un ejemplo sería la siguiente:

192.168.0.10

Vemos que existe lo siguiente: 192, 168, 0 y 10 que están separados por puntos.

También lo podemos expresar en binario y la dirección IP sería:

11000000.10101000.00000000.00001010

Este formato es único e invariable en el protocolo IPv4 que es el usado en Internet.

Cada uno de los octetos varía entre 0 y 255 por lo que la menor dirección IP direccionable es:

0.0.0.0

y la mayor dirección IP direccionable será:

255.255.255.255

Luego veremos que dichas direcciones están reservadas y por tanto no se le puede asignar a ninguna máquina o equipo o mejor dicho a ningún interfaz de red.

En una dirección IP se definen dos partes:

- Una parte que identifica a la parte de la red a la que pertenece el equipo o hosts.
- Una parte que identifica al equipo o host en la red.

Cuando hablamos de parte nos referimos a una porción de la dirección IP (el primer octeto, el primer y segundo octeto, los tres primeros octetos, etc.) el cual identifica a la red o identifica al host.

El cómo identificar qué parte pertenece a la parte de la red y qué parte corresponde a la parte del host, dependerá del análisis del octeto y de su rango.

Clases de dirección IP:

Las direcciones IP se clasifican en 5 clases:

CLASE	OCTETOS DE LA PARTE DE RED	OCTETOS DE LA PARTE DE HOST	RANGO
A	1º octecto	2º, 3º y 4º octeto	0.0.0.0 a 127.255.255.255
B	1º y 2º octeto	3º y 4º octeto	128.0.0.0 a 191.255.255.255
C	1º, 2º y 3º octeto	4º octeto	192.0.0.0 a 223.255.255.255
D	-	-	224.0.0.0 a 239.255.255.255
E	-	-	240.0.0.0 a 255.255.255.255

En base a la tabla anterior, podemos identificar en una dirección IP qué octetos pertenecen a la parte de red y qué octetos pertenecen a la parte del host o máquina.
Veremos a continuación y con más detalles cada una de las clases de direcciones IP.

Direcciones IP de clase A:

Estas direcciones se caracterizan porque el primer octeto (los primeros 8 bits) identifican o pertenecen a la dirección de la parte de red y los tres octetos siguientes (los siguientes 24 bits) identifican al host o máquina de la red.
Todas las direcciones pertenecientes a esta clase tienen su primer bit a 0.
El rango de direcciones IP van desde el 0.0.0.0 hasta el 127.255.255.255.
A continuación, veremos en la siguiente tabla el número de redes de clase A que pueden ser direccionadas y el número de host que tiene cada subred.

Nº de redes de clase A	1 octeto = 27 bits= 128 subredes
Nº de hosts	3 octetos= 224 bits -2 = 16.277.214 host (*)

En esta clase de direcciones IP se encuentran las grandes redes, ya que cada subred puede direccionar a un gran número de host.
(*) El número de host ha sido corregido en 2 hosts menos ya que, como veremos más adelante, la primera dirección IP con todos los bits a 0 y la última dirección IP con todos los bits a uno, están reservados para la dirección de la subred y la dirección de broadcast, por lo que no es utilizable para direccionar un host.

Direcciones IP de clase B:

Estas direcciones se caracterizan porque los dos primeros octetos (los primeros 16 bits) identifican o pertenecen a la dirección de la parte de red y los dos octetos siguientes (los siguientes 16 bits) identifican al host o máquina de la red.
Todas las direcciones pertenecientes a esta clase empiezan por 10 (en binario) su primer octeto.
El rango de direcciones IP van desde el 128.0.0.0 hasta el 191.255 .255.255.
A continuación, veremos en la siguiente tabla, el número de redes de clase B que pueden ser direccionados y el número de host que tiene cada subred.

Nº de redes de clase B	26 (primer octeto) x 28 (segundo octeto) = =64 x 256 = 16.384
Nº de hosts	2 octetos= 216 bits -2 = 65.534 host (*)

En esta clase de direcciones IP se encuentra las redes medianas, ya que cada subred puede direccionar a un gran elevado de host.
(*) El número de host ha sido corregido en 2 hosts, menos ya que como veremos más adelante, la primera dirección IP con todos los bits a 0 y la última dirección IP con todos los bits a uno, están reservados para la dirección de la subred y la dirección de broadcast, por lo que no es utilizable para direccionar un host.

Direcciones IP de clase C:

Estas direcciones se caracterizan porque los tres primeros octetos (los primeros 24 bits) identifica o pertenece a la dirección de la parte de red y el cuarto octeto (los siguientes 8 bits) identifican al host o máquina de la red.
Todas las direcciones pertenecientes a esta clase empiezan por 110 (en binario) su primer octeto.
El rango de direcciones IP van desde el 192.0.0.0 hasta el 223.255.255.0.
A continuación, veremos en la siguiente tabla el número de redes de clase c que pueden ser direccionados y el número de host que tiene cada subred.

Nº de redes de clase B	25 (primer octero) x 28 (segundo octeto) x 28 (tercer octeto) = =32 x 256 x 256 =2.097.152
Nº de hosts	1 octetos= 28 bits -2 = 254 host (*)

En esta clase de direcciones IP se encuentra las redes locales (LAN).
(*) El número de host ha sido corregido en 2 hosts menos ya que como veremos más adelante la primera dirección IP con todos los bits a 0 y la última dirección IP con todos los bits a uno están reservados para la dirección de la subred y la dirección de broadcast por lo que no es utilizable para direccionar un host.

Direcciones IP de clase D:

Estas direcciones se caracterizan porque comienzan por 111 los primeros tres bits y son direcciones destinadas a multidifusión.
El rango de direcciones IP van desde el 224.0.0.0 hasta el 239.255.255.255

Direcciones IP de clase E:

Estas direcciones se caracterizan porque comienzan por 1111 los primeros tres bits y son direcciones reservadas para usos futuros.
El rango de direcciones IP van desde el 240.0.0.0 hasta el 255.255.255.255

Direcciones Reservadas:

Hay una serie de direcciones que no pueden ser utilizadas para un interfaz de red. Son las direcciones reservadas o especiales.
En todas las subredes definidas anteriormente existen siempre dos direcciones reservadas:

La dirección de red:

Es la dirección IP que tiene la parte de Host todos a 0.

La dirección de broadcast:

Es la dirección IP que tiene la parte de Host todos a 1.

Veamos un **ejemplo**:
En la dirección IP 192.168.0.10 lo pasamos a binario y su dirección IP será:

$$192.168.0.10_{(10)} = 11000000.10101000.00000000.00001010_{(2)}$$

Como se puede comprobar, es una dirección que empieza por 110, es decir, es una dirección de clase C, donde los tres primeros octetos pertenecen a la parte de red y el último a la parte de host.

- ⇨ Parte de subred = 192.168.0
- ⇨ Parte de host= 10

La dirección de red será aquella en la que la parte de host tenga todos sus bits a 0, es decir:

- ⇨ Dirección IP de subred = 192.168.0.0

La parte de broadcast (transmisión) será aquella en la que la parte de host tenga todos sus bits a 1, es decir:

- ⇨ Dirección IP de broadcast = 192.168.0.255

Veamos otro **ejemplo**:
Averigua la clase de la siguiente dirección IP y di además cuál es su dirección de subred y cuál es su dirección de broadcast:

Dirección IP = **150.40.0.80**

Para ello pasamos la dirección IP a binario y nos queda:

$$150.40.0.80_{(10)}=10010110.00101000.00000000.01010000_{(2)}$$

Como la dirección IP comienza por 10 luego se trata de una dirección IP de clase B.
Su dirección IP de subred será con su parte de host puesto todos a 0, es decir, el 3º y 4º octeto puesto a 0.

- ⇨ Dirección IP de subred = 150.40.0.0

Y su dirección de broadcast será aquella con su parte de host puesto todos a 1, es decir, el 3º y 4º octeto puesto a 1.

- ⇨ Dirección IP de broadcast = 150.40.127.255

Más adelante, veremos que esta dirección de clase B, es realmente el tercer octeto, aunque no los tiene todos a 1, puesto que esta dirección de clase B tiene dos subredes y la IP del host 80 pertenece a la primera subred.

Veamos un último **ejemplo** sobre direcciones IP y sus clases:
Dada la dirección IP 142.226.0.15, indica cuál es su clase y qué parte de la dirección pertenece a subred y cuál al host, e indica por último a cuántos hosts de una misma subred puede direccionar.
Solución:
Para averiguar a qué clase pertenece, pasamos la dirección IP a binario y nos queda:

$$142.226.0.15_{(10)} = 10001110.11100010.00000000.00001111_{(2)}$$

Dado que comienza por 10, se trata de una dirección IP de clase B y por tanto, los dos primeros octetos pertenecen a la parte de subred y los dos octetos siguientes (tercero y cuarto) pertenecen a la parte de host.
El número de hosts que puede direccionar esta dirección de red dentro de la subred 142.226 será la de 28 (tercer octeto) x 28 (cuarto octeto) = 256 x 256 = 65.536 -2 (dirección de subred y broadcast) = 65.534 hosts.

En una red como, por ejemplo, Internet se pueden dar dos casos de Direcciones IP:

- Una dirección IP pública.
- Una dirección IP privada.

Una dirección IP privada es aquella que pertenece a un entorno privado, por ejemplo, una LAN
Una dirección IP privada es aquella que pertenece a un entorno privado, por ejemplo, una LAN en la cual asignamos dirección IP a nuestros equipos que forman la red. Su gestión y administración corresponde al administrador de red.
Fuera de esa red privada (LAN), esa dirección IP no es direccionable (no es enrutable por el router), y por tanto dichas direcciones se pueden replicar en múltiples redes privadas.
Una dirección IP pública es aquella que es enrutable por el router y pertenece al dominio de Internet, por tanto, su gestión y administración pertenecen a los organismos nacionales e internacionales de asignación de IPs.
En consecuencia de lo anterior, las direcciones IP públicas son únicas en Internet (sólo un equipo puede tener la misma IP), pero en cambio las direcciones IP privadas pueden estar replicadas en múltiples locales diferentes.
Otra clasificación que puede realizarse con las direcciones IP es:

- IP fija.
- IP dinámica.

Una dirección IP fija es aquella que es asignada a un interfaz de red (equipo o máquina) y permanece fija y constante en el tiempo. Es el caso de las direcciones de los servidores de red.
Una dirección IP dinámica es aquella que es asignada temporalmente a un interfaz de red (equipo o máquina). Es el caso de asignación de IP en las redes locales cuando existe un servidor DHCP.
Esta clasificación no es incompatible con la clasificación de IP pública y privada descrita anteriormente.
De hecho en las redes locales pueden darse dos casos:

- Son IP privadas pero pueden ser fijas, es decir, las asigna el administrador de red de forma manual.
- Son IP privadas pero pueden ser dinámicas, es decir, las asigna un servidor de DHCP.

Por operatividad, éste último es el que se emplea.
Para las redes públicas pueden darse los mismos dos casos:

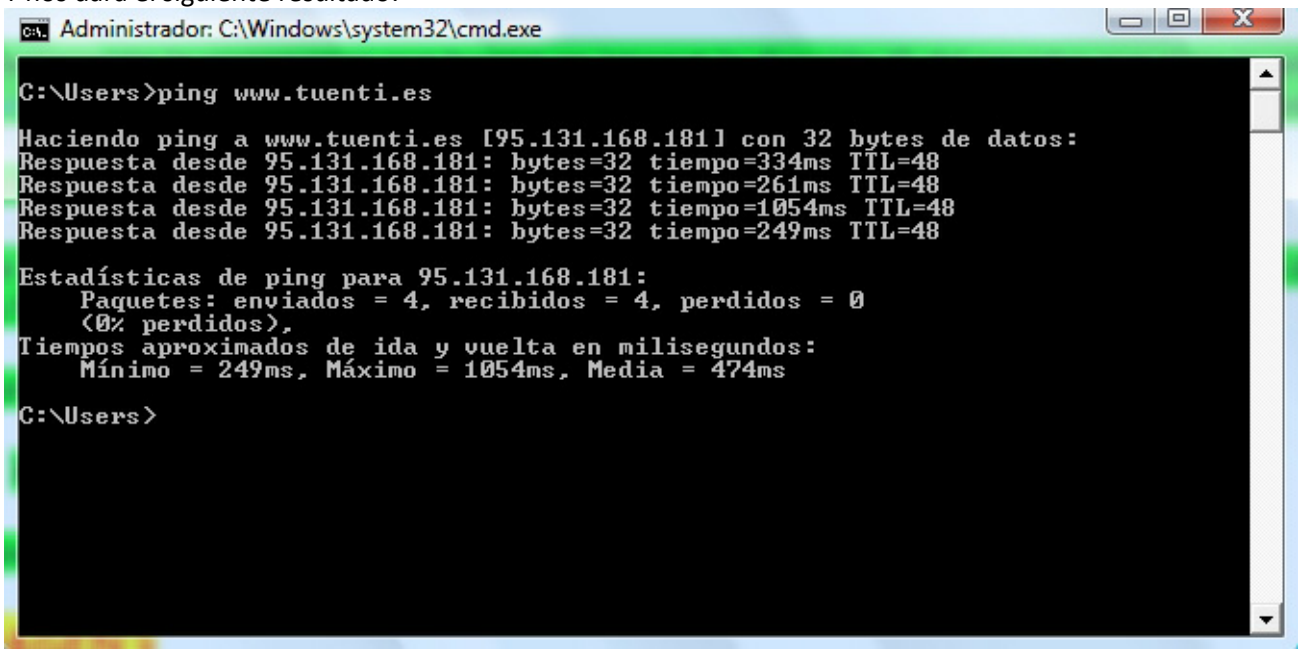
- Un servidor o equipo con una dirección IP pública pero fija. Es el caso de los servidores de Internet como servidores DNS, de búsqueda (Google, Yahoo, etc.).
- Un servidor o equipo con una dirección IP pública pero dinámica. Es el caso de los router que se conectan a Internet, que en el ámbito de Internet tiene una dirección pública pero dinámica al ser asignado temporalmente por el operador.

Por tanto ambas clasificaciones de direcciones IP se refieren a aspectos diferentes y pueden combinarse entre sí, dando lugar a diferentes configuraciones.

Ejemplo:
A continuación, te proponemos que busques en Internet la dirección IP del servidor que aloja la web de www.tuenti.es, y digas si es una dirección IP pública o privada y si es fija o dinámica. Razona la respuesta.
Solución:
Para averiguar la dirección IP de una página web hay numerosas formas de hacerlo, aunque una de las más habituales y más sencilla es utilizando el comando ping a esa web.
Así en la consola de comandos realizamos:

Ping www.tuenti.es

Y nos dará el siguiente resultado:



Nos da como resultado que la dirección IP es 95.131.168.181. Es decir se trata de una dirección de clase A. La dirección es una dirección pública, ya que dicha página es visualizada desde cualquier equipo conectado a Internet y no sólo desde nuestro ámbito privado. Se trata además de una IP fija, ya que cada vez que lo direccionamos desde nuestro navegador con la URL www.tuenti.es, el servidor DNS asocia dicha URL a dicha dirección IP. Si fuese dinámica, tendría que ir actualizando constantemente la asociación de la URL a la nueva dirección IP del servidor que aloja la aplicación web.

Dirección MAC:

Se define dirección MAC (Media Access Control address) como la dirección física de un interfaz de red.
Es decir, todas las tarjetas de red como dispositivo electrónico tienen una dirección física (como si fuera el número de serie), que es un identificador de 48 bits (6 bytes) en formato hexadecimal, que lo identifica de manera única.
A diferencia de la dirección IP (que es asignado por la red) y puede variar, la dirección MAC es fija e invariable (aunque para esto último existen hoy día herramientas para modificarlas).
Estas direcciones MAC son únicas ya que son 'grabadas' directamente por el fabricante en el chipset de la tarjeta de red.
Estas direcciones MAC son utilizadas por algunos protocolos para asociar direcciones MAC con direcciones IP.

Asignación de direcciones IP:

Hemos visto anteriormente que las direcciones IP pueden ser fijas o dinámicas. En base a esto, cuando un equipo o máquina se conecta a una red que dispone de un servidor DHCP, hay que asignarle una dirección IP y su asignación puede realizarse de tres formas:

Una asignación IP asociada a su MAC.

En este caso el servidor DHCP tiene configurado una tabla de direcciones IP con direcciones MAC de los equipos. Cuando un equipo se conecta a la red, comprueba que la MAC de dicho equipo (realmente la de su tarjeta de red) y si está en la lista le asigna la dirección IP que le corresponde según la tabla.

Si la MAC no está en la lista, sencillamente no le da dirección IP y por tanto no se puede conectar a la red.

Este sistema se emplea mucho para controlar el número y qué equipos pueden conectarse a una red LAN concreta.

Una asignación IP fija

En este caso, cuando el equipo o máquina se conecta a la red, el servidor DHCP le asigna una dirección IP libre en ese momento, y queda asignada esa dirección IP a esa MAC de ese equipo, no pudiéndose reutilizar dicha IP para otro equipo, ya que ha sido asignado al primero.

Este sistema es poco eficiente, ya que si ese equipo es baja del sistema, realmente se 'pierde' una dirección IP asignable.

Asignación dinámica IP.

En este caso, cuando el equipo o máquina se conecta a la red, el servidor DHCP le asigna una dirección IP libre en ese momento, pero que quedará libre de nuevo cuando el equipo es bajo o se desconecta, pudiéndose reasignárselo a otro. Por tanto, dicha IP no queda asignada a una MAC de forma constante (sólo durante la conexión) y consigue con ello una eficiencia en la gestión de las IP del sistema.

Este último caso es el caso más habitual empleado actualmente en la asignación de IP en todas las redes locales e incluso en redes metropolitanas por la eficiencia anteriormente descrita.

Máscara de red:

La máscara de red es una combinación de bits que se emplea junto la dirección IP para indicar qué parte de la dirección IP pertenece a la subred y que parte de la dirección IP pertenece al host.

Esto permite a los protocolos de comunicaciones y en concreto a los router, saber si una dirección IP debe ser enrutada dentro o fuera de la red que gestiona el router.

La máscara de red tiene, al igual que la dirección IP, una notación por puntos, es decir, se trata de 4 octetos separados por puntos.

Un ejemplo sería:

255.255.255.0

A diferencia de las direcciones IP, no todos los números son posibles sin un determinado número de valores.

La máscara de red, junto con la dirección IP, son los dos parámetros necesarios para crear subredes dentro de Internet.

Puerta de enlace:

Se define la puerta de enlace con la dirección IP del equipo o máquina, que siendo parte de la red, proporciona la salida para salir de ella.

Generalmente es la dirección IP del router o del servidor, que actúa como router.

El router además suele incluir el protocolo NAT que, como veremos más adelante, permite enmascarar las direcciones IP privadas dentro de la red pública (Internet, y con ello permitir que muchos equipos conectados a una red local puedan compartir la misma conexión de Internet.

El router, por tanto, tendrá un dirección pública de cara a Internet y una dirección privada que será la puerta de enlace.

Configuración de un equipo en la red:

Una vez visto todo lo anterior, podemos resumir que cuando un equipo o máquina se conecta a una red, es preciso configurarle los siguientes parámetros de red (manualmente o mediante un servidor DHCP):

- Dirección IP.
- Máscara de red.
- Puerta de enlace.

También veremos más adelante que será necesario además configurarle la dirección de al menos un servidor DNS, generalmente uno primario y otro alternativo, para que puedan ser traducidas las direcciones URL de nuestro navegador a direcciones IP de las webs solicitadas.
También cabe destacar que la puerta de enlace no es estrictamente necesaria configurarla (pero altamente recomendable) ya que sin ella no tendremos conexión a Internet, aunque podremos comunicarnos con los equipos de nuestra propia red local.

Creación de subredes:

La asignación de direcciones IP por clases (A, B, C, D y E) es un sistema muy rígido para crear redes y subredes.
Para solucionar esto, se emplea la mascara de red (vista anteriormente) para que junto con la dirección IP sirva para crear subredes.
Como ya se ha descrito anteriormente, la máscara de subred es una secuencia de 4 octetos en el cual sólo es posible un determinado número de valores.
El objetivo de la máscara de red es identificar qué parte de la dirección IP de la máquina o equipo pertenece a la dirección de red, y qué parte (u octetos) pertenecen a la parte del host.
Así, poniendo a 1 los bits más significativos (empezando por la izquierda) de la máscara de red, indican (por asociación lugar) qué parte de la dirección IP es la parte de subred y cuál es la parte de host.

Ejemplo:
Dada la dirección IP 192.168.90.10 y con máscara 255.255.255.0, indica qué parte de la dirección IP representa la parte de subred y cuál representa la parte de host.
Solución:
En primer lugar, pasamos la dirección IP y la máscara de red a binario:

$$192.168.90.10_{(10)} = 11000000.10101000.01011010.00001010_{(2)}$$
$$255.255.255.0_{(10)} = 11111111.\ 11111111.\ 11111111.00000000_{(2)}$$

La máscara de red tiene sus tres primeros octetos puesto a 1, y por la asociación vista anteriormente, nos indica entonces que los tres primeros octetos de la dirección IP pertenece a la red y el cuarto pertenece a la dirección de host.
Por tanto, para este ejemplo, esa dirección IP pertenece a un host que está en la red con dirección 192.168.90.0 y el host es el número 10, y por eso tiene la dirección IP 192.168.90.10.
Con la máscara de red se puede obtener además la dirección de red, y la dirección de broadcast de la red, según se ha descrito en anteriores capítulos.
Para ello:
–Para obtener la dirección de subred, se debe aplicar la operación AND entre la IP del equipo y la máscara de red.
–Para obtener la dirección de broadcast, se debe aplicar la operación OR entre la IP del equipo con la NOT de la máscara de red.

Veamos esto con el **ejemplo** descrito anteriormente.
Dada la dirección IP 192.168.90.10 y con máscara 255.255.255.0, indica la dirección IP de la subred a la que pertenece el host y la dirección de broadcast.
Solución:
Para obtener la dirección de subred, debemos realizar la operación de AND entre la dirección IP y la máscara de red:

192.168.90.1010 = 11000000.10101000.01011010.000010102

AND

255.255.255.010 = 11111111. 11111111. 11111111.000000002

y el resultado es 192.168.90.1010 AND 255.255.255.010

11000000.10101000.01011010.000000002 = 192.168.90.010

Para obtener la dirección de broadcast, debemos aplicar la operación OR entre la dirección IP y NOT de la máscara de red.

192.168.90.1010 = 11000000.10101000.01011010.000010102

OR

0.0.0.25510 = 00000000.00000000.00000000.111111112

y el resultado es 192.168.90.1010 OR (NOT) 255.255.255.010

11000000.10101000.01011010.111111112 = 192.168.90.25510

Veamos un **ejemplo** más de cómo averiguar la dirección de subred y la dirección de broadcast con la máscara de red.
Dada la dirección IP 18.120.16.255 y con máscara 255.255.0.0, indica la dirección IP de la subred a la que pertenece el host y la dirección de broadcast.
Solución:
Para obtener la dirección de subred debemos de realizar la operación de AND entre la dirección IP y la máscara de red:

$18.120.16.255_{(10)}$ = 00010010.01111000.00010000.$11111111_{(2)}$

AND

$255.255.0.0_{(10)}$ = 11111111. 11111111. 00000000.$00000000_{(2)}$

y el resultado es $18.120.16.255_{(10)}$ AND $255.255.0.0_{(10)}$

$00010010.01111000.00000000.00000000_{(2)}$ = $18.120.0.0_{(10)}$

Para obtener la dirección de broadcast debemos de aplicar la operación OR entre la dirección IP y NOT de la máscara de red.

$18.120.16.255_{(10)}$ = 00010010.01111000.00010000.$11111111_{(2)}$

OR

0.0.255.255(10) = 00000000.00000000.11111111.11111111(2)

y el resultado es 18.120.16.255(10) OR (NOT) 255.255.0.0(10)

00010010.01111000. 11111111.11111111(2) = 18.120.255.255(10)

Como ya se ha comentado anteriormente, la máscara de red sólo puede adoptar determinados valores, es decir, cada octeto tendrá que poner sus bits a 1 de forma consecutiva, por lo que los valores que puede adoptar (cada octeto) serán las siguientes:

0 = 0000000
128 = 10000000
192 = 11000000
224 = 11100000
240 = 11110000
248 = 11111000
252 = 11111100
254 = 11111110
255 = 11111111

Con todos estos valores de la máscara se pueden generar numerosas subredes más allá de los valores 0 y 255, que hasta ahora hemos considerado en los octetos de la máscara de red.
Adoptando un valor de 0, 128, 192, 224, 240, 248, 252, 254 y 255, podemos crear diferentes subredes y donde una dirección IP puede pertenecer a cualquier de las subredes generadas.
Esto se emplea para separar lógicamente equipos (aunque físicamente compartan la misma red), y con ello crear grupos de trabajo pero que además puedan compartir determinados equipos y aplicaciones en red, como por ejemplo, el router que da el acceso a Internet.
También pueden compartir recursos como un servidor de datos, un servidor web, una impresora, etc.

Ejemplos:

Mascara 255.255.255.0 = Formato CIDR /24

Solo 1 subred Permitida – 254 Host por subred

192.168.1.0 : Dirección de Red (Dirección NO utilizable)
192.168.1.1 - 192.168.1.254 (Rango de Direcciones Válidos)
192.168.1.255: Dirección de Broadcast (Dirección NO utilizable)

Mascara 255.255.255.128 = Formato CIDR /25

2 subredes Permitidas – 126 Host por subred

1ª Subred:

192.168.1.0 : Dirección de Red (Dirección NO utilizable)
192.168.1.1 - 192.168.1.126 (Rango de Direcciones Válidos)
192.168.1.127: Dirección de Broadcast (Dirección NO utilizable)

2ª Subred:

192.168.1.128 : Dirección de Red (Dirección NO utilizable)
192.168.1.129 - 192.168.1.254 (Rango de Direcciones Válidos)
192.168.1.255: Dirección de Broadcast (Dirección NO utilizable)

Mascara 255.255.255.192 = Formato CIDR /26

4 subredes Permitidas – 62 Host por subred

1ª Subred:

192.168.1.0 : Dirección de Red (Dirección NO utilizable)
192.168.1.1 - 192.168.1.62 (Rango de Direcciones Válidos)
192.168.1.63: Dirección de Broadcast (Dirección NO utilizable)

2ª Subred:

192.168.1.64 : Dirección de Red (Dirección NO utilizable)
192.168.1.65 - 192.168.1.126 (Rango de Direcciones Válidos)
192.168.1.127: Dirección de Broadcast (Dirección NO utilizable)

3ª Subred:

192.168.1.128 : Dirección de Red (Dirección NO utilizable)
192.168.1.129 - 192.168.1.190 (Rango de Direcciones Válidos)
192.168.1.191: Dirección de Broadcast (Dirección NO utilizable)

4ª Subred:

192.168.1.192 : Dirección de Red (Dirección NO utilizable)
192.168.1.193 - 192.168.1.254 (Rango de Direcciones Válidos)
192.168.1.255: Dirección de Broadcast (Dirección NO utilizable)

Mascara 255.255.255.224 = Formato CIDR /28

8 subredes Permitidas – 30 Host por subred

6.1.3. Enrutamiento

El enrutamiento también denominado encaminamiento, o simplemente ruteo es la técnica basada en buscar un camino de entre muchos posibles para transmitir un paquete de un punto a otro en base a unos criterios.

Estos criterios están basados en buscar la mejor ruta que puede ser:

- El más corto.
- El de menor coste.
- El de menos tráfico o carga de red.
- Combinaciones de varias.

Por tanto, el criterio para buscar la mejor ruta depende muchos factores.

Existen diferentes algoritmos (basado sobre todo en teoría de grafos) para calcular la ruta óptima.

6.1.4. Clasificación de los métodos de enrutamiento

Como se ha descrito anteriormente, existen diferentes métodos o algoritmos de encaminamiento.

Estos algoritmos pueden clasificarse en:

- **Estáticos**:
  Existe una tabla predefinida donde se indica la ruta por la que debe seguir cada paquete y no se tiene en cuenta el estado de la red en cada momento.
  Son por tanto algoritmos poco eficientes, al no adaptarse a los cambios de la red.
  Son algoritmos rígidos, rápidos y de diseño rápido. Un ejemplo es el algoritmo de Dijkstra.
- Algoritmos adaptativos o **dinámicos**:
  Son algoritmos que se adaptan al estado de la red en cada momento. Dispone de una tabla de encaminamiento que se va adaptando en función de varios parámetros.
  Son algoritmos más complejos pero más eficientes.

6.1.5. BGP (Border Gateway Protocol)

Se trata de un algoritmo de encaminamiento entre sistemas autónomos muy usado en Internet.

Están basados en tablas de rutas que son almacenadas en los Gateways de la red.

En este protocolo se intercambia información entre los diferentes sistemas autónomos de una red, de forma que se garantiza en todo momento rutas libres para la transmisión de paquetes.

Es un protocolo ampliamente utilizado por las compañías ISP, ya que no utiliza para el cálculo de las rutas ópticas el número de saltos, retardos en la transmisión, etc.

El protocolo BGP utiliza el denominado protocolo vector de caminos para intercambiar la información del router entre los diferentes equipos de interconexión de la red.

De esta forma, se pueden conocer las rutas ópticas para cada tipo de paquete.

6.1.6. OSPF (Open Shortest Path First)

Se trata de otro algoritmo de encaminamiento basado en el algoritmo de Dijkstra, aunque con matizaciones, ya que se trata de una técnica de encaminamiento adaptativo.

Su funcionamiento está basado siempre en la búsqueda de la ruta de menor coste.

Es habitual que las redes que emplean OSPF estén segmentadas en redes más pequeñas, pero una de ellas constituye lo que se denomina el backbone, es decir, es la red principal al que se conectan todas ellas.

Las rutas establecidas según este algoritmo siempre pasan por este backbone por lo que el control de tráfico de esta red principal forma parte de los criterios utilizados para establecer las rutas óptimas de la red.

Este algoritmo es ampliamente utilizado en grandes redes por su eficiencia (es adaptativo), y donde además cuenta con una red principal (backbone), en la cual suelen estar todos los equipos mallados para dar robustez al sistema.

6.2. Protocolo de transporte

El protocolo de transporte, como ya se ha visto anteriormente, define una serie de reglas que trabajan en el nivel 4 del modelo OSI o del modelo TCP/IP.
Su misión principal es asegurar la transmisión fiable extremo a extremo de la información enviada, es decir, que el mensaje llegue al destinatario de forma correcta, de forma ordenada y sin errores.
Para ello, emplea diversas técnicas de corrección de control de flujo y control de errores, como pueden ser en este último caso, las retransmisiones de los paquetes.
Este protocolo de transporte tiene dos implementaciones que veremos con más detalle a continuación:

- Protocolo TCP.
- Protocolo UDP.

6.2.1. Protocolo TCP (Transmission Control Protocol)

TCP es un protocolo del nivel de transporte orientado a conexión y es por ello un protocolo que asegura una transmisión fiable de la información.
El que sea un protocolo orientado a conexión significa que antes de enviar cualquier información el protocolo crea una conexión virtual (un túnel) entre emisor y receptor que es por donde viajarán todos los paquetes.
Dicha conexión virtual se libera cuando acaba la transmisión.
Por tanto, en este protocolo se establecen los siguientes pasos:

- Establecimiento de una conexión entre emisor y receptor.
- Envío de paquetes por la conexión establecida.
- Liberación de la conexión.

Durante la conexión se establecen mecanismos de control de errores como control del flujo y retransmisiones de paquetes con errores.
Este protocolo TCP, a diferencia del protocolo UDP que veremos más adelante, sacrifica velocidad de transmisión a favor de la fiabilidad de la transmisión.
Sacrifica velocidad porque requiere un establecimiento de la velocidad y un control de flujo antes del envío de los paquetes, además de liberar la conexión cuando se termina la transmisión. Esto genera retardos (bajada de velocidad) pero se consigue fiabilidad en la transmisión ya que nos asegura que los paquetes llegarán de forma correcta y sin errores al receptor.
Es por ello que la cabecera del protocolo TCP es de mayor tamaño al incluir numerosos campos de control de errores y control de flujos.
Este protocolo se emplea para aplicaciones, como no se permiten errores en la transmisión como el correo electrónico, la navegación web, la transferencia de archivos, etc., donde es preciso asegurar la transmisión fiable aunque se incluya por ello milisegundos de retardo.
El protocolo TCP como todos los protocolos del modelo OSI o del modelo TCP/IP adhiere al mensaje una cabecera, es decir, la cabecera de transporte dando lugar a lo que se denomina segmento TCP que es lo que se envía por la red.
Esta cabecera TCP consta de los siguientes campos y que veremos con más detalle a continuación:

CABECERA TCP

Como ya se ha comentado anteriormente, a diferencia del protocolo UDP esta cabecera es de mayor longitud al incluir numerosos campos de control de flujo y control de errores.

Dirección del puerto de origen:

Se trata de un campo de 16 bits donde se indica el puerto de la máquina origen de la que parten los paquetes, es decir, de la aplicación que abre la conexión.

Dirección del puerto de destino:

Se trata de un campo de 16 bits donde se indica el puerto de la máquina destino a la que van dirigido los paquetes, es decir, de la aplicación que debe recibir la información.

Número de secuencia:

Cuando la información que se quiere transmitir es muy larga, el protocolo lo 'trocea' en segmentos y los envía de forma individual por la red (para asegurar el control de flujo y aplicar mejor el control de errores). Luego en el destino estos segmentos se deben de 'reensamblar' para mostrárselo al destino de forma ordenada y correcta.
Este campo indica el número que ocupa dicho segmento que forma parte de un mensaje que se ha 'troceado', para que luego en el destino pueda ser 'reensamblado' correctamente.

Número de confirmación:

Como el protocolo TCP es un protocolo fiable y orientado a conexión, para asegurar que el segmento enviado ha llegado correctamente, espera que el receptor le envíe una confirmación de recepción (un ACK). Durante la conexión habrá tantos ACK como paquetes se haya enviado, y en este campo se especifica el número de ACK siguiente que espera el emisor de confirmación por parte del receptor antes de enviar el siguiente paquete.

Longitud de cabecera (HLEN).

La cabecera del protocolo TCP tiene un tamaño mínimo de 20 bytes y un tamaño máximo de 60 bytes segmentado en trozos de 32 bits. En este campo se indica el número de 32 bits de longitud de la cabecera. Tiene cuatro bits ya que con estos cuatros bits se puede representar los 24=16 números posibles de 32 bits que puede tener la longitud de la cabecera.

Reservado.

Es un campo que en IPv4 no tiene función.

Bits de control o flags:

En la cabecera TCP existen seis bits de control donde cada uno de ellos tiene una función específica:

- Bit URG: Indica a la red que este segmento contiene información que debe ser priorizada en la transmisión. En la práctica la priorización de los paquetes la determinan capas superiores (nivel de aplicación) por lo que no tiene efecto práctico alguno el activar o desactivar este bit.
- Bit ACK: Si está activo indica que dicho segmento ha sido validado por el receptor, es decir, el receptor confirma que dicho paquete ha llegado correctamente y sin errores.
- Bit PSH: Este bit (bit de PUSH) se utiliza para forzar el enviado inmediato de los datos tan pronto como sea posible. Si el TCP emisor envía un paquete con este flag activado, el TCP receptor sabe que tiene que entregar los datos inmediatamente a la aplicación receptora sin ponerlo en un buffer y esperar a más datos.
- Bit RST: Este bit (bit de RESET) se utiliza para forzar un reinicio de la conexión ya que se ha producido un error en los números de secuencia que obliga a retransmitir de nuevos los segmentos.
- Bit SYN: Este bit (bit de SYNCRONIZACION) se utiliza para sincronizar los números de secuencia.
- Bit FIN: Este bit se utiliza para liberar la conexión.

Tamaño de la ventana:

Indica el número de segmentos que se pueden enviar sin esperar confirmación ACK por parte del receptor. Pasado ese número de segmentos, no se enviarán más segmentos hasta que no se espere confirmación de los segmentos anteriormente enviados. Actúa como buffer de salida.
Es un campo de 16 bits por lo que pueden enviarse 216=65.536 segmentos sin confirmación.

Suma de comprobación:

Se utiliza para la detección de errores.

Puntero urgente:

Este campo junto con el bit URG es activado por el emisor para indicar al receptor que hay datos urgentes en el trozo de segmento que se está enviando, para que sea tenido en cuenta.

Opciones y relleno:

Es un campo donde se incluye información adicional que el emisor quiere enviar al receptor y cuya longitud dependerá de la información que incluya hasta el máximo permitido por la cabecera del protocolo TCP.

6.2.2. Protocolo UDP (User Datagram Protocol)

UDP es un protocolo del nivel de transporte no orientado a conexión y es por ello un protocolo que no asegura una transmisión fiable de la información.
El que sea un protocolo orientado a no conexión significa que no se crea ninguna conexión virtual entre el emisor y receptor (a diferencia del protocolo TCP), y por ello los segmentos UDP pueden ir por diferentes rutas (dependiendo de la carga y congestión de la red), dando lugar a que lleguen al receptor de forma desordenada, con errores o incluso que no llegue.
Serán los niveles superiores (los de aplicación) los que deberán corregir los errores producidos en la transmisión.
La ventaja de este protocolo (que no es fiable en la transmisión de la información) es su velocidad, ya que sacrifica la fiabilidad en beneficio de aumentar su velocidad de transmisión (no requiere retardos por establecimiento de conexión, confirmación de ACK, liberación de conexión, etc.).
Este protocolo se emplea para servicios de datos como streaming de video, VoIP, etc., donde es importante la velocidad (son servicios críticos en el tiempo) y donde si se pierde un segmento, apenas se percibe pero se asegura la velocidad de la transmisión.
Al igual que TCP, este protocolo UDP añade una cabecera al paquete procedente de los niveles superiores dando lugar al datagrama UDP que es lo que se transmite.
Al no realizar control de errores ni control de flujo, esta cabecera incluye pocos campos y es por ello una cabecera de longitud corta.

CABECERA UDP

Dirección puerto origen	Dirección puerto destino
Longitud total	Checksum

Veremos a continuación y con más detalles el significado y función de cada uno de los campos que componen la cabecera UDP.

Dirección del puerto de origen:

Se trata de un campo de 16 bits donde se indica el puerto de la máquina origen de la que parte los datagramas, es decir, de la aplicación que envía dichos datagramas.

Dirección del puerto de destino:

Se trata de un campo de 16 bits donde se indica el puerto de la máquina destino a la que va dirigidos los datagramas, es decir, de la aplicación que debe recibir la información.

Longitud total:

En este campo se define la longitud total en bytes que tiene el datagrama en bytes. Como es de 16 bits la longitud máxima del datagrama será de 216= 65536 bytes.

Suma de comprobación:

Es un campo de 16 bits utilizado para la detección de errores. Realmente representa un checksum del datagrama enviado.
UDP sólo proporciona las funciones necesarias para la entrega de datagramas extremo a extremos donde no garantiza que lleguen todos los datagramas al destinatario y en el orden correcto.
Proporciona un control de errores que advierte que el paquete recibido tiene errores pero no los corrige, sino que los notifica para que aplicaciones superiores realicen la corrección de errores necesarios.
UDP es generalmente el protocolo usado en la transmisión de vídeo y voz a través de una red, ya que al ser servicios en tiempo real no hay tiempo para enviar de nuevo paquetes perdidos cuando se está escuchando a alguien o viendo un vídeo en tiempo real. Se pierde fiabilidad a favor de la velocidad.

A continuación mostramos en una tabla las **diferencias sustanciales entre los protocolos TCP y UDP** vistos anteriormente.

PROTOCOLO TCP	PROTOCOLO UDP
Orientado a conexión	Orientado a no conexión
Fiable en la transmisión	No fiable en la transmisión
Realiza control de flujo, detección de errores y corrección de errores (retransmisiones)	No realiza control de flujo, detecta errores pero no los corrige
Es más lento a favor de la fiabilidad	Es más rápido en detrimento de la fiabilidad
No apto para aplicaciones en tiempo real	Apto para aplicaciones en tiempo real

6.2.3. Puertos

Se define puerto como un interfaz mediante el cual un programa o aplicación puede comunicarse con la red. De la gestión de los puertos y su administración se encargan los protocolos del nivel de transporte, es decir, los protocolos TCP y UDP vistos anteriormente.
Los puertos están numerados según una tabla definida por la entidad IANA, que se encarga de describir para qué aplicaciones se emplea cada puerto.
Así, dependiendo de la aplicación que emplee la red usará un puerto u otro, y es por ello, que para el empleo de estas aplicaciones el puerto debe estar habilitado (abierto).
La existencia de los puertos permite que cada equipo pueda tener establecidas múltiples conexiones con una o varias máquinas, pero cada conexión trabaja con un puerto diferente. Así, podemos tener abierta una aplicación de correo electrónico (que emplea el puerto 25) y una aplicación de FTP (que emplea el puerto 21).
Existen 2^{16} puertos, es decir, 65535 puertos aunque no todos se usan. En cambio otros están reservados para aplicaciones específicas que veremos a continuación.

En la siguiente tabla se muestran aquellos puertos que están reservados para las aplicaciones más habituales usadas en Internet.

Puerto	Aplicación que lo emplea
20 y 21	Aplicaciones de FTP
22	Aplicaciones SSH
23	Aplicaciones de TELNET
25	Aplicaciones de SMTP
80	Aplicaciones de http
110	Aplicaciones de POP3
143	Aplicaciones de IMAP
161	Aplicaciones de SNMP
389	Aplicaciones de LDAP

El resto de los puertos están reservados a aplicaciones del sistema operativo o no tienen uno predefinido.

6.2.4. NAT (Network Address Translation). Direccionamiento

En una red existen dos tipos de direcciones:

- Direcciones públicas.
- Direcciones privadas.

Ambos, evidentemente manteniendo el mismo formato de cuatro octetos pero que difieren en el ámbito en que opera: un ámbito global (dirección pública) o un ámbito local (dirección privada).

En la asignación de las IP existen una serie de direcciones IP destinadas a direcciones públicas y una serie de IP destinadas a direcciones privadas. Estas últimas tienen un uso local, por lo que no son enrutables por parte de los router, es decir, no 'las entiende' y por tanto no las enrutan.

Esto es lo que permite que Internet esté formado por múltiples redes locales, de forma que una misma dirección privada, por ejemplo, la 192.168.0.10 pueda ser utilizada en diferentes redes privadas porque sencillamente no pasan del router y por ello no hay conflicto de IP en la red.

Esto no pasa con las redes públicas cuyo ámbito es global en toda la red y sólo puede ser utilizado en un único equipo o host, por ejemplo, 66.90.10.74.

Imaginemos ahora el siguiente caso:

Una red de área local (LAN) en el cual un equipo con IP 192.168.10.15 está realizando una navegación web y solicita la dirección de Google, es decir, 173.194.34.248. Hasta ahora no hay problema porque el router encamina mi petición a Internet y en el segmento TCP va nuestra dirección IP (la 192.168.10.15), entonces, según lo dicho anteriormente el router no puede enrutar dicha dirección privada en Internet y por tanto en teoría no será atendida nuestra solicitud.

Como sabemos, nuestra solicitud es atendida y el router nos devuelve la web de Google a nuestro navegador. Ello es gracias al protocolo NAT.
NAT es un protocolo que traduce IP privadas en IP públicas y básicamente lo que realiza es encapsular nuestra dirección privada (192.168.0.10) en una dirección pública de Internet (la del router) y cuando le llega la respuesta del servidor (que va a la dirección pública que es la del router) éste desencapsula la dirección privada para enviarla al equipo de la red local que ha hecho la petición.

6.3. Seguridad en redes

La seguridad en las redes es un concepto que cada vez más se tiene en cuanto en este mundo hiperconectado.
Hasta hace poco las redes sólo eran utilizadas por determinadas multinacionales y organizaciones por lo que su seguridad también estaba acotado a ellos.
Hoy día, todo el mundo (empresas, organizaciones, particulares e incluso objetos) está conectado a la red (generalmente a Internet) y es por ello que cada vez surge más el concepto de seguridad en las redes, como aquel que permita que su conectividad y acceso se realice de forma segura.
En este apartado nos adentraremos en sus conceptos, sus objetivos y aquellas técnicas que actualmente se emplean para las redes de comunicaciones.

6.3.1. Conceptos generales

Hoy día todos queremos estar interconectados con todos. Están conectados a las redes (Internet): las personas, los equipos, las aplicaciones, etc.
Gracias a las redes podemos comunicarnos con todos, en cualquier parte del mundo y a cualquier hora.
Pero esto hace también que seamos vulnerables a intrusiones y ataques no deseados por personas (hacker o cracker) o aplicaciones (virus, rootkit).
En base a esto surgió la seguridad informática como conjunto de técnicas o mecanismos que intentan proteger el almacenamiento, procesamiento y transmisión de la información que circula por las redes y en particular por Internet.
Con la seguridad informática conseguimos que nuestras conversaciones telefónicas y nuestros mensajes sean privados y confidenciales, y que por ejemplo nuestros mensajes lleguen al destinatario deseado y no a otros y que además lleguen sin alteración ni manipulación.
También con la seguridad informática evitamos que nuestros equipos y aplicaciones puedan ser controlados o manipulados por terceros sin nuestro consentimiento.

Propiedades de una comunicación segura

En una red constantemente están transmitiéndose datos de un equipo a otro. Es por ello que debemos asegurar que dichas transmisiones sean seguras y de ello se encarga la seguridad informática. Es decir, debemos de proteger la información que se transmita con objeto de que llegue a su destino de forma segura, no sea alterada ni manipulada, ni sea leída por terceros no deseados.
Para conseguir una comunicación segura se emplea como técnica de seguridad en redes el cifrado de las conexiones, es decir, el mensaje no se transmite tal cual se ha generado, sino que se codifica (según una clave) en un mensaje cifrado que es el que se transmite. El receptor (que conoce la clave) es capaz de descifrar este mensaje cifrado para poder visualizar el mensaje original.

Criptografía. Tipos

Como se ha descrito anteriormente para conseguir una comunicación segura, cifrados nuestros mensajes y documentos antes de enviarlos.
De esto se encarga la criptografía que es una técnica o ciencia capaz de crear mensajes ocultos.
La criptografía consiste en aplicar un algoritmo matemático sobre un documento original y legible con objeto de obtener otro documento no legible (cifrado) que es el que se transmite.
Este algoritmo matemático emplea una clave denominada clave del algoritmo, que sólo es conocida por emisor y receptor y que debe aplicarla sobre el algoritmo para cifrar y descifrar el documento.
El algoritmo es un conjunto de reglas ampliamente conocido, pero lo que es privado es la clave del algoritmo que es realmente la fortaleza del sistema.

Los algoritmos criptográficos emplean claves que son necesarias para el cifrado de los mensajes y/o documentos.
Pero estas claves pueden ser descifradas por hackers o crackers con la técnica denominada **ataque de fuerza bruta**, es decir, probar todas las combinaciones de símbolos posibles hasta dar con la clave buscada.
Para evitar el descifrado de la clave del algoritmo y con ello dar fortaleza al sistema de cifrado, se deben tomar ciertas medidas en la elección de la clave del algoritmo. Entre ellas están:

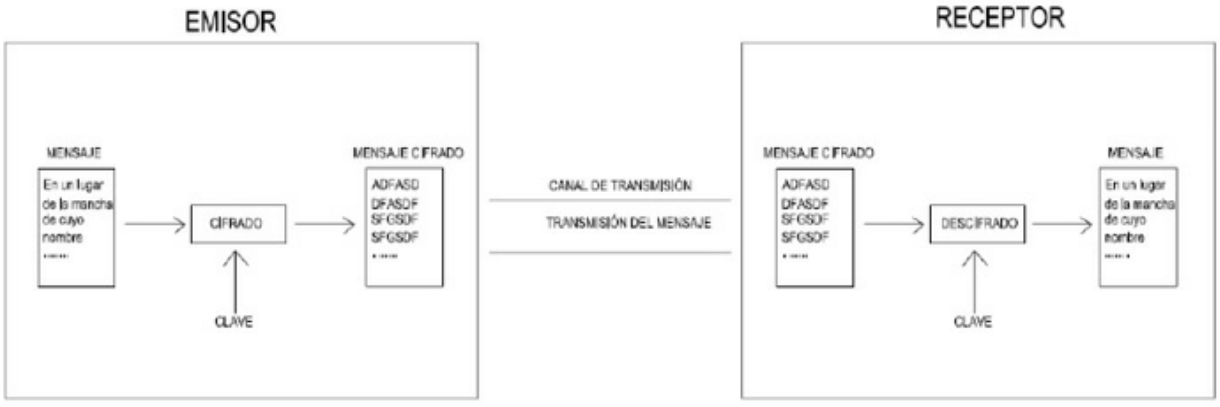
- La clave de cifrado debe ser de gran longitud:
  Por ejemplo emplear claves de 512, 1024 o incluso 20148 bytes de forma que el atacante necesite de muchos recursos hardware y software para conseguirlo. Con ello se genera la desmotivación del atacante.
- Cambiar la clave regularmente:
  Con ello se consigue que en el caso de descifrarlo sólo la tiene disponible un corto espacio de tiempo.
- Emplear todo tipo de símbolos disponibles:
  El uso de caracteres especiales (%, &, #, etc) junto con valores números y alfanuméricos hace más difícil su descifrado.
- No emplear palabras conocidas o identificables:
  Es decir fechas de nacimientos, película favorita, etc., que puede el atacante asociar la clave con la persona atacada.
- Detectar intentos fallidos continuos en un intervalo corto de tiempo.

Los algoritmos criptográficos existentes pueden ser de dos tipos:

- Emplean una criptografía simétrica:
  Es decir, emplean la misma clave para cifrar (para el envío del mensaje o documento) que para descifrar (en la recepción del mensaje o documento).
- Emplean una criptografía asimétrica:
  Es decir, emplean la misma clave para cifrar (para el envío del mensaje o documento) pero emplean otra diferente para descifrar (en la recepción del mensaje o documento).

Veremos a continuación las diferencias existentes entre uno y otro.

- Criptografía simétrica:
  Evidentemente, la clave debe ser conocida sólo por emisor y receptor para que la comunicación sea realmente segura.
  En la criptografía simétrica se emplea la misma clave del algoritmo para cifrar que para descifrar.
  Es el tipo de criptografía más sencillo y que se ha empleado desde la antigüedad.
  En ella el emisor emplea un clave de cifrado antes de enviar el mensaje. El documento cifrado es el que se envía y una vez recibido por el receptor emplea la misma clave para descifrar.
  Evidentemente, la clave debe ser la misma para ambos, para obtener el documento cifrado y luego obtener el documento de descifrado.



La criptografía simétrica presenta varios problemas o inconvenientes:

- La clave del algoritmo debe ser conocida por emisor y receptor y en algún momento debe ser enviada al 'otro' para poder emplear el algoritmo. Evidentemente no podemos usar el mismo canal 'inseguro' para enviar la clave.
- Además debemos tener una clave diferente por cada pareja emisor-receptor, ya que no se puede emplear la misma clave para varios receptores. Por ello, para cada usuario receptor (que puede ser un trabajador de una empresa) debemos disponer de una clave diferente. Esto hace que tengamos que tener almacenada una gran cantidad de claves, una por cada receptor al que queramos enviar el mensaje.

En base a lo anterior en los años 70 surgió la criptografía asimétrica que solucionaba los problemas de la criptografía simétrica y es el método criptográfico más empleado actualmente.

- Criptografía asimétrica:

La criptografía asimétrica soluciona los problemas de la criptografía simétrica, al emplear una clave de cifrado distinto para cifrar y otra para descifrar.

El emisor cuando va a enviar un documento o mensaje emplea una clave (denominada clave pública) con la que cifrar el documento. Esta clave puede ser conocida por cualquiera ya que se emplea para cifrar.

Pero el documento sólo puede ser cifrado por otra clave (clave privada) que sólo lo conoce el receptor al que va dirigido el mensaje o documento que emplea dicha clave privada para descifrar el documento.

No existe relación matemática entre la clave pública o privada, por lo que conociendo la clave pública con que se cifró el mensaje, no se puede descifrar el mensaje que sólo puede descifrarse con la clave privada que sólo lo conoce el receptor al que va dirigido el mensaje.

Con la criptografía asimétrica hemos resuelto los siguientes problemas:

- No es preciso transmitir la clave de cifrado:
  Es una clave que puede ser conocida por cualquiera (por eso se le denomina clave pública) ya que sólo se emplea para cifrar el documento o mensaje.
- No hay problema de almacenamiento de clave:
  Ya que por cada documento que se envía a diferentes usuarios sólo se emplea una clave de cifrado. Sí aumenta la clave privada para el descifrado pero esa clave privada la tiene almacenada cada receptor, porque el emisor sólo guarda la clave de cifrado (clave pública).

No obstante la criptografía asimétrica presenta ciertos problemas o vulnerabilidades que son las siguientes:

- Se debe proteger la clave privada:
  La clave privada empleada por cada receptor debe ser protegida para que nadie pueda emplearla para descifrar el mensaje cifrado recibido.
- La clave privada debe ser transportada:
  La clave privada en algún momento debe ser transportada y para ello se emplean mecanismos como el llavero de claves.
- Son poco eficientes:
  Las claves de cifrado y descifrado suelen ser largas por lo que se tarda tiempo en cifrar y descifrar los documentos; esto las hace ineficientes en este sentido.

Autenticación

En seguridad informática, la autenticación se define como la confirmación que un usuario, equipo o aplicación es quien dice ser y no otro.

Es decir, evitamos la suplantación y al impostor.

Está técnica constituye uno de los pilares básicos en toda comunicación segura. Para conseguir esta autenticación, generalmente en la transmisión de un documento o mensaje se debe loguear el usuario o máquina, es decir, le exigimos que introduzca su usuario y contraseña, con lo cual el sistema confirma que la persona que envía el documento o mensaje es quien dice ser.

Esta técnica de autenticación está plenamente integrada en nuestras vidas cotidianas: nuestro DNI representa la autenticación de que esa persona es quien dice ser; el PIN de nuestro móvil indica al sistema que quien tiene acceso a usar la red móvil es quien dice ser el abonado; el código de nuestra tarjeta de crédito indica que la persona que intenta sacar el dinero del cajero es realmente el titular de la cuenta, etc.

Integridad

En seguridad informática, la integridad se define como la seguridad en la que los datos almacenados son realmente los datos que se espera almacenar, es decir, que no han sido alterados ni manipulados.
Por tanto, cuando se intentan recuperar dichos datos, son los mismos que se almacenaron ya que no han sufrido alteración alguna en su forma o contenido.
Esto es otro de los pilares básicos en la seguridad de los datos.
Esta técnica, al igual que la autenticación, está plenamente integrada en nuestra vida cotidiana.
Por ejemplo, nuestro DNI lo forman ocho números seguidos de una letra. Existe un algoritmo que comprueba que dicha letra corresponde a esa numeración, ya que la letra se obtiene a través de una combinación aritmética de los números. Cuando se introduce un DNI en un sistema informático, lo primero que se hace es comprobar si dicho DNI es válido, y para ello aplica la combinación aritmética a los números. Si la letra que obtiene es la misma que la introducida en el DNI, dicho documento es válido. Con esto se verifica la integridad del DNI introducido y el usuario puede operar con el sistema.

Distribución de claves y certificación

Hemos visto que en los algoritmos criptográficos tanto simétricos como asimétricos necesitan una clave privada que ambos -emisor y receptor- deben compartir y que en algún momento debe ser transportada por un canal seguro.
Para transportar esta clave de cifrado (distribuir la clave) existen mecanismos de transporte de claves, siendo el más habitual la tarjeta inteligente.
Esta tarjeta es un dispositivo generalmente de plástico y provisto de un chip electrónico donde se almacena nuestra clave y que para usarla nos pedirá un PIN de acceso a la clave.
La implementación de esta tarjeta inteligente puede ser de dos tipos:

- Mediante una tarjeta de memoria flash.
- Mediante una tarjeta preprocesadora.

La primera es más insegura, ya que cuando se introduce la tarjeta en el equipo para utilizar la clave, se realiza una copia temporal de dicha clave en el equipo. Aquí es donde está la vulnerabilidad.
En cambio, en la segunda, la clave nunca sale de la tarjeta preprocesadora, ya que el proceso matemático de cifrado y descifrado que emplea la clave la realiza el propio chip de la tarjeta preprocesadora.
Otra clasificación de las tarjetas inteligentes se puede realizar en función del interfaz de comunicación que emplea. Así encontramos:

- Tarjeta de contacto:
  Es aquella en la que debe existir un contacto (generalmente metálico) entre el equipo y la tarjeta inteligente para poder operar. Es el caso más habitual y más seguro.
- Tarjeta sin contacto:
  Es aquella en la que no existe contacto físico entre la tarjeta inteligente y el equipo. Generalmente la transmisión se realiza por radiofrecuencia. Es más inseguro (utiliza un canal como el aire que es inseguro) pero es más rápido, y por ello, se emplea en lugar donde se busca gran rapidez como por ejemplo en estaciones de tren, aeropuertos, etc.

6.3.2. Aplicaciones

Las aplicaciones en red son realmente los puntos críticos en la seguridad de las redes.
Son numerosas las aplicaciones que presentan vulnerabilidades y el hecho de que se emplea en red, hace más fácil que códigos maliciosos puedan propagarse de un equipo a otro de manera muy rápida.
Es por ello que la seguridad informática debe estar centrada en aquellas aplicaciones que más se utilizan en las redes para detectar sus vulnerabilidades y crear parches a dichos programas para asegurar su integridad.
A continuación veremos aquellas aplicaciones y sus protocolos asociados que más se emplean en red, donde se describirá su funcionamiento y cómo la seguridad informática actúa sobre ellos para conseguir unas transmisiones fiables y seguras.

SSL (Secure Sockets Layer)

SSL representa un protocolo que trabaja en el nivel de transporte del modelo OSI o TCP/IP y que proporciona una transmisión segura de la información entre los equipos, generalmente entre un equipo cliente y un servidor.
Trabaja a nivel de transporte, que lo hace transparente de la arquitectura de los elementos de interconexión o encaminadores que trabajan a nivel 3 o nivel de red.
SSL surgió para proteger las conexiones existentes entre clientes y servidores web con el protocolo http que se empleaban para el comercio electrónico. Esta protección debía asegurar al cliente que se había conectado al servidor auténtico, y enviarle en consecuencia datos confidenciales, como por ejemplo los datos de su número de tarjeta de crédito.
El protocolo se encarga de encapsular el trabajo de los elementos de la capa superior, construyendo un canal de comunicaciones entre los dos extremos objeto de la comunicación. Esto lo realiza empleando la técnica de Handshake que es el encargado de intercambiar la clave que se utilizará para crear un canal seguro, mediante un algoritmo eficiente de cifrado simétrico.
SSL representa a un protocolo que trabaja en el nivel de transporte del modelo OSI o TCP/IP y que asegura una transmisión segura de la información entre los equipos generalmente entre un equipo cliente y un servidor.
Que trabaja a nivel de transporte lo hace transparente de la arquitectura de los elementos de interconexión o encaminadores que trabajan a nivel 3 o nivel de red.
SSL surgió para proteger las conexiones existentes entre clientes y servidores web con el protocolo http que se empleaban para el comercio electrónico. Esta protección debía asegurar al cliente que se había conectado al servidor auténtico, y enviarle en consecuencia datos confidenciales, como por ejemplo los datos de su número de tarjeta de crédito.
El protocolo se encarga de encapsular el trabajo de los elementos de la capa superior, construyendo un canal de comunicaciones entre los dos extremos objeto de la comunicación. Esto lo realiza empleando la técnica de Handshake que es el encargado de intercambiar la clave que se utilizará para crear un canal seguro mediante un algoritmo eficiente de cifrado simétrico.

SSH (Secure Shell)

En SSH se define una serie de reglas que permite una transmisión segura de un equipo a otro al cifrar la información que transmite de extremo a extremo.
Es muy empleado para la configuración remota de equipos (sustituyendo al TELNET), para transferencia de archivos (sustituyendo al FTP), crear canales seguros de comunicaciones, etc.
En la actualidad existen dos versiones de este sistema SSH: SSH1 y SSH2 siendo ésta última la más usada al tener mejoras sobre la primera
Una de las aplicaciones más usadas que emplea dicho protocolo es el OpenSSH.

IPsec

IPsec es un protocolo que define una serie de reglas que, trabajando a nivel de red (a diferencia de SSL que trabaja a nivel de transporte), permite una comunicación segura y fiable entre extremos o dicho de otro modo, entre equipos.

Para ello, este protocolo usa técnicas criptográficas además de la autenticación para la transmisión segura de los datos.

Cortafuegos

Un cortafuegos o firewall es una aplicación software especializada que se intercala entre las aplicaciones y la tarjeta de red para realizar un filtrado de los paquetes.
El objetivo no es más que controlar los paquetes que entran y salen del equipo por la red, con objeto de actuar correctamente ante paquetes sospechosos.
Es una herramienta básica para la seguridad de las redes, todos los equipos siempre deberían tenerlo instalado y activado.
El firewall se puede instalar tanto en equipos clientes como en equipos servidores actuando de forma diferentes aunque empleando las mismas técnicas.
Veremos a continuación cómo trabaja según sea un equipo cliente o un equipo servidor.
–Cortafuegos en un equipo cliente:
En un equipo cliente, el cortafuegos actúa aplicando un filtrado de paquetes.
En el tráfico saliente, es decir, de paquetes que salen del equipo hacia la red el cortafuegos o firewall analiza la cabecera de cada paquete y en función de las reglas que tenga definidas en el cortafuegos realiza una acción u otra. Por ejemplo, si detecta que la máquina cliente hace spam, bloquea el puerto 25 (puerto de correo electrónico).
En el tráfico entrante, es decir, de paquetes que entran al equipo cliente, analiza la cabecera de cada paquete y en función de las reglas de configuración actúa de una forma u otra.

–Cortafuegos en un equipo servidor:
En un equipo servidor, el cortafuegos también actúa aplicando un filtrado de paquetes.
En el tráfico saliente, es decir, de paquetes que salen del equipo hacia la red el cortafuegos o firewall, analiza la cabecera de cada paquete, y en función de las reglas que tenga definidas en el cortafuegos realiza una acción u otra. En este tráfico es donde generalmente actúa el cortafuegos, puesto que en un servidor la mayor parte del tráfico es saliente.
En el tráfico entrante, en cambio, el firewall analiza qué paquetes quieren acceder a qué puertos del servidor, para bloquear en el caso de un ataque al servidor, si así lo tiene en las reglas de configuración.

6.4. Protocolos del nivel de aplicación

Ya hemos visto anteriormente que según el modelo OSI las aplicaciones se rigen en la capa 7 o capa de aplicaciones.
Las aplicaciones pueden ser diseñadas de diferentes maneras en función del objetivo que se persigue.
Así encontramos aplicaciones P2P (Peer to Peer, son un sistema totalmente gratuito para compartir archivos a través de Internet) o aplicaciones cliente-servidor.
Estas aplicaciones cliente-servidor son las más usadas en aplicaciones en red y es por ello que las vamos a ver a continuación con más detalle.
No obstante, la evolución de la tecnología está mostrando una tendencia a aplicaciones con un arquitectura más distribuida como las aplicaciones P2P.

6.4.1. La arquitectura cliente-servidor

En Internet hay una serie de servicios disponibles para todos aquellos usuarios, empresas, organizaciones o incluso máquinas que quieran hacer uso de él.
Para hacer uso de estos servicios, es necesario que se ejecuten dos programas de aplicación en dos equipos u ordenadores diferentes: una programa cliente en una máquina (el solicitante) y un programa servidor en otra máquina (el que proporciona el servicio).
El esquema anteriormente descrito es lo que se denomina arquitectura cliente-servidor que debe asimismo cumplir una serie de requisitos:
–El programa cliente se ejecuta en una máquina o equipo local y solicita un servicio del servidor. Es una aplicación finita ya que arranca cuando lo solicita el usuario y termina cuanto éste lo termina o cuando se ha completado el servicio.
–El programa servidor se ejecuta en una máquina remota y ofrece un servicio a muchos clientes. Cuando arranca, abre un puerto para atender a las solicitudes de los clientes pero no termina nunca (siempre está disponible) a no ser que se le solicite expresamente. Es por tanto un programa infinito.

6.4.2. Aplicaciones cliente-servidor

En una arquitectura cliente-servidor siempre se produce la misma secuencia de acciones:
–Un programa cliente solicita un servicio a un servidor que se encuentra en una máquina remota.
–Un programa servidor se está ejecutando en una máquina remota esperando la petición de uno o varios clientes. Para ello tiene habilitado o abierto uno o varios puertos para ofrecer el servicio.
–El programa servidor atiende a las peticiones de los programas clientes y cuando finaliza lo indica al programa cliente que da por finalizada la petición.
Los servicios utilizados muy frecuentemente por muchos usuarios tienen programas de aplicación cliente-servidor específicos.
A continuación veremos diferentes aplicaciones cliente-servidor que son utilizadas en Internet como son el http, Ftp, Telnet, Smtp, entre otros.
HTTP (Hypertext Transfer Protocol)
Es una aplicación cliente-servidor en la cual el cliente solicita consultar datos de la World Wide Web.
La World Wide Web no es más que un repositorio de información diseminada por todas las redes y entrelazada entre sí (Internet).
En esta aplicación lo que se transfiere son datos en forma de texto, sonidos, vídeos, etc., en un formato denominado hipertexto que no es más que un formato que permite integrar los diferentes recursos multimedia.
La información es solicitadas por una aplicación cliente usando un cliente http (un navegador) capaz de interpretar el hipertexto y mostrarlo al usuario. El servidor http es quien atiende esta petición del cliente enviando el mensaje de hipertexto.

Tipos de mensajes http:

Existen dos tipos generales de mensajes http:
–Mensaje de petición:
Lo solicita la aplicación cliente y consta de una línea de petición, cabeceras y en algunos casos de un cuerpo.

–Mensaje de respuesta:
Es el mensaje que aporta la aplicación servidor y que contiene una línea de estado, varias cabeceras y en algunos casos de un cuerpo.

Localizador uniforme de recursos (URL):

La información localizada en la World Wide Web requiere de una dirección.
Para acceder a esa información, la aplicación cliente debe enviar en el mensaje de petición la dirección de la información que solicita.
Esta dirección sigue un formato denominado URL (Uniform Resource Location) que contiene cuatro campos:
–Método: define el protocolo empleado para acceder al documento o información. Puede ser http, ftp, etc.
–Estación: es la dirección IP del equipo u ordenador que aloja la información solicitada. Habitualmente se emplea los servicios DNS en la cual esta dirección es sustituida por un alias que comienza por www.
Ejemplo: www.google.es.
–Puerto: es un campo opcional y que indica el número del puerto del servidor por el cual se va suministrar la información. Deberá estar habilitado (abierto) por la aplicación servidor.
–Camino: es la ruta del archivo donde se encuentra la información.

Navegadores:

Los navegadores son aplicaciones clientes que interpretan el mensaje de hipertexto que se solicita al servidor http y lo muestra al usuario.
Todos los navegadores contienen al menos dos partes:
–Controlador: es la línea de comandos donde se escribe la dirección URL de la información a solicitar.
–Intérprete: es la 'página' donde se muestra la información de hipetexto solicitada y traducida para que pueda ser visualizada correctamente por el usuario.
Actualmente existen en el mercado numerosos navegadores siendo los más conocidos Google Chrome, Edge, Mozilla, Ópera, etc.

FTP (File Transfer Protocol)

La aplicación cliente-servidor FTP es aquella que permite la transferencia de archivos y ficheros de una máquina u ordenador a otro.
Es un estándar muy empleado en TCP/IP para copiar un archivo de una estación a otra.
Como en toda arquitectura cliente-servidor, una máquina cliente ejecuta una aplicación cliente en la cual solicita un archivo a otra máquina o transfiere un archivo local a otra máquina. Por el otro lado, existirá una máquina servidor en la cual se ejecuta una aplicación servidor que recibe las peticiones de los equipos clientes atendiendo a la transferencia de archivos solicitada.
En una aplicación FTP siempre se establecen dos conexiones entre las dos máquinas:
–Una conexión para la transferencia de órdenes y comandos.
–Una conexión para la transferencia de la información, archivos o ficheros en sí.

Conexión para la transferencia de órdenes y comandos:

En ella se transfieren comandos simples siendo los más habituales los siguientes:
–PUT <nombre_archivo_local> <nombre_archivo_remoto>
Este comando indica que se transfiera el archivo local denominado "nombre_archivo_local" a la máquina remota con el nombre "nombre_archivo_remoto>.
Si no se indica el "nombre_archivo_remoto" (que es un parámetro opcional) se transferirá con el mismo nombre.
–GET <nombre_archivo_remoto> <nombre_archivo_local>
Este comando indica que se transfiera el archivo remoto denominado "nombre_archivo_remoto" a la máquina local con el nombre "nombre_archivo_remoto>.
Si no se indica el "nombre_archivo_local" (que es un parámetro opcional) se transferirá con el mismo nombre.
–MKDIR /ruta/nombre_carpeta
Este comando crea una carpeta con el nombre "nombre_carpeta" en la ruta indicada en la máquina remota.

–RMDIR /ruta/nombre_carpeta
Este comando elimina la carpeta con el nombre “nombre_carpeta” en la ruta indicada en la máquina remota.
–CD /ruta/nombre_carpeta
Este comando cambia el directorio actual de trabajo (en la máquina remota) a la indicada por /ruta/nombre_carpeta.
–DELETE <nombre_archivo>
Este comando elimina el archivo indicado “nombre_archivo” de la máquina remota.
–LS
Este comando realiza un listado de carpeta y archivo alojados en la máquina remota de la carpeta actual de trabajo. En algunas aplicaciones cliente-servidor, este comando se sustituye por DIR.
–RENAME <nombre_actual> <nombre_nuevo>
Este comando cambia el nombre (renombra) el fichero con nombre “nombre_actual” por el nombre “nombre_nuevo”.
–PWD
Este comando indica la ruta actual de trabajo.
–OPEN
Este comando inicia una sesión de trabajo de FTP en la máquina remota. Será necesario introducir nuestras credenciales (nombre de usuario y contraseña) y estar autorizado en el servidor para poder realizar las operaciones.
–CLOSE
Este comando cierra la conexión de FTP con la máquina remota.

Conexión para la transferencia de datos:

Esta es la conexión que se establece para la propia transferencia de los archivos y ficheros.
Emplea amplia variedad de tipos de datos transferidos y junto con la conexión para la transferencia de órdenes y comandos permite que el protocolo de FTP sea eficiente.
La conexión para la transferencia de datos sólo aparece abierta durante el tiempo de la propia transferencia de archivos y ficheros, abriéndose o cerrándose por cada transferencia.
En cambio la conexión para la transferencia de órdenes y comandos permanece siempre abierta durante toda la sesión ftp interactiva. Sólo se cierra a petición expresa de la aplicación cliente o por el propio servidor.

TFTP (Trivial File Transfer Protocol)

Existe una variante del FTP denominada TFTP (Trivial File Transfer Protocol) que representa un protocolo simplificado del FTP convencional.
Se aplica cuando se pretende enviar o copiar archivos de la máquina local a la remota o viceversa y es por ello que la lista de comandos queda simplificados a los comandos más básicos (GET, PUT) quedando excluidos muchos de los comandos más complejos que incluye el FTP convencional.
Este protocolo utiliza el puerto 69 a diferencia del puerto 20 y 21 del FTP.
Tampoco incluye mecanismos de cifrado y autentificación.
Sí soporta (al igual que el FTP) que la transferencia de ficheros se realice de forma binaria o en formato ASCIII.

SMTP (Simple Mail Transfer Protocol)

Es un protocolo que permite enviar mensajes de un usuario en una máquina a otros usuarios de otras máquinas o equipos.
Es en definitiva la implementación de un correo electrónico para equipos conectados en red.
Con este protocolo se pueden realizar las siguientes acciones:
–Envío de un único mensaje de un usuario a otro usuario conectado en red.
–Envío de varios mensajes de un usuario a uno o varios usuarios conectados a la red.
–Envío de mensajes que incluyen textos, imágenes y vídeos a uno o varios usuarios en red.

Para la implementación de este protocolo es preciso que el sistema incluya al menos los siguientes elementos:
–Agente de usuario (UA).
–Formato de direcciones.
–Gestor o Servidor de correo.
A continuación veremos con más detalles cada uno de estos componentes.

Agente de usuario (UA):

Es un programa o aplicación para recibir o enviar correos.
Estas aplicaciones suelen incluir una interfaz amigable para el usuario además de numerosas funcionalidades para enriquecer el mensaje a enviar. Es por ello que incluyen funciones para agregar imágenes, vídeos, texto enriquecido, etc.
Entre las aplicaciones UA más utilizadas y conocidas se encuentra: Outlook, Outlook express, Mozilla Thunderbird, Eudora Mail, etc.

Formato de direcciones:

Para la implementación de un SMTP, el sistema gestor debe utilizar un formato de correo que es único para el sistema.
Este formato consta de dos partes separados por el signo @:
–Una parte local: que define el buzón del correo del usuario y que es donde se almacenan todos los correos entrantes y salientes de ese usuario.
–Una parte de dominio: que representa la base de datos según el DNS o el nombre lógico de la organización o empresa de esos buzones de correo.
Por ejemplo, una dirección de correo sería: jperez@gmail.com donde jperez representa la parte local, es decir, es el buzón de correo del usuario Juan perez y gmail.com representa el servidor u organización donde se aloja dicho buzón de correo con todos los mensajes que incluye.

Gestor o servidor de correo:

También denominado MTA se trata de una máquina con un programa servidor capaz de recibir las órdenes de los UA para enviar y recibir los correos que éste último solicita.
En la arquitectura del SMTP se habla de dos tipos de servidores de correo:
–MTA (Mail Transport Agent): es el servidor de correo el cual recibe los correos enviados por el UA y los enruta a través de otros MTA para hacerlo llegar a su destino.
–MDA (Mail Delivery Agent): es el servidor de correo donde se almacena los correos a la espera que su receptor los acepte.
El esquema anterior permite que no sea necesario que los destinatarios estén conectados para poder enviarles un correo electrónico.
Como se ha descrito anteriormente, no es necesario que emisor y receptor estén 'en línea' para enviar un correo.
El correo enviado se almacenará en un servidor MDA a la espera de que el recepto se conecte y lo reciba.
Para esta recepción existen dos protocolos ampliamente utilizados:
–Protocolo POP3 (Post Office Protocol):
Es el más antiguo y permite recuperar el correo electrónico del MDA. Permite funcionalidades añadidas como 'Dejar copia en el servidor'.
–IMAP (Internet Message Access Protocol):
Este protocolo permite la recepción de los correos desde varios agentes UA manteniendo la sincronización entre todos (leído, eliminado, movido). Con IMAP, se guarda una copia de cada mensaje en el servidor, de manera que esta tarea de sincronización se realiza desde el MDA.
En cualquier de los casos se requiere que el usuario deba identificarse en el sistema (usuario y contraseña) para leer y enviar los mensajes.
TELNET (Telecommunication NETwork)

Es una aplicación cliente-servidor que permite a un usuario desde una máquina local conectarse a otra máquina de forma remota.
Para ello, el usuario debe identificarse en la máquina remota y disponer de los privilegios necesarios para su conexión.
El protocolo TELNET establece para ello una conexión virtual en la red, de forma que el usuario visualiza en su pantalla la ejecución de aplicaciones y comandos como si estuviera en la máquina remota.
El puerto que utiliza este protocolo generalmente es el puerto 23.
Este protocolo define una serie de comandos para la gestión de la máquina remota desde un terminal.
A continuación veremos los comandos más comunmente utilizados.

Comandos TELNET:

Todos los comandos se deben ejecutar en modo consola o línea de comandos para su ejecución.
–Telnet <dirección IP máquina remota> <puerto>
Este comando permite iniciar una sesión telnet donde se debe especificar la IP de la máquina remota a la queremos conectarnos y el puerto a utilizar (si no se especifica nada será el puerto 23).
–Close
Permite cerrar de forma ordenada una sesión telnet abierta.
–Open
Abre otra conexión telnet además de la actual.
–Quit
Cierra la conexión telnet previamente abierta.
–Set
Cambia la configuración de la conexión telnet.

SNMP (Simple Network Management Protocol)

Es una aplicación cliente-servidor que permite gestionar los dispositivos que están conectados en red y que emplean el protocolo TCP/IP con objeto de monitorizar el estado de la red y el mantenimiento de la misma.
Es por tanto un protocolo de gestión de redes.
En este protocolo se distingue dos conceptos:
–Gestor:
Es un dispositivo y/o aplicación que controla y monitoriza un conjunto de agentes.
–Agentes:
Son dispositivos conectados a la red que realizan determinadas funciones. Generalmente son los elementos de interconexión como router, gateways, switches, etc.
Veremos a continuación con más detalle cada uno de estos elementos.

Gestor:

Un gestor es una máquina que ejecuta un cliente SNMP que se encarga de controlar y monitorizar clientes de la red.
Para ello, periódicamente solicita información del estado de cada uno de los agentes para analizar el estado de la red y notificando las incidencias producidas.
El gestor también puede actuar sobre los agentes enviando órdenes y comandos a los agentes para que realicen determinadas tareas para el correcto mantenimiento de la red.
En ocasiones puede incluir el provocar el reinicio de los valores de un agente si así fuese necesario.

Agente:

Un agente es un dispositivo o máquina de la red que realiza determinadas funciones de red como por ejemplo encaminar los mensajes, tramas o paquetes.
Por tanto, los agentes suelen ser elementos de interconexión como router y gateways mayoritariamente.
Un agente (o encaminador) puede almacenar variables como número de paquetes recibidos y enviados y así trasladarlo al gestor.

Los agentes también pueden contribuir en el proceso de gestión. El agente puede comprobar el entorno de la red donde realiza sus funciones y advertir al gestor de posibles problemas para que éste último adopte las medidas preventivas y/o correctoras necesarias.
Existen otros protocolos que cooperan con el SNMP para la gestión de la red.
Estos protocolos son los siguientes:
–SMI:
Es un protocolo cuya función es nombrar los objetos de la red, definir el tipo de datos que es capaz de almacenar y cómo mostrarlo y transmitirlo por la red.
–MIB:
Es un protocolo que define la colección o estructura jerárquica de objetos que de un agente y que puede manejar un gestor.
El protocolo SNMP define una serie de mensajes para el intercambio de información entre gestor y agentes con objeto de cumplir con las funcionalidades de gestión de la red.
Entre todos los mensajes que se describe en el protocolo describimos los más importantes:
–GetRequest:
Es un mensaje petición enviada desde el gestor a un agente para solicitarle el valor de una variable.
–GetResponse:
Es un mensaje de respuesta enviada desde un agente a un gestor (tras un GetRequest) donde se adjunta el valor de la variable solicitada.
–SetRequest:
Es el mensaje enviado desde un gestor a un agente para almacenar un valor en una variable del agente.
–Trap:
Es un mensaje enviado desde un agente a un gestor para informarle de un evento.

Otros

Hay numerosas aplicaciones cliente-servidor, aunque ya se han descrito anteriormente las más usadas y habituales.
No obstante, destacamos a continuación algunas otras aplicaciones cliente-servidor también ampliamente usadas actualmente.
Destacamos las siguientes:
–Protocolo de arranque (BOOTP).
–Protocolo de configuración dinámica de estaciones (DHCP).
–Protocolo DNS.
A continuación, describiremos con más detalle el funcionamiento de cada uno de estos protocolos, ya que todos siguen la misma arquitectura cliente-servidor.

Protocolo de arranque (BOOTP):

Se trata de un protocolo, algo obsoleto ya, que permite la conectividad de una máquina o equipo a una red de una forma automática.
Es decir, para que una máquina se conecte a una red necesita tener configurados los siguientes parámetros:
–Su dirección IP.
–La máscara de red.
–La dirección IP del router o encaminador.
–La dirección IP de un servidor DNS (no estrictamente necesario si no va a ser utilizado para navegación aunque altamente recomendable).
Sin estos parámetros, la máquina o equipo no puede conectarse a la red porque son los parámetros necesarios para identificarse en la red que se quiere conectar.
El protocolo BOOTP es una aplicación cliente-servidor que proporciona esta información a aquella máquina que se conecta a la red.
Es decir, en la red se está ejecutando un servidor con una aplicación BOOTP, el cual recibe peticiones de equipos que quieran conectarse a la red. El servidor responde a esta petición enviando al equipo los parámetros de red anteriormente descritos y que son necesarios para su conectividad.

Una vez recibidos estos parámetros, el equipo solicitante queda configurado (estas variables las almacena en un archivo de configuración) y puede operar en la red normalmente.

Protocolo de configuración dinámica de estaciones (DHCP):

El protocolo BOOTP anteriormente descrito presenta varias problemas:
–La asignación de los parámetros de red a un equipo se realiza de forma estática, es decir, el servidor BOOTP tiene una tabla de direcciones donde a cada dirección física de un equipo (su MAC) le asigna siempre la misma dirección o parámetros de red.
–Si a la red se quieren añadir nuevos equipos que no vienen en la lista de direcciones del servidor, el servidor no podrá configurar sus parámetros de red, a no ser que tengamos que actualizar esta lista en el servidor (tarea poco operativa cuando se manejan redes con múltiples equipos).
–Además si un equipo se da de baja definitivamente, la dirección IP asociada a esa MAC no podrá ser utilizada para otros equipos. Esto provoca baja eficiencia del protocolo BOOTP.
Los problemas anteriores son solucionados con el protocolo DHCP que como su propio nombre indica (Dinamic Host Configuration Protocol) asigna dinámicamente (y no estáticamente) direcciones IP a aquellas máquinas o equipos que se lo soliciten para su conectividad a la red.
Con este protocolo DHCP se solucionan los problemas del protocolo BOOTP porque:
–La asignación de los parámetros de red a un equipo se realiza de forma dinámica, es decir, cuando una máquina o equipo solicita parámetros de red, el servidor DHCP le asigna una dirección disponible sin tener que estar asociado a su MAC.
–Por ello, cualquier equipo puede ser conectado a la red (siempre que haya IP disponibles) y no es necesario actualizar ninguna lista de configuración de IP en el servidor DHCP.
–La asignación de los parámetros de red a un equipo o máquina se realiza de forma temporal, es decir, mientras el equipo o máquina está conectado tendrá esa IP y esos parámetros de red, pero cuando se desconecta liberará esa IP para que el servidor DHCP lo tenga disponible para otra máquina o equipo que se lo solicite.

Protocolo DNS (Domain Name System):

Este protocolo emplea una arquitectura cliente-servidor para resolver o etiquetar direcciones IP en nombres alfanuméricos fácilmente de recordar.
Es decir, según lo descrito anteriormente, todas las máquinas, equipos y recursos en la red están identificados por una dirección IP que no es más que un conjunto de cuatro octetos separados por puntos (por ejemplo 92.01.10.128).
Cuando queramos solicitar un recurso de la red (por ejemplo una página web que está alojado en una máquina) debemos proporcionar la dirección IP de la máquina que contiene el recurso.
Memorizar direcciones IP es poco operativo y difícil de manejar y por ello surgió el protocolo DNS.
Este protocolo lo que realiza es asociar direcciones IP a nombre o etiquetas alfanuméricas fácilmente recordables. Por ejemplo, el servidor de Google está en la dirección IP pública 66.249.66.16 pero cuando queremos dirigirnos a ese recurso en vez de poner en el navegador 66.249.66.16 pondremos www.google.es (que es más fácil de recordar).
Esta petición de solicitud desde el navegador llega a un servidor DNS que traduce la etiqueta www.google.es en la dirección IP real 66.249.66.16 que es donde se aloja el recurso solicitado. Así este recurso es respondido y proporcionado a la máquina o usuario que lo ha solicitado.
Este protocolo emplea una arquitectura cliente-servidor para resolver o etiquetar direcciones IP en nombres alfanuméricos fácilmente de recordar.
Es decir, según lo descrito anteriormente, todas las máquinas, equipos y recursos en la red están identificados por una dirección IP que no es más que un conjunto de cuatro octetos separados por puntos (por ejemplo 92.01.10.128).
Cuando queramos solicitar un recurso de la red (por ejemplo una página web que está alojado en una máquina) debemos proporcionar la dirección IP de la máquina que contiene el recurso.
Memorizar direcciones IP es poco operativa y difícil de manejar y por ello surgió el protocolo DNS.

Este protocolo lo que realiza es asociar direcciones IP a nombre o etiquetas alfanuméricas fácilmente recordables. Por ejemplo, el servidor de google está en la dirección IP pública 66.249.66.16 pero cuando queremos dirigirnos a ese recurso en vez de poner en el navegador 66.249.66.16 pondremos www.google.es (que es más fácil de recordar).
Esta petición de solicitud desde el navegador llega a un servidor DNS que traduce la etiqueta www.google.es en la dirección IP real 66.249.66.16 que es donde se aloja el recurso solicitado. Así este recurso es respondido y proporcionado a la máquina o usuario que lo ha solicitado.
El protocolo DNS es un protocolo que puede ser utilizado en diversas plataformas.
El espacio de dominios se divide en tres secciones diferentes:
–Dominios genéricos.
–Dominios de país.
–Dominios inversos.
Se entiende por dominio la identificación o etiqueta se da a un equipo dentro de una red.
Un dominio puede estar formado por uno o varios equipos de red.
En el dominio genérico se definen etiquetas que describen el tipo de organización donde se alojan los equipos o máquinas.
Entre ellos encontramos los siguientes:

Etiqueta	Descripción
.com	organización comercial
.edu	organización educativa
.org	organización sin ánimo de luco
.int	organización internacional
.mil	organización militar
.net	organización de red

En el dominio genérico se definen etiquetas que describen al país donde se alojan los equipos o máquinas que contienen los recursos.
Así existirán los dominios .es (España), .it (Italia), .us (EEUU), .fr (Francia), etc.
En el dominio inverso lo que se pretende es que el solicitante proporciona la dirección IP para que el servidor DNS compruebe que dicha dirección IP corresponde a una etiqueta ya asignada. Se emplea generalmente para fines estadísticos y uno de los más conocidos es el dominio in-add.arpa.
Este tipo de dominio inversos se emplea además para la comprobación de identidad del cliente.
–La capa de red o capa de 3 del modelo OSI es aquella que se encarga del enrutamiento de los paquetes de información desde el nodo origen al nodo destino a través de la red.
–La capa de transporte o capa 4 del modelo OSI es aquella que se encarga de la transmisión fiable y libre de errores de los paquetes extremo a extremo, es decir, del nodo origen al nodo destino.
–Esta capa de transporte permite dos implementaciones de protocolo: TCP (fiable pero más lento) y UDP (no fiable pero más rápido).
–La seguridad informática es un concepto cada vez más implementado y a tratar en el diseño de cualquier red.

–Numerosos programas maliciosos, virus, suplantación de usuarios, etc., son nuevos ataques que se producen a las redes y sobre los que la seguridad informática debe actuar con mecanismos eficientes.
–Las aplicaciones de red más empleadas actualmente son las que se implementan en los protocolos HTTP (navegación web), FTP (transferencia de archivos), TELNET (acceso remoto a equipos) y SMTP (correo electrónico) entre otros.

7. Equipos de interconexión de red

7.1. Dispositivos de interconexión de redes

Cuando se quieren interconectar varios dispositivos u ordenadores formando una red es necesario emplear dispositivos de interconexión.

Los dispositivos de interconexión de redes por tanto no son más que elementos de una red que permiten conectar equipos, dispositivos u ordenadores.

Pero estos equipos no sólo interconectan equipos sino que pueden realizar otras funciones como:

- Gestión del tráfico.
- Enrutamiento.
- Actuar de cortafuegos.
- Traducción de protocolos.
- Detección y control de errores.
- Etc.

Estos dispositivos no sólo sirven para interconectar equipos sino redes entre sí formando redes de mayor ámbito como puede ser Internet.

7.1.1. Funciones y modelo de referencia OSI

Los dispositivos de interconexión puede ser de muchos tipos dependiendo del nivel del modelo OSI o modelo TCP/IP en el que trabaja.

Así encontramos los siguientes dispositivos de interconexión:

- Repetidores o Hub.
- Puentes o Switch.
- Encaminadores o Router.
- Pasarelas o Gateways.

Cada uno de ellos trabaja en un nivel del modelo de OSI o modelo TCP/IP anteriormente descrito teniendo por tanto unas funciones concretas.

La relación de cada dispositivo con el nivel en el que opera es la siguiente:

Dispositivo	Nivel del Modelo OSI	Nivel del Modelo TCP/IP
Repetidor o Hub	Nivel físico	Nivel de enlace de datos
Puente o switch	Nivel de control de enlace	Nivel de enlace de datos
Encaminador o Router	Nivel de red	Nivel de red
Pasarela o Gateway	Nivel de transporte	Nivel de aplicación

Veremos a continuación el funcionamiento de cada uno de ellos con más detalle.

7.1.2. Prestaciones y características

Repetidores o Hub:

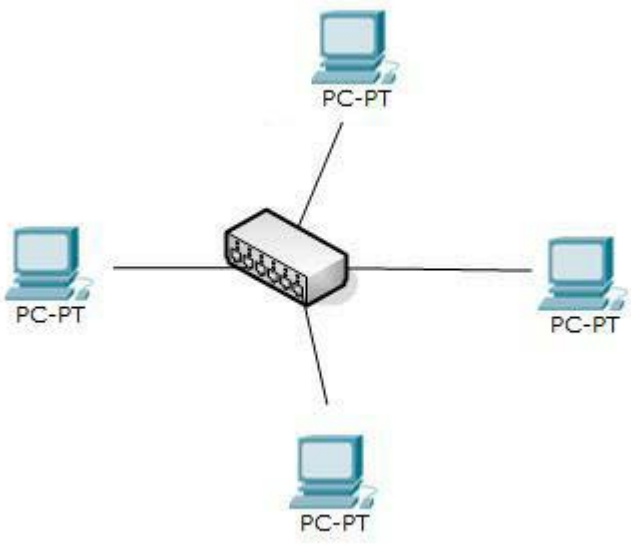
Se trata de un dispositivo de interconexión de redes que trabaja a nivel físico o nivel 1 del modelo OSI.

Su funcionamiento se basa en recibir señales y transmitirlas por sus puertos de salida.

Se denomina repetidor, ya que lo que hace es regenerar la señal que pueden venir débiles, y replicarlas a su salida para alcanzar con ello mayores distancias en los enlaces.

No realiza ningún tipo de enrutamiento, ni control de errores, etc., ya que toda la información que le llega, lo único que hace es replicarla a todos sus puertos de salida, y será el equipo a niveles superiores el que

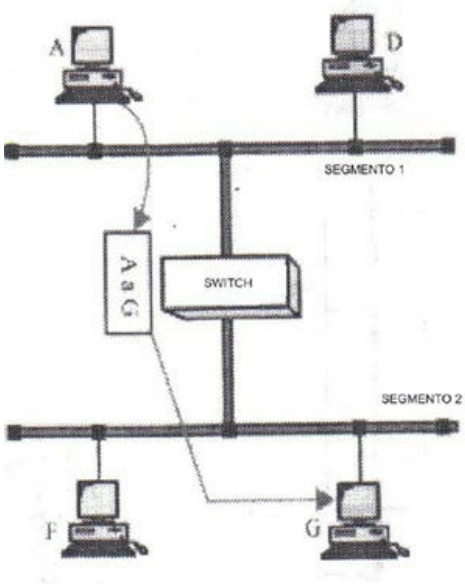
decida si dicho paquete era para él y por tanto se lo queda, o por el contrario lo descarta porque no iba dirigido a él.
En base a lo anterior, se trata de un dispositivo bastante ineficiente, ya que toda la información que le llega lo replica a todos los puertos.
En la siguiente imagen podemos ver cómo se intercala un repetidor o hub en una red.



Con un repetidor o hub podemos interconectar diferentes equipos, dispositivo u ordenadores o incluso redes.
El problema en el caso de interconectar redes es que puede saturar la red, ya que al replicar toda la información que le llega puede congestionar el tráfico de la red.
Se emplea por tanto para redes pequeñas pero cuando hay un cierto número elevado de equipos es recomendable emplear otro dispositivo de interconexión que trabaja a niveles superiores.

Puente o Switch:

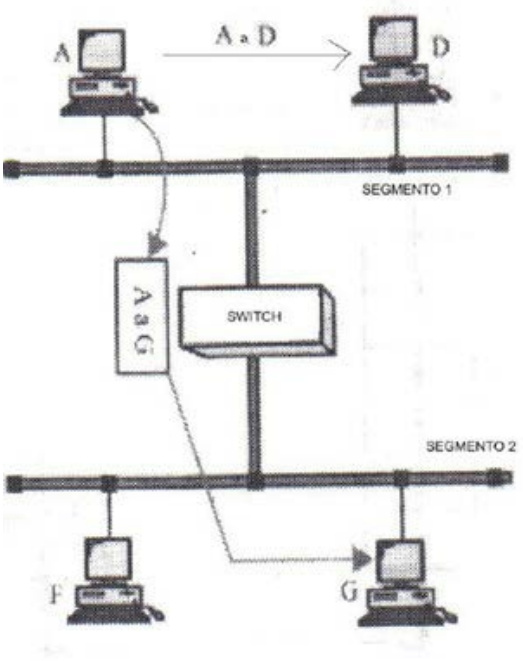
Se trata de un dispositivo de interconexión de redes que trabaja a nivel de enlace o nivel 2 del modelo OSI. Su funcionamiento se basa en la gestión del tráfico a nivel de tramas (nivel de enlace), es decir, es capaz de analizar la dirección física de origen y destino de cada trama y dirigirla al puerto o destino al que va dirigido la trama.
Es por ello que realiza una gestión eficiente del tráfico, ya que las tramas son dirigidas hacia su destino, y no replicadas por todos los puertos como en el caso de los repetidores o hub.
Los puentes o switch se emplean para separar grandes redes en redes más pequeñas (segmentar), ya que con ello se descongestiona la red al controlar el tráfico de la red y sacar fuera de la red aquellas tramas que pertenezcan a otra red.
Es por ello que se emplea como aislador de redes que pueden presentar problemas de congestión de tráfico.
En la siguiente imagen podemos ver cómo se intercala un puente o switch en una red.
Un puente o switch incorpora en sí las mismas funciones que las de nivel físico (como regeneración de señal) al que le añade las funcionalidades del nivel de enlace.
Se trata de un dispositivo más eficiente al no congestionar la red y realizar direccionamiento de tramas hacia su destino.



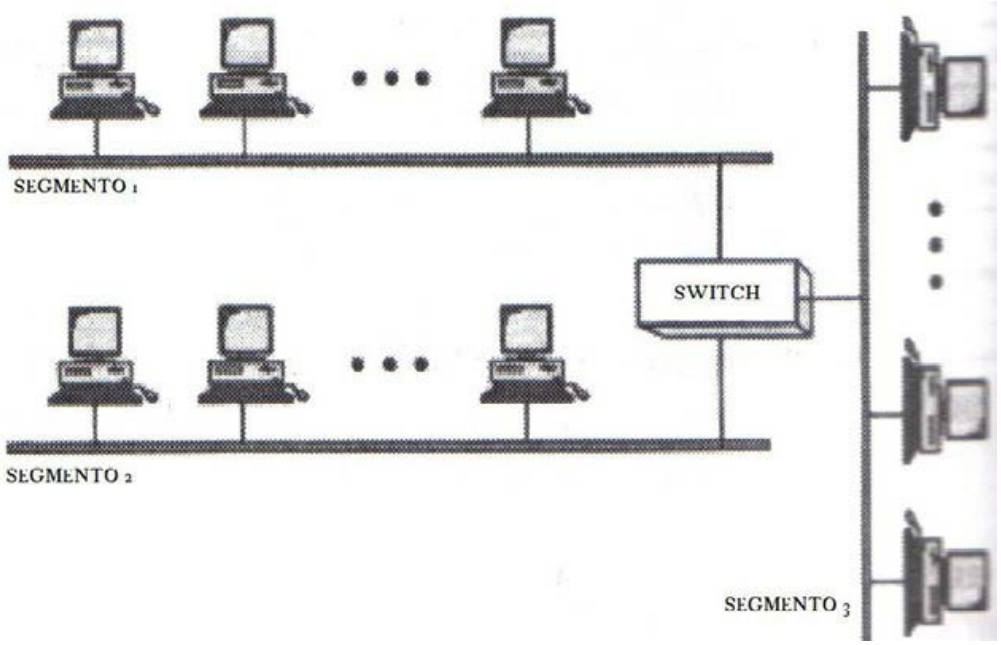
Los puentes o switch disponen de una tabla donde almacenan las direcciones físicas de los equipos que están conectados a ellas para poder realizar el direccionamiento de forma adecuada.
En base a cómo se gestionan esta tabla de direcciones existen varios tipos de puentes o switch:

- Puente o Switch simple.
- Puente o Switch Multipuerto.
- Puente o Switch Transparente.

Puente o Switch simple:
Se trata del puente o switch más básico y simple. Contiene una tabla con las direcciones físicas de todos los equipos conectados a él para realizar de forma correcta el direccionamiento de tramas. Sólo es para interconectar dos segmentos de redes.
Veamos en la siguiente figura su esquema de funcionamiento:
Dicha tabla de direcciones se realiza de forma manual, es decir, cada alta o baja de direcciones físicas se debe hacer por el administrador del sistema.



Puente o Switch multipuerto:
Se trata del puente o switch más avanzado que el anterior ya que permite interconectar varios segmentos de redes.
Contiene una tabla por cada segmento que interconecta y con ello realiza el direccionamiento de las tramas que pasan por el puente o switch.
Veamos en la siguiente figura su esquema de funcionamiento:



La administración de la tabla sigue siendo manual, es decir, la inclusión o exclusión de direcciones físicas de segmentos y equipos, las debe realizar el administrador del sistema.

Puente o Switch transparente:

Se trata del puente o switch avanzado que permite la gestión de la tabla de direcciones de forma automática (no manual) mediante la técnica del aprendizaje.

Al principio tiene una tabla vacía, y a medida que le llegan tramas anota su dirección IP origen y lo asocia con el puerto por el que le ha llegado. De esta forma, va 'aprendiendo' a identificar la dirección IP con el puerto por donde direccionarlo.

Si durante la creación de la tabla, le llega una trama con una dirección destino el cual aún no tiene identificado el puerto por el que lo tiene que enviar, lo envía por todos los puertos posibles no identificados.

Se trata de una sistema de aprendizaje que evita las altas y bajas de direcciones por parte del administrador.

Este tipo de puente o switch es el más empleado, ya que son mucho más eficientes para las actuales redes modernas que se instalan y configuran.

Esta técnica de aprendizaje permite la actualización de las direcciones, es decir, si un equipo se desconecta de un puerto o segmento y se conecta a otro puerto o segmento, el sistema es capaz de reactualizar de nuevo la tabla de direcciones para poder realizar de forma correcta el direccionamiento de tramas.

Por último, aunque este tipo de puentes o switch son más caros que los anteriores, hoy en día, por cuestión de escala, su precio es ya competitivo con los anteriores.

La mayoría de los switches comerciales están catalogados como de este tipo.

Encaminador o Router:

Se trata de un dispositivo de interconexión de redes que trabaja a nivel de red o nivel 3 del modelo OSI.

A diferencia del puente o switch, este dispositivo es capaz de direccionar los paquetes a su destino de la forma más eficiente posible, es decir, es capaz de elegir la ruta mejor lo más rápido posible para que el paquete llegue a su destino.

Es por tanto un dispositivo que gestiona la red al realizar un direccionamiento eficiente del tráfico.

Al trabajar al nivel 3 del modelo OSI realiza las funciones del nivel 1 y dos además del nivel 3.

Con un encaminador o router podemos enlazar redes de diferentes topologías, ya que el dispositivo es capaz de direccionar paquetes de datos para diferentes topologías de red.

La técnica de encaminamiento se realiza por los encaminadores o router y puede seguir dos criterios:

- Encaminamiento estático.
  Una vez elegido el camino óptimo para que un paquete llegue a su destino, el resto de paquetes sucesivos con el mismo destino van por la misma ruta.
- Encaminamiento dinámico.
  A diferencia del anterior, para cada paquete se analiza de nuevo la ruta óptima, por lo que paquetes con el mismo destino, pueden seguir rutas diferentes en función de la carga del tráfico que haya en cada momento.

Este último caso es el caso más eficiente para la gestión de una red.

La ruta óptima no siempre implica el camino más corto.

Para elegir esta ruta se tienen en cuenta muchos criterios como:

- Número de saltos o nodos necesarios para llegar al destino.
- Carga del tráfico en cada enlace.
- Fiabilidad de cada enlace.
- Coste de cada enlace.
- Etc.

Por tanto, son muchos los factores que influyen para un encaminador o router para la elección de la ruta en la cual muchas veces se tienen en cuenta todos los factores anteriores, pero ponderados de una forma u otra en función de cómo se quiera gestionar la red.

En cualquier caso, es un proceso que se realiza de forma automática y con la mínima intervención del administrador de la red.

Todos los paquetes disponen de un campo denominado TTL (Time to live), es decir, tiempo de vida del paquete.

Se trata de un campo que intenta impedir que un paquete se quede circulando por la red de nodo a nodo sin llegar a su destino, debido a errores en el direccionamiento, alteración de la dirección IP del paquete, etc., y que puede entorpecer el tráfico por la red.
Es por ello que cuando a un encaminador o router le llega un paquete, siempre resta una unidad al valor de este campo (previamente está definido por un valor) y comprueba además si tras la resta el valor sale cero. En caso afirmativo, descarta el paquete.
De esta manera, se evita que estén los paquetes circulando por la red sin llegar a su destino.

Pasarelas o Gateways:

Se trata de un dispositivo de interconexión de redes que trabaja a nivel de transporte o nivel 4 del modelo OSI, o bien a nivel de aplicación del modelo TCP/IP..
Integra todas las funciones de las capas inferiores y por ello actúa intrínsecamente como hub, switch y router.
Se trata de un dispositivo avanzado de interconexión que se caracteriza por ser capaz de convertir protocolos, es decir, es capaz de unir redes que emplean protocolos de comunicación diferentes, ya que reformatea los paquetes de un protocolo a otro para que puedan circular de una red a otra.
Las pasarelas realmente son aplicaciones software que se instalan en encaminadores o router para ampliar sus funcionalidades y con ello actuar como gateways o pasarelas.
Entre las funciones que realiza una pasarela destacan:

- Conversión de protocolos.
- Funcionamiento como NAT.
- Funcionamiento como cortafuegos.
- Gestión eficiente de redes.
- Etc.

Aunque su coste es más caro que en el resto de los dispositivos de interconexión se emplean para la interconexión de grandes redes.

Routers. Conmutadores de nivel 3

Anteriormente se ha descrito que los routers son dispositivos de interconexión que trabajan a nivel de red o nivel 3 del modelo OSI.
En cambio, los conmutadores o switch son dispositivos de interconexión de redes que trabajan a nivel de enlace o nivel 2 del modelo OSI.
Es por ello que un router es un dispositivo que ofrece mayor 'inteligencia' y funciones más avanzadas para la gestión e interconexión de redes.
No obstante, existen los denominados conmutadores de nivel 3, que son switches que incorporan funciones avanzadas propias del nivel 3.
No incorpora todas las funciones propias de un router pero sí algunas funciones de ruteo y encaminamiento.
Entre las funciones propias del nivel 3 que incluyen estos conmutadores se encuentran:

- Detección de errores a nivel 3 mediante checksum.
- Determinación de rutas óptimas o de camino mínimo.
- Implementación de redes virtuales VLAN.

También son muy empleados los conmutadores de nivel 3 cuando se quieren segmentar redes grandes, para conseguir con ello una mejor gestión del tráfico de la red o simplemente una mejora del rendimiento.
Este tipo de dispositivos lo que hacen, en definitiva, es partir en trozos una red, de forma que sólo los paquetes que vayan a otra red son direccionados hacia ello, impidiendo que todos circulen por toda la red con la consiguiente pérdida de eficiencia.
Esto último es muy utilizado en redes de difusión o broadcast.

Existen dos tipos de conmutadores de nivel 3:

- Conmutador de paquete por paquete.
  Se trata de un tipo de conmutador que realiza las siguientes funciones en esta secuencia:
  - ⇨ Abre la cabecera del paquete y lo examina.
  - ⇨ Calcula su CRC (verificación por redundancia cíclica) para ver que el paquete no es erróneo.
  - ⇨ Si es erróneo lo descarta y pide retransmisión.
  - ⇨ Si es correcto decodifica su dirección IP origen y destino y lo enruta por la ruta según el protocolo establecido.

  Se trata de un conmutador de nivel 3 sencillo y básico que realiza las funciones propias del nivel 2 (conmutador) pero algunas funciones del nivel 3 como las descritas anteriormente.
- Conmutador Cut-though:
  Se trata de un conmutador de nivel 3, más avanzado que el conmutador de paquete, ya que realiza las siguientes funciones:
  - ⇨ Examina varios campos de la cabecera del nivel 3.
  - ⇨ Obtiene la dirección IP destino.
  - ⇨ Enruta el paquete por la ruta óptica según el protocolo establecido estableciendo para ello una conexión punto a punto.

  El establecimiento de esta conexión punto a punto es lo que le da esa funcionalidad avanzada a este tipo de conmutador, ya que con ello se consigue una alta tasa transferencia de paquetes.
  Este tipo de conmutadores se utiliza con bastante frecuencia y es por ello que existen numerosos fabricantes de este tipo de conmutadores.

Concentradores

Los concentradores son los dispositivos de interconexión anteriormente descritos como repetidores o hub.
Trabajan a nivel 1 o nivel físico del modelo OSI y básicamente su función es recibir la señal por un puerto, regenerarla y reenviarla por todos sus puertos de salida.
Con ello se pretende alcanzar mayores distancias en los enlaces pero no realiza ninguna gestión del tráfico.
De hecho no enruta ni siquiera el paquete, ya que lo reenvía por todos sus puertos y tendrán que ser niveles superiores quienes enruten el paquete.
Actualmente, los concentradores están siendo sustituidos por los switches que incorporan estas funciones, además de las propias del nivel 2 o nivel de enlace en la que trabajan.

Conmutadores

Los conmutadores, como ya se ha descrito anteriormente, son dispositivos de interconexión que trabajan a nivel 2 o nivel de enlace del modelo OSI.
Son también llamados puentes o switch.
Además de integrar las funciones de niveles inferiores (las del nivel físico, es decir, las propias de un hub) realiza funciones como detección de errores a nivel de trama, direccionamiento lógico de tramas, segmentación de redes, etc.
Es uno de los dispositivos más empleados en la actualidad para la interconexión de redes junto con los routers.
Existen en el mercado una amplia variedad de ellos, ya que son muchos los fabricantes quienes lo comercializan.
Dentro de ellos destacan los conmutadores de nivel 3 que incorporan determinadas funcionalidades de ruteo propia del nivel 3 o nivel de red del modelo OSI.

Servidores VPN (Redes privadas virtuales)

El teletrabajo es una modalidad que se está imponiendo cada vez más en las relaciones laborales entre empresas y empleados.
Este sistema permite que cualquier empleado de una empresa pueda estar conectado a la red de área local (LAN) de su empresa sin estar físicamente allí y que pueda ejercer sus funciones propias que le tienen asignadas.

Esto hoy día ya es posible gracias a las redes y a los diferentes equipos, protocolos y dispositivos de interconexión que existen.
De esta manera, cualquier empresa con una conexión a Internet puede habilitar (es necesario habilitar) que algunos de sus empleados o incluso todos puedan acceder de forma remota a su red de área local.
Esta habilitación requiere de varios elementos:

- Que la red de área local (LAN o WLAN) de la empresa disponga de conexión a Internet.
- Que se configure un servidor VPN.
- Que el empleado o personas que quieran acceder de forma remota tenga un cliente VPN.
- Que estén configurados los permisos adecuados.

Un servidor VPN (Virtual Private Network) es un equipo hardware o una aplicación que 'corre' sobre un servidor de propósito general que permite accesos externos y remotos a una LAN o WLAN con los permisos adecuados a través de Internet.
La persona o empleado que quiera acceder a esta LAN o WLAN de forma remota, también deberá tener instalado un cliente VPN que es la aplicación que se conecta con el servidor VPN para intercambiar información de autenticación y de control para establecer la conexión.
El objetivo de una VPN es que el equipo remoto no note que está fuera de la red LAN o WLAN.
Es obvio que se requiere que la conexión a Internet por ambas partes (equipo remoto y empresa) sea de alta velocidad para evitar caídas y cortes en la conexión que impidan el trabajo por parte del equipo remoto.
En una red privada virtual o VPN se debe establecer un procedimiento o gestión para que pueda el equipo remoto acceder a la LAN o WLAN de la empresa.
Esta gestión o protocolo sigue los siguientes pasos:

- Se debe autentificar al cliente VPN:
  Para ello el software cliente VPN (el del equipo remoto) se debe conectar con el servidor VPN (en la LAN o WLAN de la empresa) en el que se debe loguear para verificar que es un cliente registrado. De esta forma se evita intrusos no deseados (téngase en cuenta que una vez conectado tiene accesos a todos los recursos de la red).
- Se debe establecer un túnel de Internet:
  La VPN consiste en establecer un 'túnel' entre el equipo remoto y la LAN o WLAN de la empresa de forma que todos los paquetes que se intercambian se encapsulen para que pueda traspasar una red insegura como es Internet.
- Se debe proteger el túnel:
  El uso de una red insegura como es Internet implica que la VPN debe cifrar la información para evitar que la información transmitida por el túnel sea interceptada, manipulada o corrompida durante la transmisión.
- Liberar el túnel:
  Una vez terminada la conexión se debe liberar el túnel.

El establecimiento del túnel mencionado anteriormente implica además que cuando el equipo se conecta a la red debe tener asignada una IP de la LAN o WLAN de la empresa. Esta asignación generalmente la realiza el servidor DHCP de la empresa.
La encapsulación es una técnica que consiste en empaquetar un paquete propia de una red LAN o WLAN (con su dirección IP local correspondiente) en un paquete que pueda circular por una red pública (como Internet) con una IP pública. Así, una vez llegado al Servidor VPN, elimina la IP pública y descifra la IP privada para que pueda ser redirigido al equipo local correspondiente.

Cortafuegos

Un cortafuegos o firewall es una aplicación software especializado que se intercala entre las aplicaciones y la tarjeta de red para realizar un filtrado de los paquetes.
El objetivo no es más que controlar los paquetes que entran y salen del equipo por la red con objeto de actuar correctamente ante paquetes sospechosos.
Es una herramienta básica para la seguridad de las redes y todos los equipos siempre deberían tenerlo instalado y activado.

El firewall se puede instalar tanto en equipos clientes como en equipos servidores, actuando de forma diferentes aunque empleando las mismas técnicas.
Un cortafuegos puede instalarse y funcionar en:

- Cortafuegos en un equipo cliente:
  En un equipo cliente, el cortafuegos actúa aplicando un filtrado de paquetes.
  En el tráfico saliente, es decir, de paquetes que salen del equipo hacia la red el cortafuegos o firewall analiza la cabecera de cada paquete y en función de las reglas que tenga definidas en el cortafuegos realiza una acción u otra. Por ejemplo, si detecta que la máquina cliente hace spam bloquea el puerto 25 (puerto de correo electrónico).
  En el tráfico entrante, es decir, de paquetes que entran al equipo cliente, analiza la cabecera de cada paquete, y en función de las reglas de configuración, actúa de una forma u otra.
- Cortafuegos en un equipo servidor:
  En un equipo servidor, el cortafuegos también actúa aplicando un filtrado de paquetes.
  En el tráfico saliente, es decir, de paquetes que salen del equipo hacia la red, el cortafuegos o firewall analiza la cabecera de cada paquete, y en función de las reglas que tenga definidas en el cortafuegos realiza una acción u otra. En este tráfico es donde generalmente actúa el cortafuegos, puesto que en un servidor la mayor parte del tráfico es saliente.
  En el tráfico entrante, en cambio, el firewall analiza qué paquetes quieren acceder a qué puertos del servidor para bloquear en el caso de un ataque al servidor si así lo tiene en las reglas de configuración.

7.1.3. Influencia sobre las prestaciones de red

Los dispositivos de interconexión anteriormente descritos tienen como objetivo la conexión de equipos y redes, de forma que los diferentes usuarios puedan intercambiar información entre sí de forma electrónica y telemática.
En toda interconexión estos equipos deben realizar al menos las siguientes funciones básicas:

- Búsqueda de equipos conectados en la red e identificación de su IP para la actualización de la base de datos o tabla de direccionamiento.
- Señalización de los paquetes, tramas o datagramas en la red y gestión del tráfico.
- Codificación y decodificación de paquetes, tramas o datagramas que pasen por el dispositivo de interconexión.

Estas funciones que realizan los dispositivos de interconexión permiten mejorar las redes en los siguientes aspectos:

- Mejora la gestión de la red y del tráfico existente.
- Permite interconectar equipos y redes entre sí.
- Permite ofrecer multiservicios a todos los equipos con la compartición de recursos.
- Reducción de recursos y costes.

Pero también la inclusión de equipos de interconexión en la red, pueden tener e introducir una serie de desventajas (que aunque pueden minimizarse) que deben ser tenidas en cuenta:

- El proceso de señalización, routeo y codificación/descodificación siempre introduce retardos y jitters que deben ser tenidos en cuenta en las transmisiones, sobre todo para servicios críticos como servicios en tiempo real.
- Como todo elemento de red es un punto más de posible fallo.
- Además, en este caso el fallo de un dispositivo de interconexión puede afectar a muchos equipos que forman parte de una misma red.
- Suele ser un dispositivo que debe ser administrado y gestionado por un administrador de red por lo que supone un coste humano y técnico a veces considerable.

No obstante, la influencia de cada dispositivo de interconexión vendrá condicionada por el nivel en el que actúa: nivel físico, de enlace, de red, etc.

7.1.4. Requerimientos ambientales de los equipos de comunicaciones

Los dispositivos de interconexión, como todo elemento electrónico, deben cumplir una serie de requerimientos del entorno ambiental, con objeto de garantizar su buen funcionamiento.
Estos requerimientos pueden clasificarse en base a dos parámetros:

- Emplazamiento.
  - Los equipos deben estar siempre en lugares accesibles para su mantenimiento.
  - Deben estar alejados de zona de interferencias eléctricas, de inundación, de humedades, etc.
  - Lejos de materiales peligrosos o inflamables.
  - Etc.
- Condiciones del entorno.
  - Temperatura entre -10º y 40º.
  - Humedad relativa entre 30% y 55%.
  - Renovación del aire al menos 2 veces/hora.
  - Alejado de ruidos impulsivos.
  - Alejados de maquinarias vibratorias y mecánicas.

Los fabricantes en su hoja de características de los dispositivos indican el rango de funcionamiento en los cuales garantiza el correcto funcionamiento del equipo.
Es por ello recomendable seguir dichas indicaciones para evitar fallos en los dispositivos de interconexión.

7.1.5. Catálogos de productos de equipos de interconexión

Existen en el mercado numerosos fabricantes de equipos de interconexión, como pueden ser TP-LINK, NetGear, Cisco, etc.
Todos ellos fabrican o distribuyen los dispositivos anteriormente descritos como son hub, switch, router y gateways.
Existe una amplia variedad de ellos, no sólo en los fabricantes sino en los modelos existentes, ya que presentan variaciones en cuanto a prestaciones y características.
Es por ello que a la hora de comprar e instalar algunos de ellos, es recomendable consultar varios modelos de varios fabricantes ya que no son exactamente iguales y donde además del precio, es recomendable ver las funcionalidades que ofrece y que pueden ser necesarias para la red que queramos configurar.
Veamos a continuación algunos de los modelos comerciales de dispositivos.

Swith 8 puertos modelo TL-SF1008D de TP-LINK:

Se trata de un switch de 8 puertos RJ-45 10/100 Mbps.
Se trata de un switch no gestionable muy apto para entornos de oficinas pequeñas o entornos domésticos.
Destacamos a continuación sus prestaciones más relevantes:

- ⇨ 8 puertos RJ-45 10/100 Mbps con detección automática de velocidad.
- ⇨ Switch cableado con salida RJ-45.
- ⇨ Tecnología Plug&play.
- ⇨ Detección automática MDI / MDIX que hace innecesario el uso de cables cruzados.
- ⇨ Eficiencia energética de hasta un 70%.
- ⇨ Soporta todas las normas 802.3x.

Se trata de un switch no gestionable, por lo que no es válido para entornos de altas prestaciones y servicios críticos.

Swith 24 puertos modelo 24P + 4 SFP JetStream TL-SG5428 de TP-LINK:

Se trata de un switch de 24 puertos RJ-45 10/100/1000 Mbps con 4 puertos de fibra SFP (Permiten que el switch se conecte a cables de fibra óptica de diferentes tipos – incluyendo modos monomodo y multimodo).
En la siguiente figura podemos ver el dispositivo.

Se trata de un switch gestionable a nivel 2 (L2) apto para entornos profesionales y gestión de servicios de streaming y aplicaciones críticas.
Destacamos a continuación sus prestaciones más relevantes:

- ⇨ Switch de 24 puertos 10/100/1000 Mbps, es decir, puertos Gigabit Ethernet.
- ⇨ Incorpora además 4 puertos SFP Gigabyte Ethernet para fibra óptica.
- ⇨ Switch gestionable a nivel L2 (nivel de enlace).
- ⇨ Tiene un puerto de consola para la gestión del switch.
- ⇨ Soporta tecnología IGMP Snooping necesaria para transmisión de streaming.
- ⇨ Permite aplicaciones de VoIP.
- ⇨ Soporta VLAN, es decir, crear redes privadas virtuales.
- ⇨ En cuanto a seguridad, incorpora DoS Defence, Filtrado MAC, Port mirroring, entre otros.

Router inalámbrico 3G modelo TL-MR3220 de TP-LINK:

Se trata de un router inalámbrico con tecnología Wifi y con cobertura 3G.
En la siguiente figura podemos ver el dispositivo.

Además de conectividad inalámbrica, presenta cuatros puertos Rj-45 para una conectividad cableada.
Es un dispositivo apto para entornos de oficinas pequeñas y entornos domésticos.
Destacamos a continuación sus prestaciones más relevantes:

- ⇨ Router inalámbrico Wifi con cobertura 3G.
- ⇨ Incorpora además 4 puertos RJ45 10/100 Mbps para una conectividad cableada.
- ⇨ Incorpora un puerto USB 2.0 para conexión con un módem.
- ⇨ Soporta los estándares 802.11b) g) n).
- ⇨ Frecuencia de funcionamiento 2.4-2.48 Ghz (frecuencia Wifi).
- ⇨ Gestión y configuración del equipo mediante acceso web HTTP.
- ⇨ Funciones de seguridad como cortafuegos, filtrado MAC, radius, etc.

7.2. Contratación de acceso básico a redes públicas

Todas las redes privadas LAN o WLAN al final deben tener una salida a una red pública como es Internet. Esta conexión se realiza a través de un router, el cual conecta una red privada con una red pública.
La conexión puede ser cableada o inalámbrica, siendo la primera la más empleada para entornos de oficinas y entornos domésticos (conexión a la red pública).
El acceso a Internet requiere la contratación del acceso a un operador o ISP, que requiere la formalización de un contrato en el que se especifican las condiciones del servicio, fundamentalmente velocidad (3 Mbps, 5 Mbps, 10 Mbps, 20 Mbps, 50 Mbps) y su disponibilidad (generalmente 24 horas en una modalidad de tarifa plana).
Dependiendo del tráfico de nuestra red y de los servicios que queramos usar de Internet, debemos ajustar la velocidad contratada para que no tengamos problemas de baja velocidad cuando muchos equipos quieran acceder a los servicios de la red.

Conceptos más importantes de la Unidad Formativa

1. Introducción a las comunicaciones y redes de computadoras

- ⇨ Definición de Telecomunicación
- ⇨ Clasificación de las redes según el espacio que ocupan: LAN (Local), MAN (Metropolitana), WAM (Extensa)
- ⇨ Definición y funciones de los protocolos
- ⇨ Concepto del Modelo OSI y Protocolo TCP/IP

2. Principios de transmisión de datos

- ⇨ Concepto de transmisión de datos
- ⇨ Formas de Flujo de datos: símplex, semi-dúplex y dúplex
- ⇨ Modos de transmisión: Serie y Paralelo
- ⇨ Tipos de transmisión: asíncrona y síncrona
- ⇨ Formato de la señal: analógica y digital. Ventajas e inconvenientes
- ⇨ Concepto de Perturbaciones en la transmisión: Atenuación, Distorsión, Ruido

3. Medios de transmisión guiados

- ⇨ Conocer los 4 tipos de cable: Par trenzado, Coaxial, Fibra óptica y el hilo telefónico
- ⇨ Características constructivas de cada tipo de cable tanto el par trenzado, coaxial y fibra
- ⇨ Características de transmisión de cada tipo: cada cuanto hay que repetirlo, problemas, ventajas e incovenientes

4. Medios de transmisión inalámbricos

- ⇨ Medios de transmisión no guiados: por radiofrecuencias (frecuencias) o infrarrojos (Longitudes de onda)
- ⇨ Frecuencias de transmisión inalámbricas (Concepto)

5. Control de enlace de datos

- ⇨ Función de la capa de enlace (2): Tramado, Direccionamiento físico, Control de Flujo y de Errores
- ⇨ Se subdivide en 2: MAC, LLC (recordar la MAC detecta errores y la LLC realiza el control de errores)

6. Protocolos

- ⇨ En que capa trabaja cada protocolo, características principales y cuál es su función:
  IP (3), TCP(4) y UDP (4)
- ⇨ Clases de Redes: A, B, C, D, E
- ⇨ IP Privada, IP Pública, IP Fija, IP Dinámica
- ⇨ Dirección MAC (concepto)
- ⇨ Concepto de Mascara de Red, Puerta de Enlace… (Que configuramos cuando le ponemos IP Fija al ordenador)
- ⇨ Creación de Subredes, cuanto más pequeño el numero menos subredes podemos hacer y más equipos podemos conectar, por ejemplo:
  Con mascara 255.255.255.0 -> una sola subred y 254 equipos
  pero con mascara 255.255.255.192 -> 4 Subredes y 62 equipos en cada una
- ⇨ Concepto de Puerto
- ⇨ Concepto de NAT (encapsular nuestra dirección privada: 192.168.1.10 en una dirección pública de Internet, la del router)

7. Equipos de interconexión de red:

- ⇨ Conocer las características y diferencias de los dispositivos más importantes:
  Hub, switch, router y Gateway. En que capa trabajan, para que se usan, ventajas, inconvenientes…
- ⇨ Concepto de VPN (Red Privada Virtual)