PROGRAMA MODULAR EN ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED

PRÁCTICO

Proyecto

Título: Red Corporativa de Empresa físico-deportiva

Autor: Sergio López de la Hoz

Tutora: Dra. Elena Ruiz Larrocha

Curso académico: 2020-2021

AGRADECIMIENTOS

A la Dra. Elena Ruiz y a todos los profesores que me han acompañado en esta aventura dándome su total disponibilidad y principalmente a mis compañeros de trabajo, familia y pareja por su paciencia y su empuje para que siguiera estudiando a pesar de las dificultades.

Índice de contenido

Índice de figuras

Índice de tablas

1. Resumen/Summary

RESUMEN

Este Proyecto parte de la base de una empresa que se dispone a la apertura de dos gimnasios, siendo de una misma franquicia y separados geográficamente en la Comunidad de Madrid, a los que se necesita dotar de conexión informática entre ellos, por lo que se necesita diseñar una red corporativa local a través de la cual tengan accesos a los mismos recursos.

Esta interconexión se llevará a cabo a través de un controlador de dominio situado en cada sede y replicado, trabajando sobre el mismo dominio y unidos por VPNs a través de un router Mikrotik. Además, se dotará de un servidor web local utilizando un CMS como WordPress para poder reservar plaza en las distintas actividades de salas (zumba, pilates, spinning…) y de un servidor OwnCloud para compartir diferentes dietas y tablas de rutinas de definición.

SUMMARY

This Project starts from the base of a company that is preparing to open two gyms, being from the same franchise and geographically separated in the Community of Madrid, which need to be provided with a computer connection between them, so it is necessary design a local corporate network through which they have access to the same resources.

This interconnection will be carried out through a domain controller located in each headquarters and replicated, working on the same domain and joined by VPNs through a Mikrotik router. In addition, it will be equipped with a local web server using a CMS such as WordPress to be able to reserve a place in the different activities of rooms (zumba, pilates, spinning ...) and an OwnCloud server to share different diets and tables of definition routines.

2. Antecedentes/Introducción

Se parte de la base de una empresa que se dispone a la apertura de dos gimnasios pertenecientes a una franquicia a los que necesita dotar de conexión informática entre ellos, por lo que necesita diseñar una red corporativa local a través del cual tengan acceso a los mismos recursos.

Esta conexión se establecerá gracias a una VPN realizada con routers Mikrotik y servidores replicados, intentando que el sistema sea más estable aumentando la fiabilidad en caso de fallo y mejorando el rendimiento.

Las sedes se encuentran ubicadas en la Comunidad de Madrid, concretamente en Coslada y Vallecas, en las cuales se ofertará de acceso a internet para los clientes a través de ordenadores ubicados en cada una de las sedes, con Windows 10 ya instalados previamente.

Esta empresa ofrecerá a los clientes a través de un blog local poder reservar cita con una hora determinada para realizar diferentes actividades en las diferentes salas hasta agotar el cupo de clientes máximos, que será llevado a cabo con un CMS potente como es WordPress a través de plugins.

Además, será necesario un Sistema de almacenamiento de archivos para que el cliente pueda acceder a rutinas y tablas de ejercicios que estarán almacenados en la aplicación OwnCloud en un servidor dedicado a dicha tarea.

3. Objetivos generales y específicos y alcance del proyecto

Los objetivos generales se basarán en el diseño de una red local de una pequeña empresa, en este caso un gimnasio, desarrollando los conocimientos adquiridos en los distintos módulos impartidos en el grado de Asir. Se instalarán controladores de dominio con servidores replicados para trabajar en un mismo dominio y se utilizarán servicios informáticos alojados en otros servidores como un blog y un servicio de almacenamiento.

Los objetivos específicos del proyecto se centrarán en las diferentes configuraciones para su correcto funcionamiento, detallando los pasos a seguir en cada elemento que compone dicha red y sus posteriores servicios desplegados.

Concretamente, se realizarán los siguientes puntos:

Servidores de dominio: Se instalará un servidor con Windows Server 2012 r2 que actuará como controlador de dominio. Una vez creado se replicará en la otra sede para tener mayor rendimiento y disponibilidad.

Mikrotik: Se instalará y se configurará estos routers comerciales de Mikrotik[1] para poder crear las VPNs trabajando como una única red haciéndose visibles todos los elementos que componen dicha red, además de actuar como servidor de DHCP.

Blog: Se creará un servidor específico para poder albergar el blog. Dicho blog se creará mediante un CMS, concretamente WordPress[2], utilizando un plugin para poder realizar y visualizar las reservas. Se instalará previamente XAMPP[3], que nos permitirá trabajar con Apache, MySQL y PHP.

Owncloud: Instalaremos un servidor específico de OwnCloud[4] en nuestra red para así poder almacenar y compartir diferentes archivos entre las sedes.

4. Definiciones

AD: Acrónimo de Active Directory. Es el término que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos, principalmente LDAP, DNS, DHCP y Kerberos.

CMS: Un Sistema de gestión de contenido (CMS) es una aplicación que te permite publicar y administrar contenido en la web de forma intuitiva.

CNAME: Es un tipo de registro DNS que asigna un alias a un nombre de dominio auténtico o canónico.

DHCP: Dynamic Host configuration Protocol. Es un portocolo de red en el que un servidor permite una asignación automática de direcciones IP, getaways predeterminadas, así como otros parámetros de red que necesiten los clientes.

DNS: DNS es el acrónimo para "Domain Name System" (sistema de nombre de dominio). DNS es un servicio que habilita un enlace entre nombres de dominio y direcciones IP con la que están asociados.

Firewall: es un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

ISO: Es lo que se conoce como «una imagen» o copia exacta del sistema de archivos y contenido de un CD o DVD.

Mikrotik: Es un fabricante letón de equipos de red. La compañía desarrolla y vende enrutadores de red cableados e inalámbricos, conmutadores de red, puntos de acceso, así como sistemas operativos y software auxiliar.

PHP: Acrónimo recursivo de PHP: Hypertext Preprocessor. Es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML.

Plugin: Un plugin en WordPress es un fragmento de código que se conecta a tu sitio web de WordPress. En pocas palabras, es una extensión a tu sitio que modifica y mejora las funciones principales de WordPress

RouterOS: es el sistema operativo que utilizan los routers de Mikrotik, productos estrella de la compañía, basado en la robustez y versatilidad de GNU/Linux.

TCP: Es el Protocolo de Control de Transmisión que permite establecer una conexión y el intercambio de datos entre dos anfitriones.

URL: Significa Uniform Resource Locator (Localizador de Recursos Uniforme**).** Es el mecanismo usado por los navegadores para obtener cualquier recurso publicad en la web.

VMware: Es un programa que te permite ejecutar una computadora virtual dentro de una computadora física. La computadora virtual funciona como si fuese una máquina independiente.

VPN: Una VPN (Virtual Private Network) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.

Winbox: Es una pequeña aplicación que nos permite la administración de Mikrotik RouterOS usando una interfaz gráfica.

WordPress: Es un sistema de gestión de contenidos (CMS) que permite crear y mantener un blog u otro tipo de web**.**

XAMPP: es un servidor independiente de plataforma, software libre, que consiste principalmente en la base de datos MySQL, el servidor web Apache y los intérpretes para lenguajes de script: PHP y Perl.

5. Planificación y costes.

Se procede a diseñar un presupuesto con los costes que conllevará la ejecución del proyecto que se plantea, como muestra Figura 1.

Se cuenta de partida con 2 equipos informáticos funcionales para los usuarios (uno por cada sede) que proporciona la empresa con Windows 10 instalado previamente.

INFORMATICA ASIR
C/ Lagasca, 10
28006 MADRID
MADRID
Telf: 91 876 38 08
CIF.:F78037876
infoasir@informaticasir.com

Presupuesto a:
GYM ASIR
CIF E86398864

Fecha: 04/04/2021 Nº Presupuesto: 23AC789

Referencia	Descripción	Unid.	Precio	%Dto.	Importe
10276	TP-Link 24 Puertos Gigabit Switch	2	66,15	0,00	132,3
13275	Mikrotik RB3011UIAS-RM	2	152,62	0,00	305,24
12345	deleyCON CAT6 Patch Panel	2	45,49	0,00	90,98
11232	HP 24m - Monitor de 23.8" FullHD	2	109,00	0,00	218,00
12345	HPE Proliant DL20 Gen10 Intel Xeon E-2224/16GB	4	779,00	0,00	3116,00
12332	Licencia Windows server	4	287,01	0,00	1148,04
10276	Materiales varios (latiguillos, conexiones,etc)	1	90,50	0,00	90,50
12732	Armario Rack Mural 19" 9U 600x450x500mm Pared Negro	2	159,09	0,00	318,18
20	Mano de Obra	25	30,00	0,00	750,00

Este presupuesto tendrá una validez de 30 días naturales desde la fecha arriba indicada.

Nº Líneas: 9

Base Imponible Cuotas de IVA Cuotas de Rec.Equiv.

Base imponible: 4873,70 €
Total Impuestos: 1295,54 €
Total Presupuesto: 6169,24 €

El pago se realizará a través de transferencia bancaria

Figura 1. Presupuesto para su implantación.

Además del presupuesto, se hace una planificación temporal de lo que abarcará el desarrollo de dicho proyecto, acordando su finalización en una semana (5 horas diarias) de lunes a viernes, con la distribución que se muestra en la Tabla 1.

SERVICIO	TIEMPO EMPLEADO
Instalación/Configuración MIKROTIK Vallecas	4 h
Instalación/Configuración Server DC Vallecas	3 h
Instalación Server Web	2 h
Configuración WordPress	2 h
Instalación Server OwnCloud	2 h
Configuración OwnCloud	2 h
Instalación/Configuración Mikrotik Coslada	4 h
Instalación/Configuración Server DC Coslada	3 h
Comprobaciones/Correcciones para buen funcionamiento	3 h
TOTAL	**25 horas**

Tabla 1. Panificación Temporal (Fuente: propia).

6. Desarrollo del trabajo final

El proyecto consiste en el diseño de una red de una empresa que consta de varias sedes.

En la Figura 2 se muestra el esquema a desarrollar para dar solución a esta empresa.

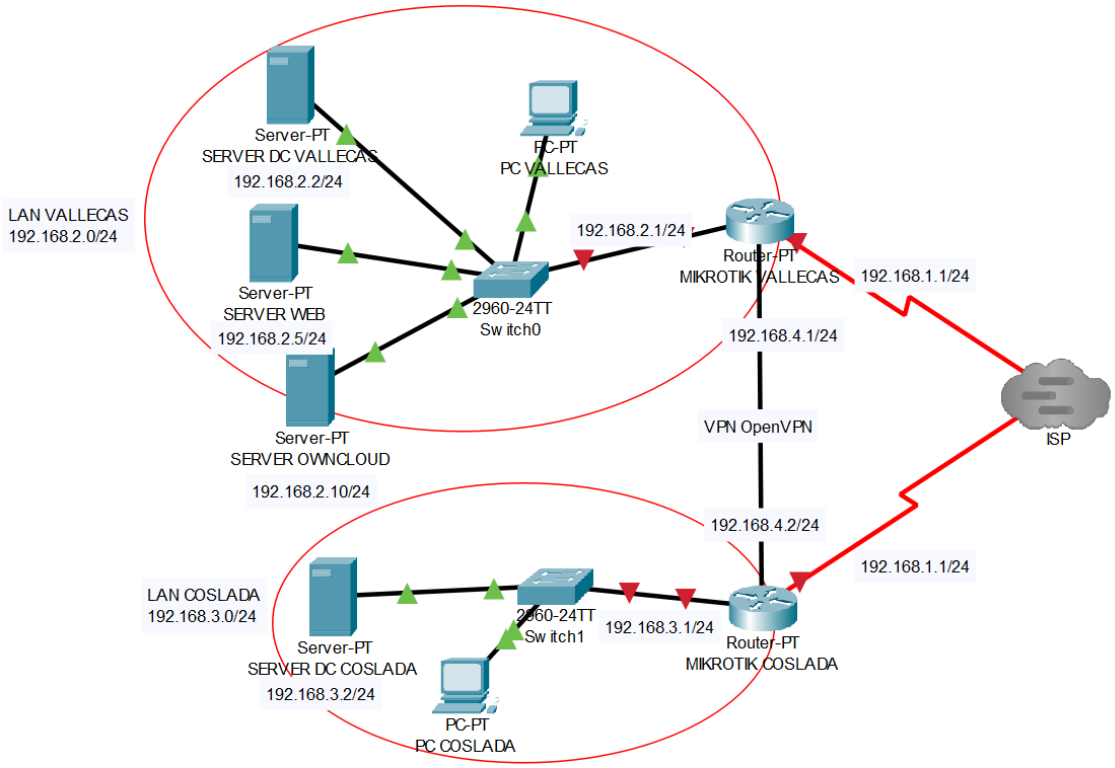

Figura 2. Esquema del sistema.

Toda la implementación de la red se va a desarrollar a través de máquinas virtuales, a través del programa de virtualización VMware.

Para ello realizaremos los siguientes puntos

6.1 Instalación y configuración de Servidores DC

Poder establecer parámetros de inicio de sesión y seguridad para todos los dispositivos desde un sitio centralizado reduce el tiempo de tener que proteger y configurar cada dispositivo individualmente, por ello es necesario instalar un controlador de dominio.

Este controlador de dominio, además de estas las ventajas, posee la virtud de tener una organización dentro del negocio, creando grupos con los usuarios de cada departamento. Con ello tenemos un control de los permisos a los recursos de la red, pudiendo por ejemplo asignar a una carpeta, dependiendo del departamento, permisos de lectura, un control total, etc.

Para ello en este apartado, vamos a ver cómo llevar a cabo la instalación de servidores de controlador de dominio y su configuración, desde la instalación en nuestra máquina virtual hasta que hacemos pertenecer un host a ese dominio.

6.1.1 Instalación de Windows Server 2012 R2

Aunque no es el más avanzado, se ha elegido Windows Server 2012 R2 para la instalación de los servidores ya que ha sido el más accesible en mi caso.

Este sistema operativo, aun no siendo el más moderno que existe actualmente, es completo y totalmente útil para nuestras necesidades.

Los siguientes pasos que vamos a describir serán válidos para la instalación de todos los servidores que vamos a necesitar.

Empezamos con la ISO de Windows Server 2012 R2 en la máquina virtual y arrancamos dicha máquina.

Esperamos que se ejecute el instalador hasta que accedemos a la primera ventana, en la que seleccionaremos el idioma, el formato de la hora y moneda y el teclado, como muestra la Figura 3. Verificamos que está en español y pasamos a la siguiente ventana donde pulsaremos “Instalar Ahora”, como podemos ver en la Figura 4Figura 5.

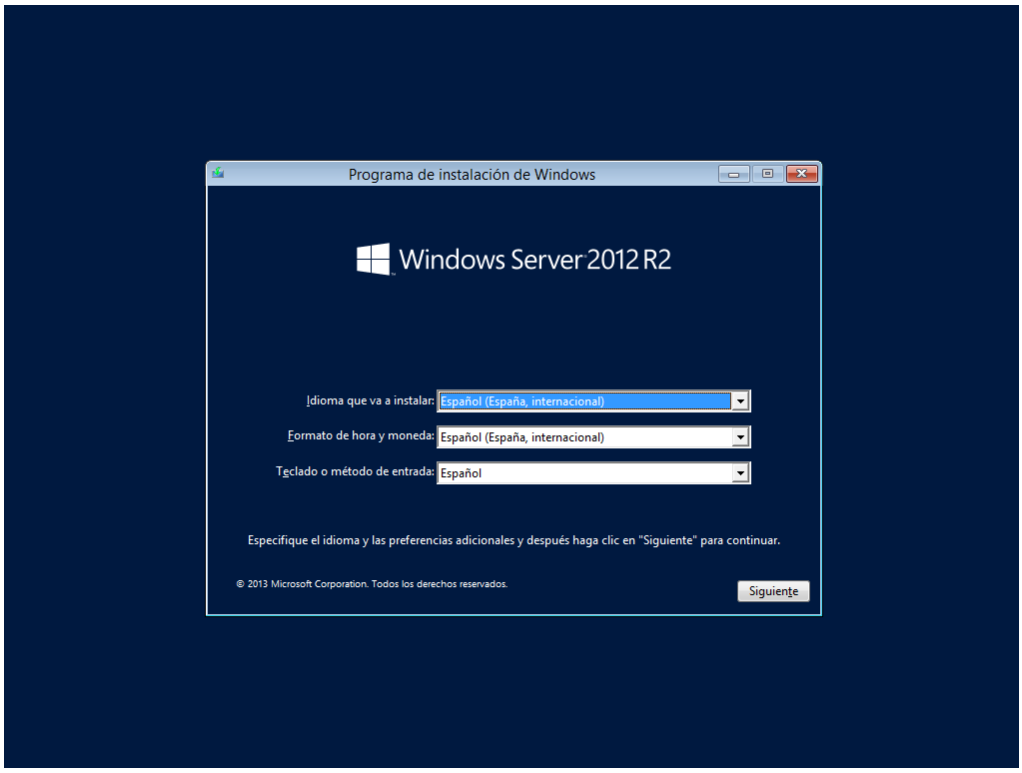

Figura 3. Selección de idioma, formato de hora y teclado.

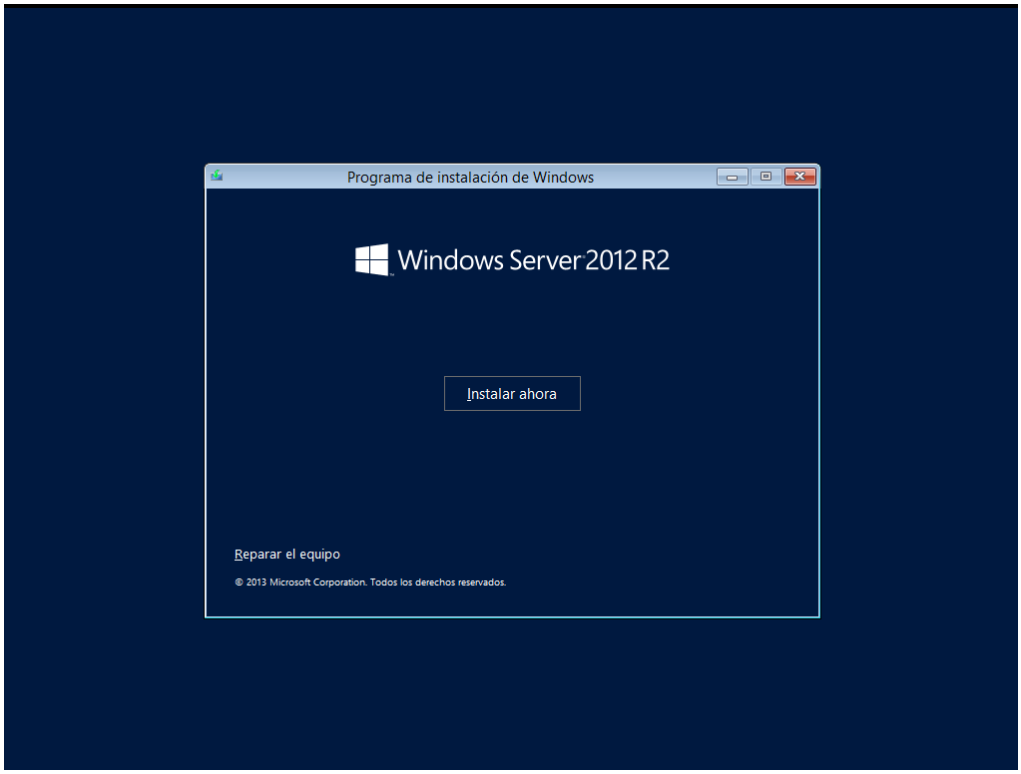

Figura 4. Ventana de inicio de instalación.

En la siguiente ventana que muestra la Figura 5Figura 5, seleccionamos “Windows Server 2012 R2 Standard (servidor con una GUI)” que es la que vamos a utilizar para los servidores de nuestra red.

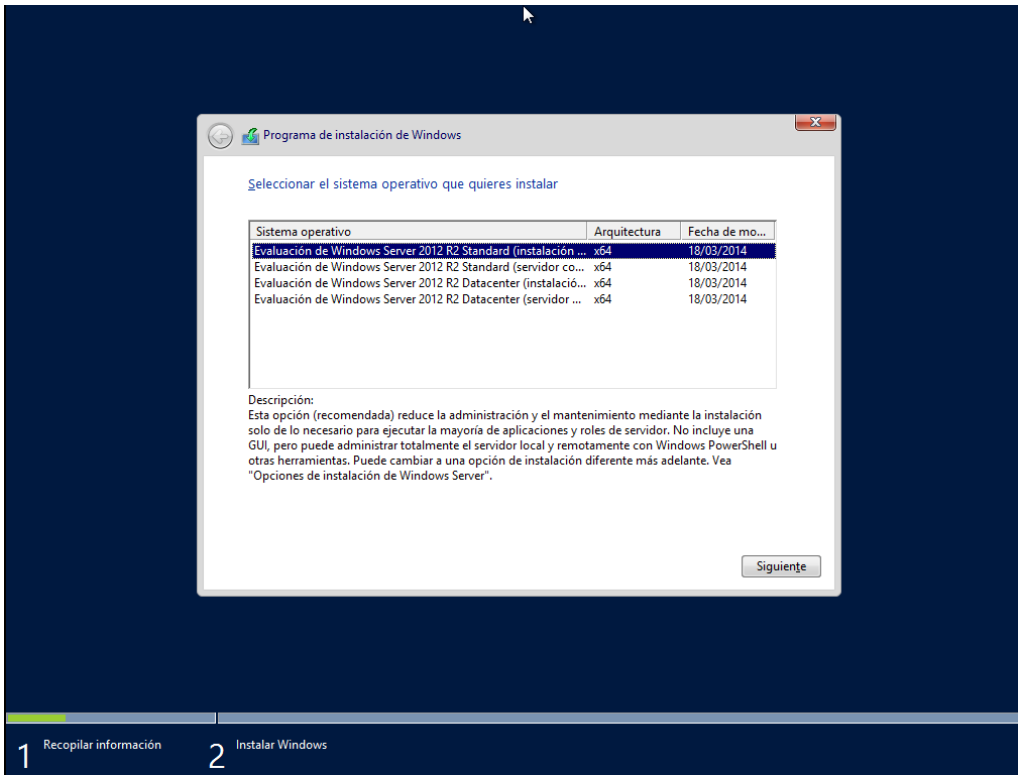

Figura 5. Selección de sistema operativo.

Lo siguiente será aceptar las condiciones de la licencia que impone Microsoft para su uso como podemos apreciar en la Figura 6.

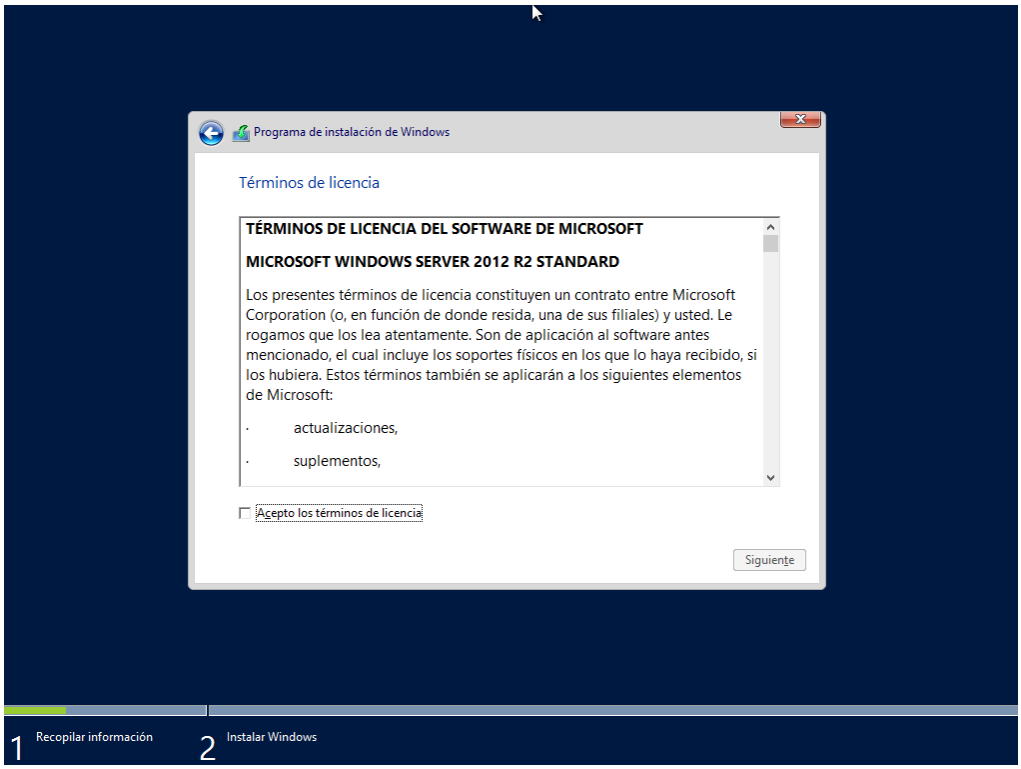

Figura 6. Términos de Licencia.

La siguiente ventana que vemos en la Figura 7 nos muestra dos opciones. Elegiremos la personalizada, ya que partimos de una instalación nueva y no queremos conservar ningún archivo anterior.

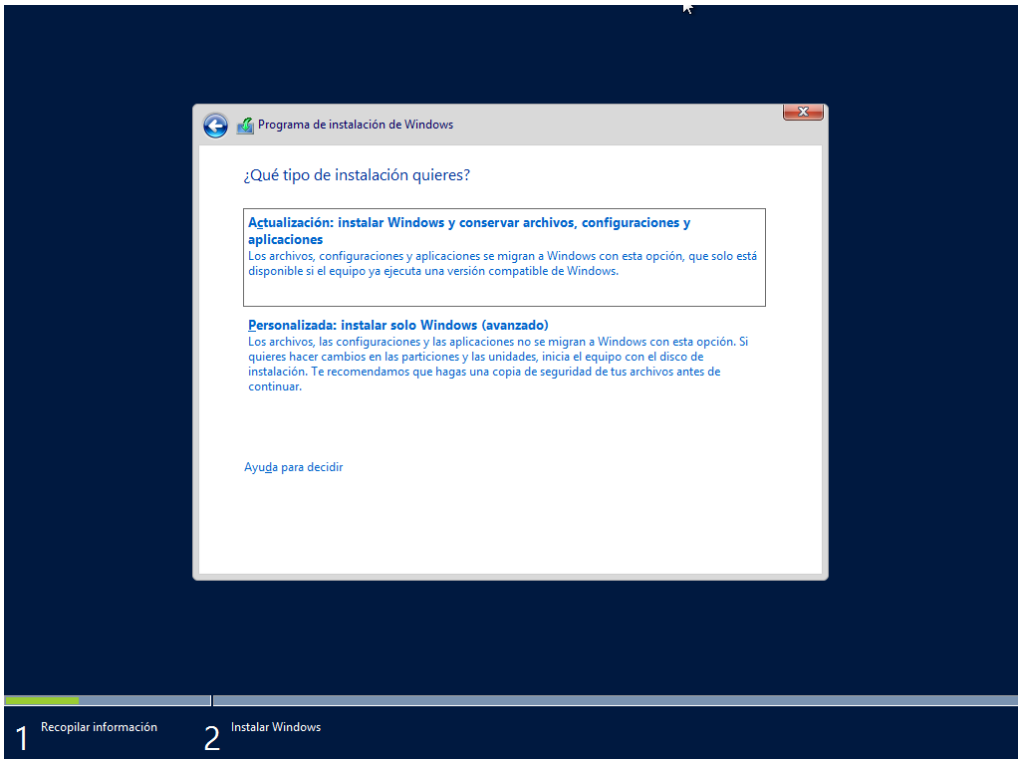

Figura 7. Selección de tipo de instalación.

La última cuestión que nos solicitará el instalador es seleccionar el disco, por lo que señalaremos el que nos muestra al ser la única partición, como podemos ver en la Figura 8.

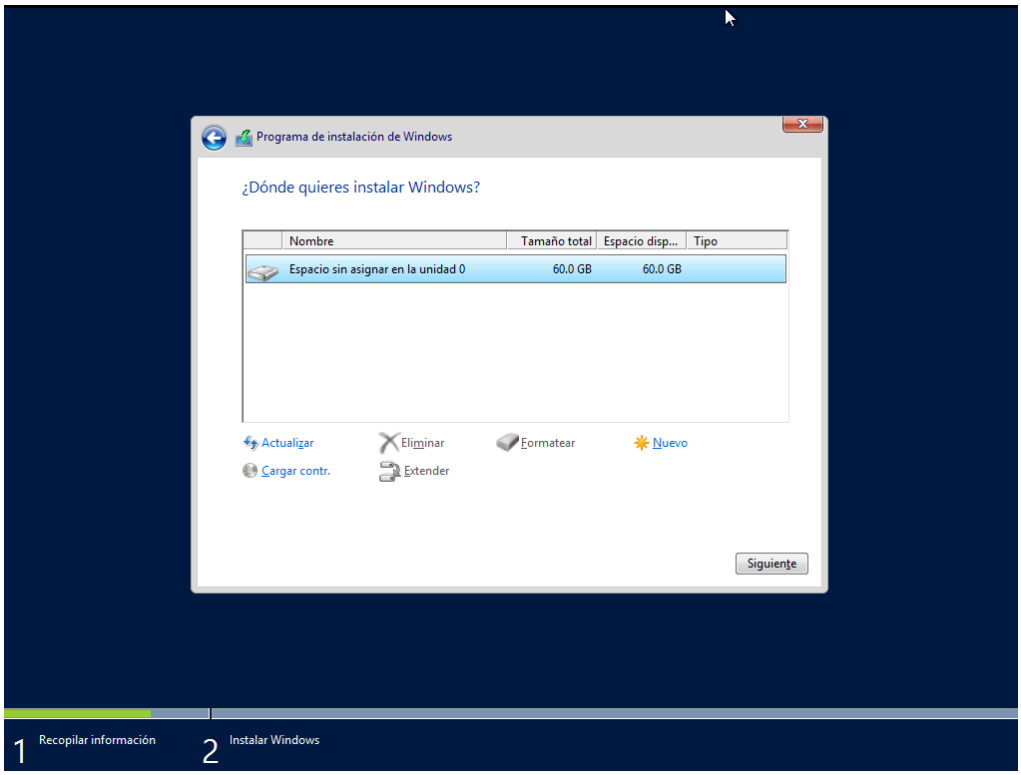

Figura 8. Selección de unidad de disco.

Una vez realizado este paso, se empezará a proceder en la instalación y se reiniciará el sistema cuando se haya completado al igual que vemos en la Figura 9.

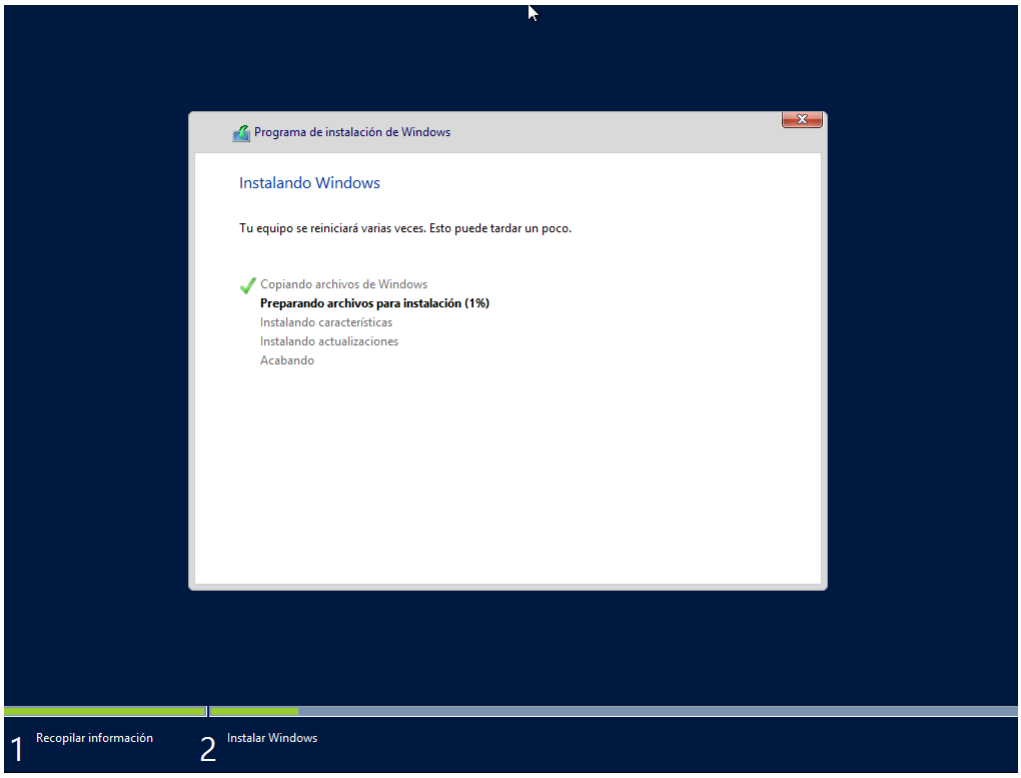

Figura 9. Proceso de instalación.

Al reiniciarse, el siguiente paso es personalizar la configuración, asignando un nombre de usuario y una contraseña, mostrándonos lo que vemos en la Figura 10.

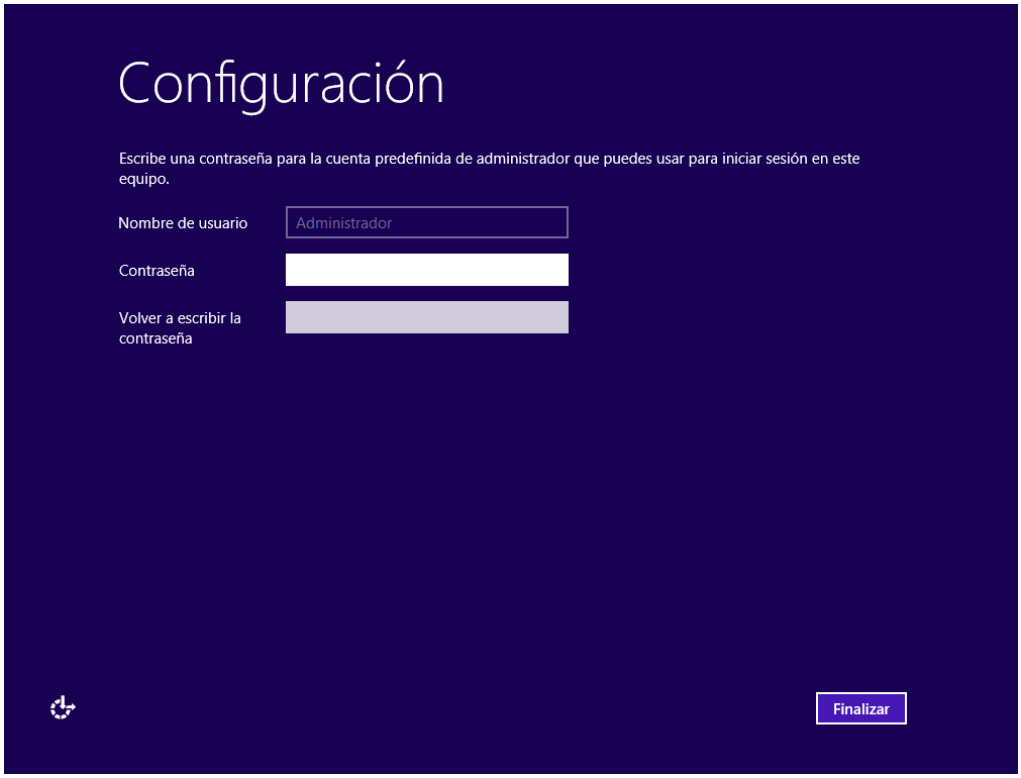

Figura 10. Configuración de la cuenta de administrador

Una vez introducidos esos datos, visualizaremos lo que muestra la Figura 11 y entraremos en el SO con dicha contraseña.

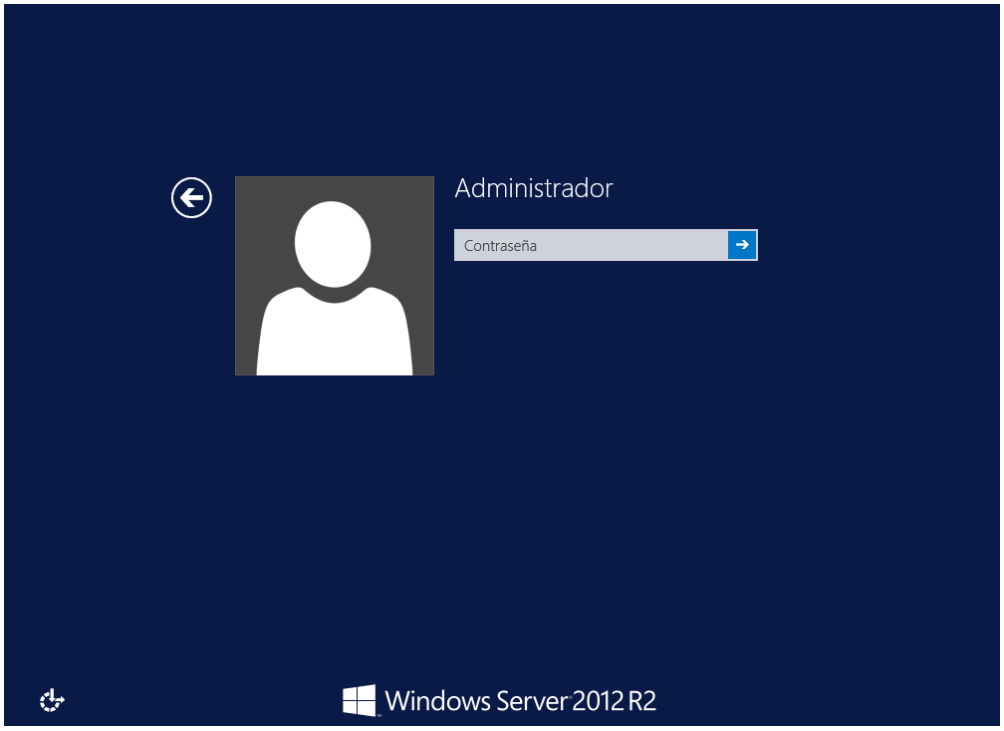

Figura 11. Finalización del proceso de instalación.

Por último, instalaremos las VMware Tools como muestra la Figura 12 para poder trabajar más cómodamente en cuanto a la visualización y volveremos a reiniciar.

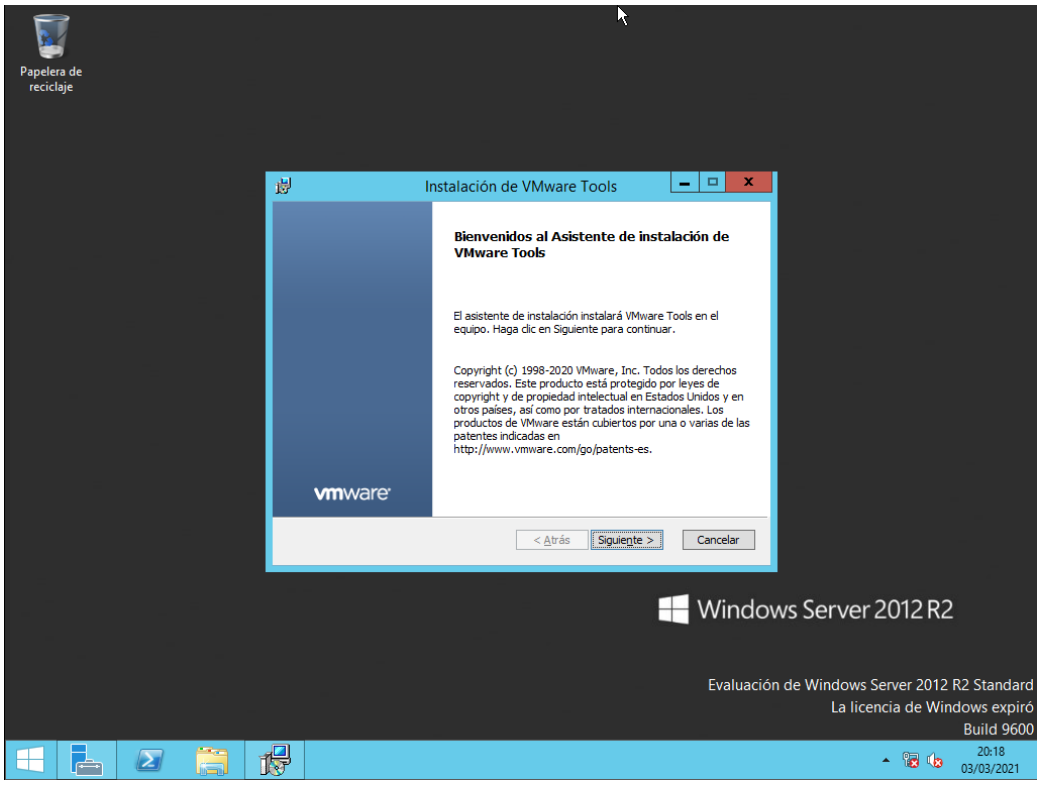

Figura 12. Instalación de WMware Tools.

6.1.2 Asignación de IP, máscara de red, DNS y nombre

Necesitamos asignar una IP fija, a nuestro Servidor y un nombre. Para ello, y según la Tabla 1, haremos los siguientes pasos.

HOST	RED LAN	PUERTA DE ENLACE	MASCARA	IP FIJA	DNS	1ª IP DHCP	Ultima IP DHCP
SerDCVallecas	192.168.2.0	192.168.2.1	255.255.255.0	192.168.2.2	192.168.2.2		
SerDCCoslada	192.168.3.0	192.168.3.1	255.255.255.0	192.168.3.2	192.168.3.2		
SerWEB	192.168.2.0	192.168.2.1	255.255.255.0	192.168.2.5	192.168.2.2		
SerOwncloud	192.168.2.0	192.168.2.1	255.255.255.0	192.168.2.10	192.168.2.2		
Windows10 Vallecas	192.168.2.0	192.168.2.1	255.255.255.0	DHCP MIKROTIK	192.168.2.2	192.168.2.50	192.168.2.254
Windows10 Coslada	192.168.3.0	192.168.3.1	255.255.255.0	DCHP MIKROTIK	192.168.3.2	192.168.3.50	192.168.3.254

Tabla 2. Direcciones de las máquinas a implementar (Fuente: propia).

Primeramente, para asignar la IP estática, accederemos al “Panel de Control” como vemos en la Figura 13 y haremos clic en “Redes e Internet”.

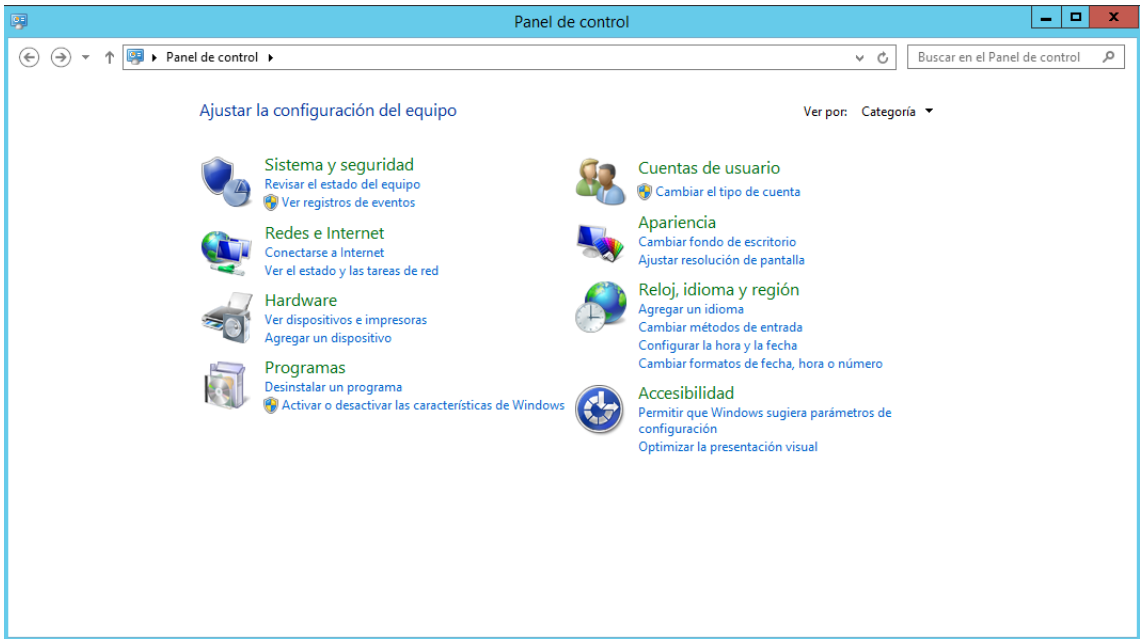

Figura 13. Pantalla del Panel de Control.

Una vez dentro como vemos en la Figura 14, iremos a “Centro de redes y recursos compartidos” y clicaremos en “Ethernet0”, que es nuestra conexión de la red visualizando una ventana similar a la de la Figura 15.

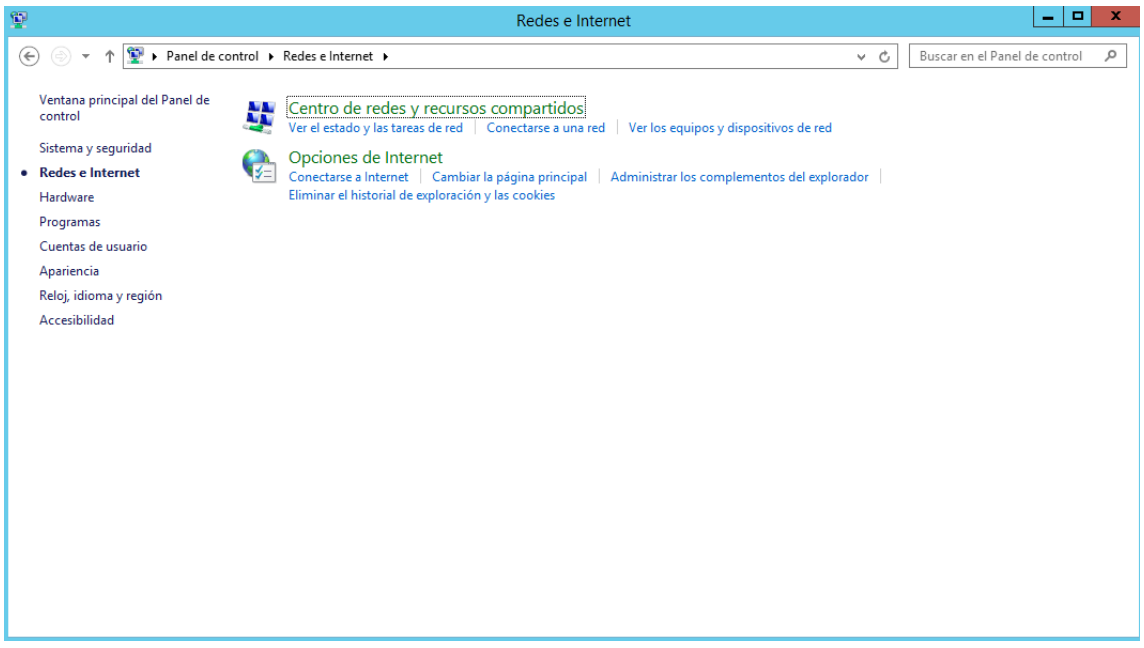

Figura 14. Pantalla de Redes e internet.

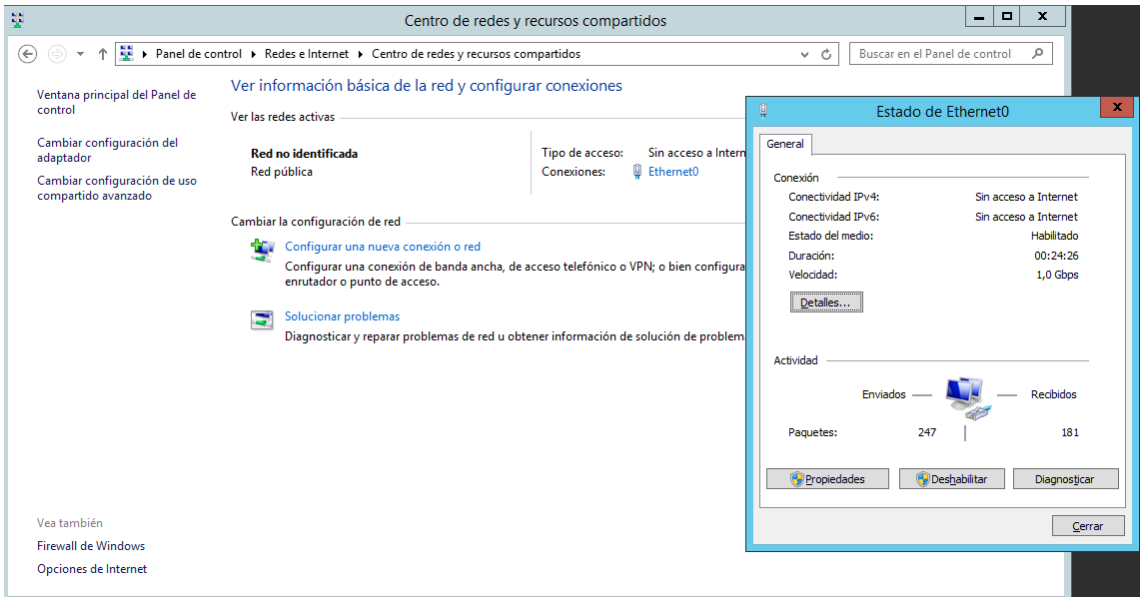

Figura 15. Estado de la red seleccionada.

Seguidamente, iremos a “Propiedades” como muestra la Figura 16 y seleccionaremos el “Protocolo de comunicación TCP/IPv4” que es en el que vamos a asignar nuestros datos introduciéndolos como en la Figura 17 y dando a aceptar.

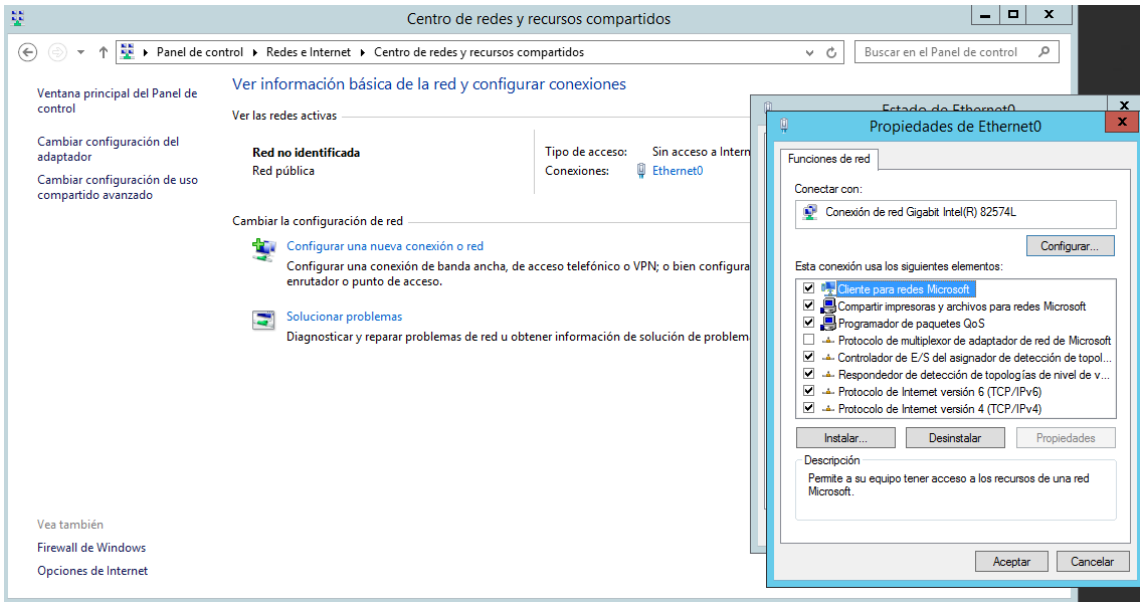

Figura 16. Propiedades de la red.

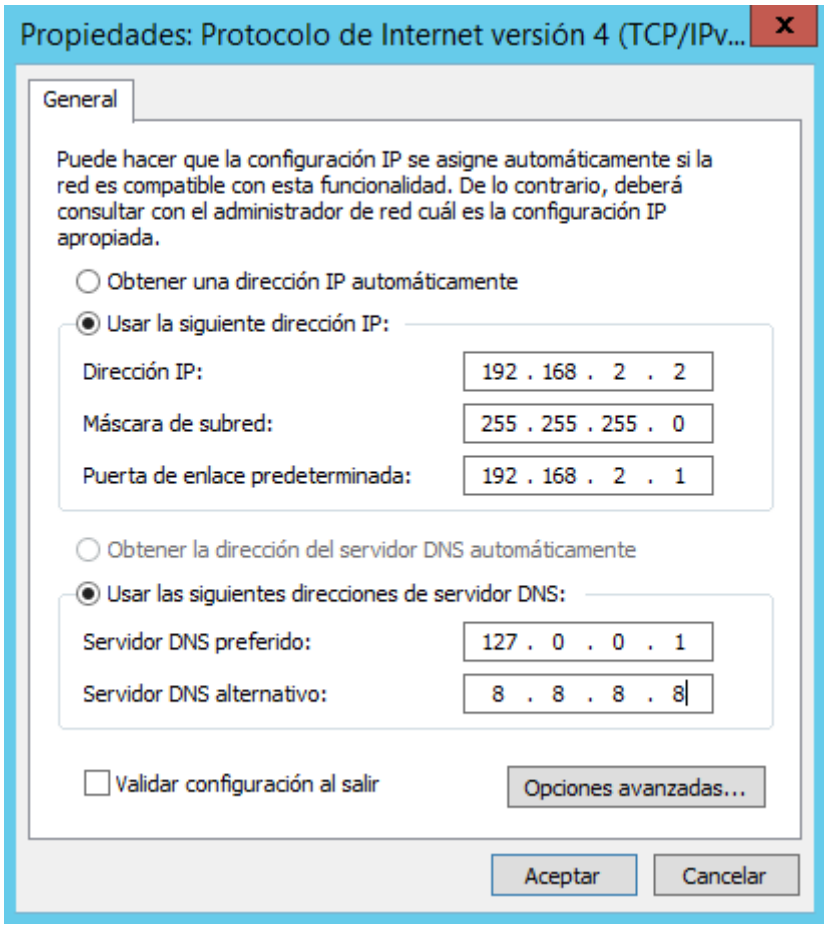

Figura 17. Configuración IP de la red

Cerramos el resto de pantallas.

Una vez asignado nuestro IP a cada servidor, le cambiaremos los nombres que están adjudicados por defecto.

En este caso iremos al “Panel de Control” y buscaremos “Sistema”, para posteriormente ir a “Cambiar configuración”.

Una vez allí en la pestaña “Nombre del equipo” como muestra la Figura 18 asignamos el nombre del equipo según la Tabla 2.

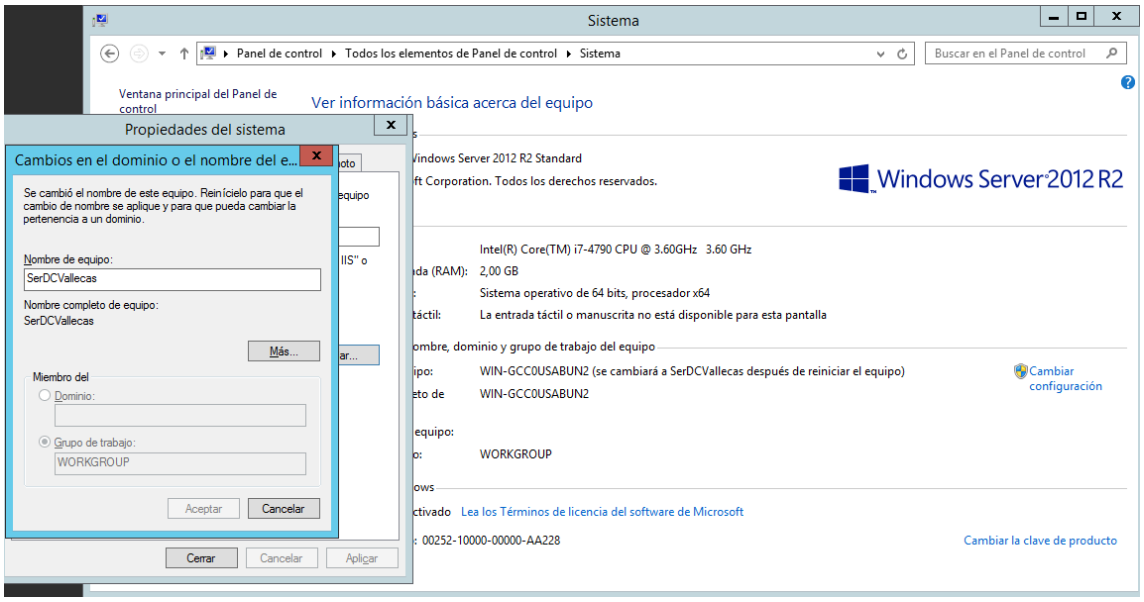

Figura 18. Asignación del nombre del equipo.

Nos solicitará reiniciar el equipo, el cual aceptaremos para que surjan efectivos los cambios que hemos realizado.

6.1.3 Creación del Dominio

En el siguiente punto vamos a centrarnos en la creación del dominio.

El dominio es donde vamos a agrupar a todos los equipos que conforman nuestra red para posteriormente gestionar todos los aspectos que tengan que ver con la seguridad, como crear usuarios, darles privilegios, etc.

Para crear el dominio, es necesario instalar el Active Directory. Es una herramienta de Windows Server que proporciona servicios de directorio en la red.

También será necesario instalar el servidor DNS, para poder responder a las consultas DNS de las máquinas que se encuentren en la red.

Primeramente, crearemos el servidor de dominio de Active Directory y el servidor DNS, que luego replicaremos en el otro servidor de la otra sede. Por así decirlo, será el primario.

Como vemos en la Figura 19, accedemos a “Administrar” y vamos a “Agregar roles y características”.

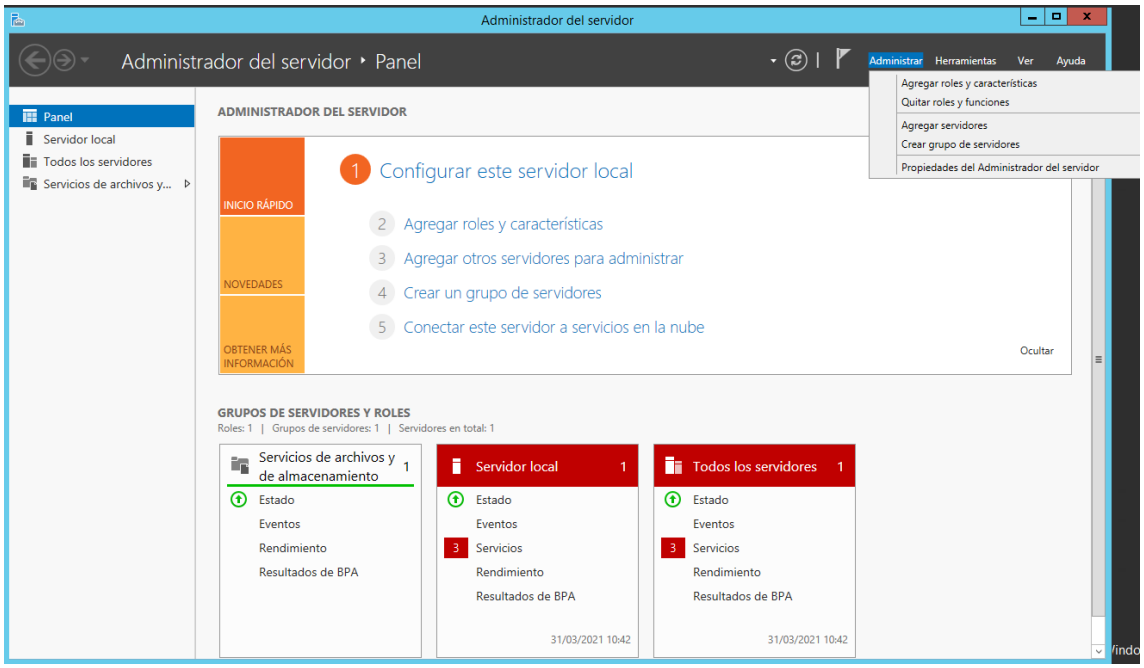

Figura 19. Pantalla principal del administrador del servidor.

Se nos desplegará una ventana de instalación, con dos opciones como muestra Figura 20. Elegiremos la “Instalación Basada en características o en roles” y daremos Siguiente.

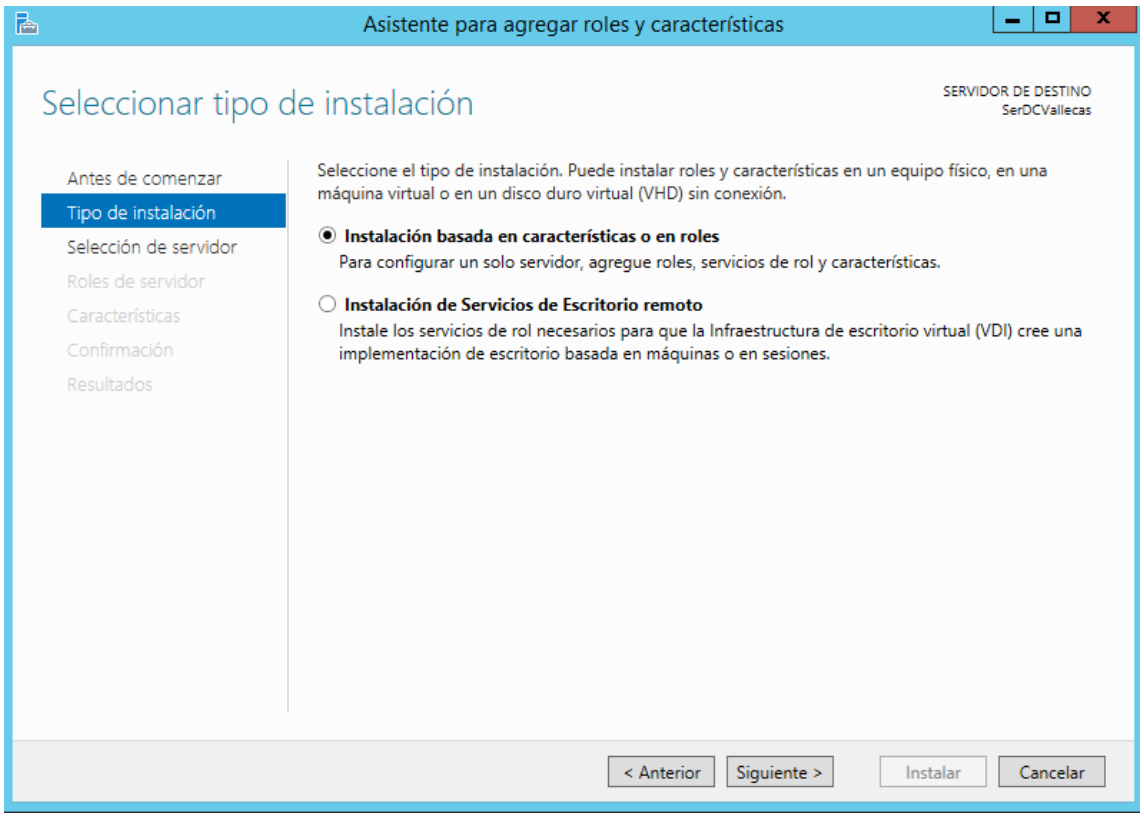

Figura 20. Asistente para agregar roles y características.

En la Figura 21, vemos que en la siguiente opción seleccionaremos el servidor. En nuestro caso el que aparece por defecto.

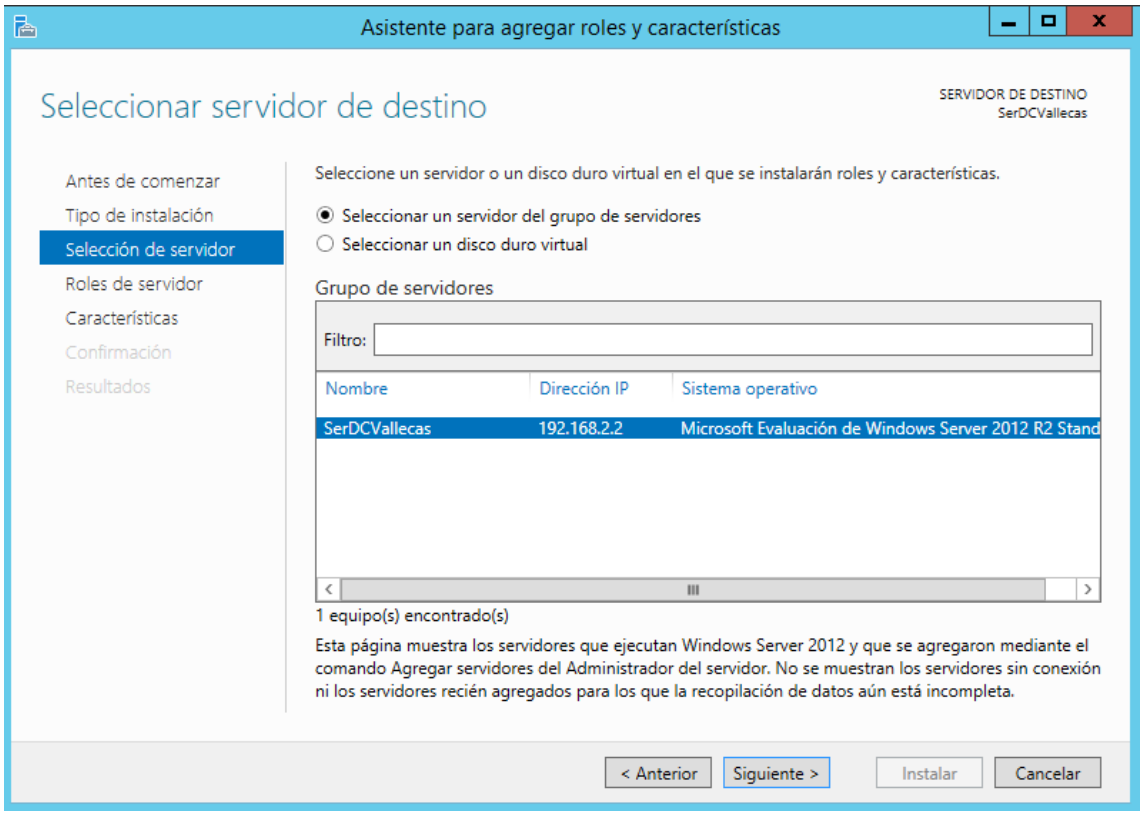

Figura 21. Selección del servidor.

Como vemos en la Figura 22, en la siguiente configuración seleccionaremos la opción de “Servicios de Dominio de Active Directory” y la opción de “Servidor DNS”. Para cada servicio que vamos a instalar agregaremos las características que nos indica el instalador.

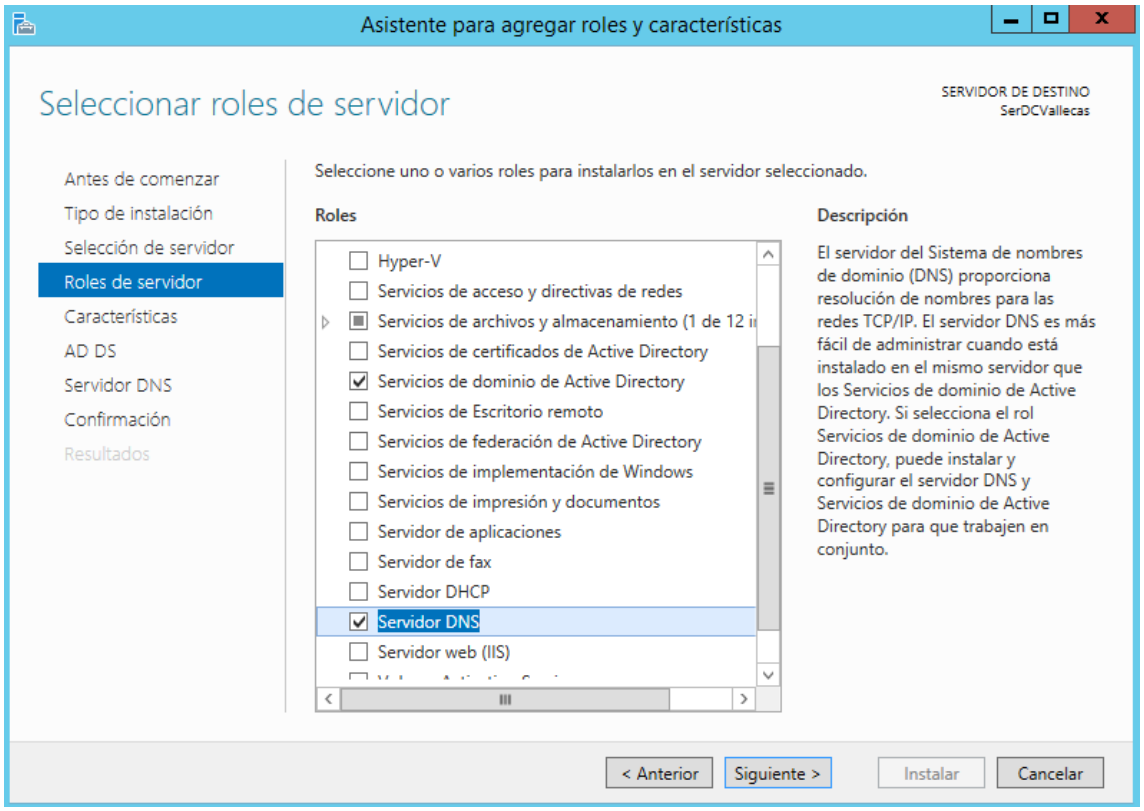

Figura 22. Selección de roles

A partir de este paso pulsaremos siguiente hasta la última ventana, como apreciamos en la Figura 23, donde instalaremos definitivamente los roles pulsando instalar.

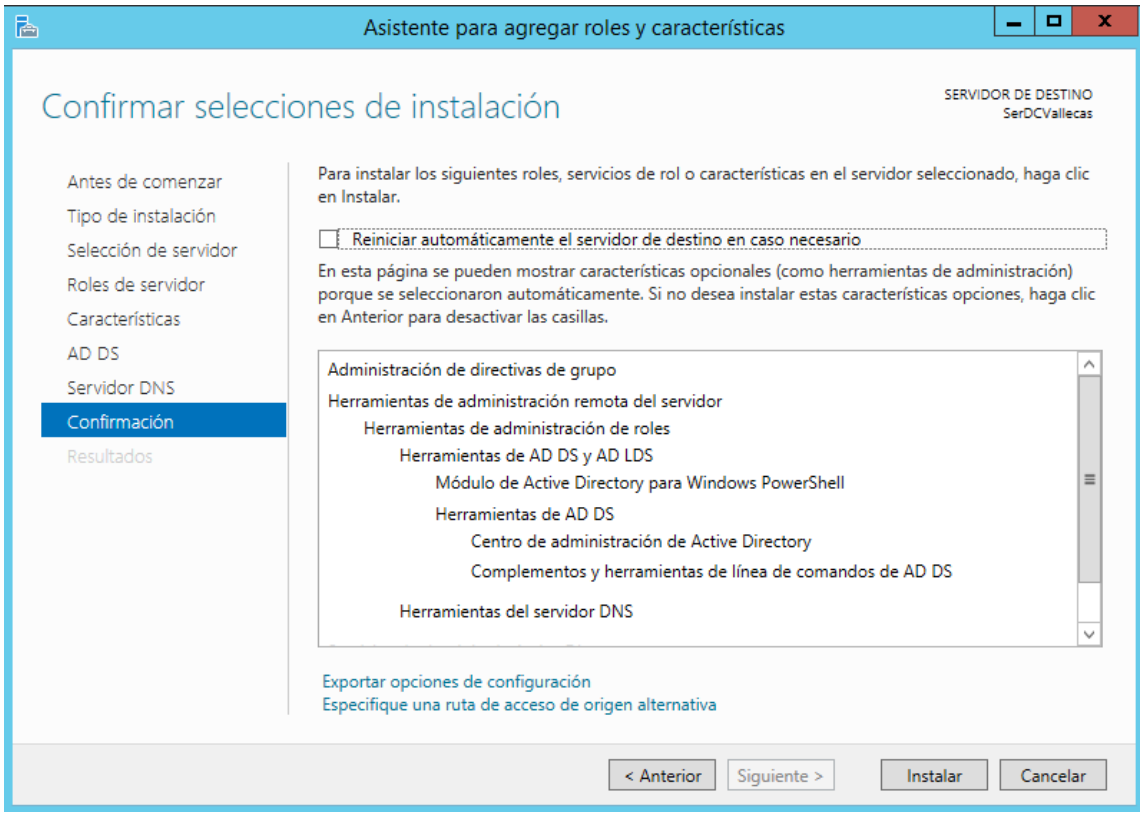

Figura 23. Resumen de las selecciones de instalación.

6.1.4 Promover a Controlador de dominio nuestro servidor

Para nuestro servidor llamado primario, se necesita que sea el controlador de dominio. Para ello, como apreciamos en la Figura 24, en la advertencia que sale con un triángulo amarillo con exclamación y pichando en él, veremos la opción de “Promover este servidor a controlador de dominio”.

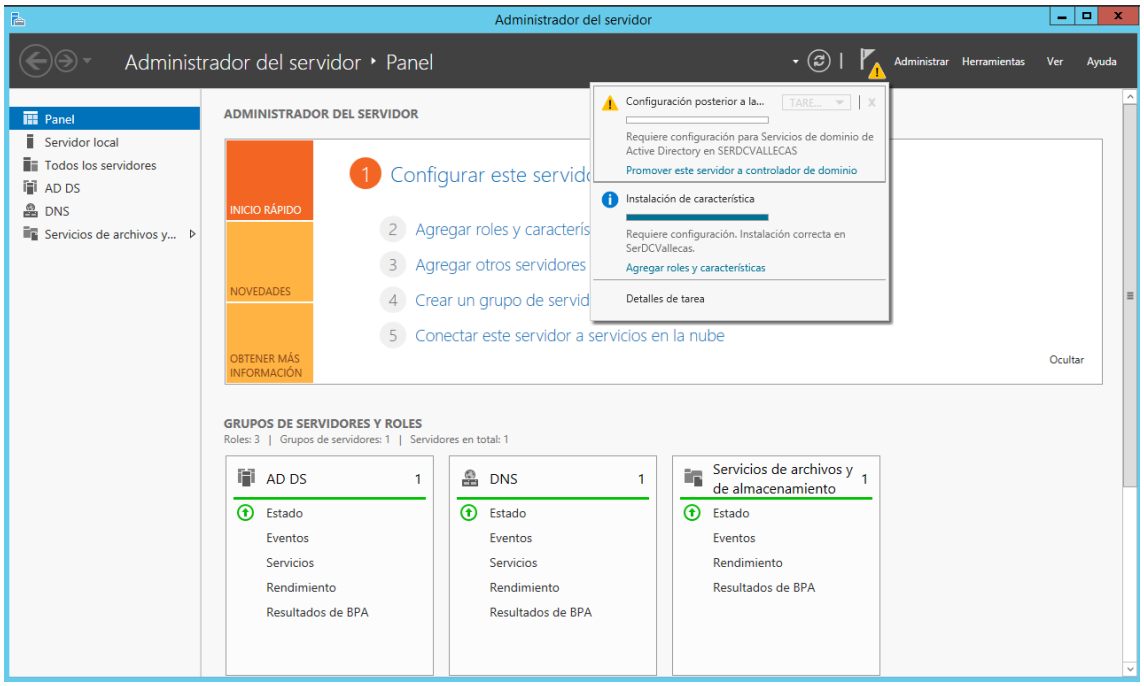

Figura 24. Promover a controlador de dominio.

En la Figura 25Figura 24 podemos ver cómo se nos despliega una ventana en el que nos da varias opciones de implementación. Al ser el primario, tendremos que crear un nuevo bosque, al que le daremos por nombre “gym.local”.

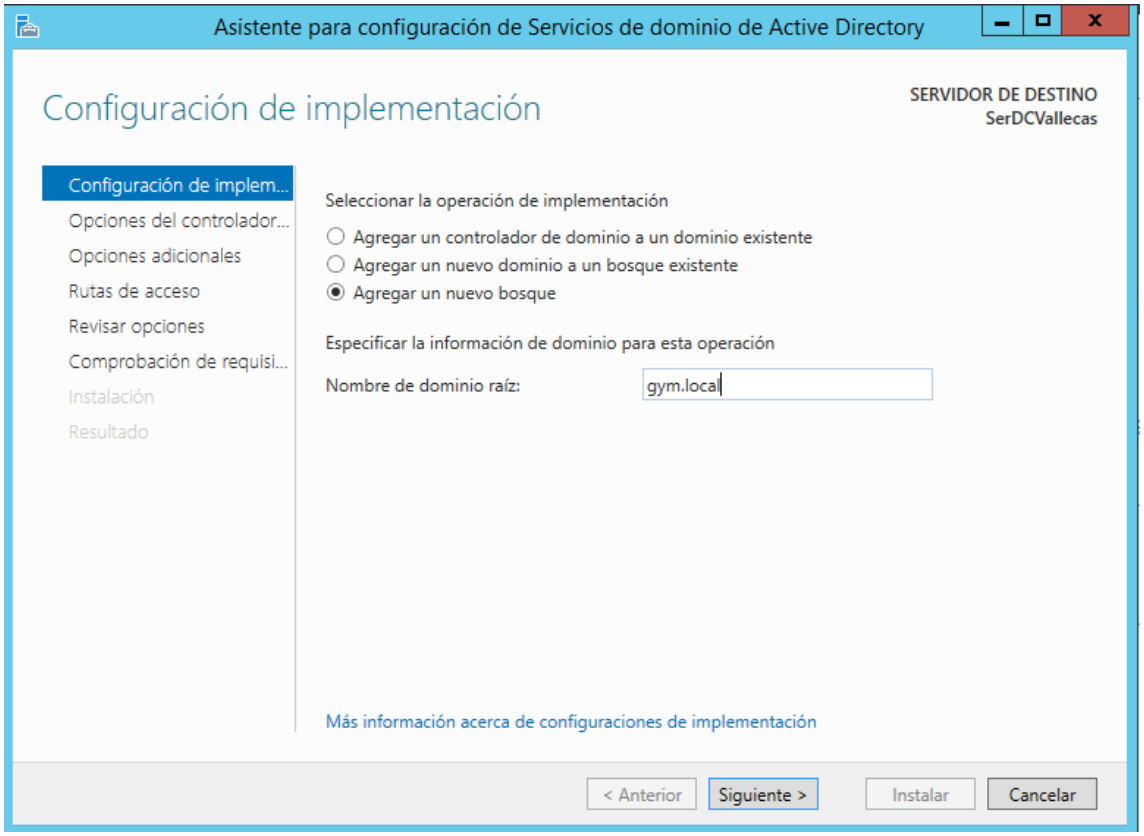

Figura 25. Creación del nuevo bosque.

Al pulsar siguiente necesitaremos dar una contraseña al administrador global del dominio. Una vez introducida esa contraseña, al hacer clic en siguiente, nos saldrá una advertencia que obviaremos.

Seguidamente, se mostrará el nombre de la NetBIOS como muestra la Figura 26,Figura 25 que dejaremos como está pulsando siguiente.

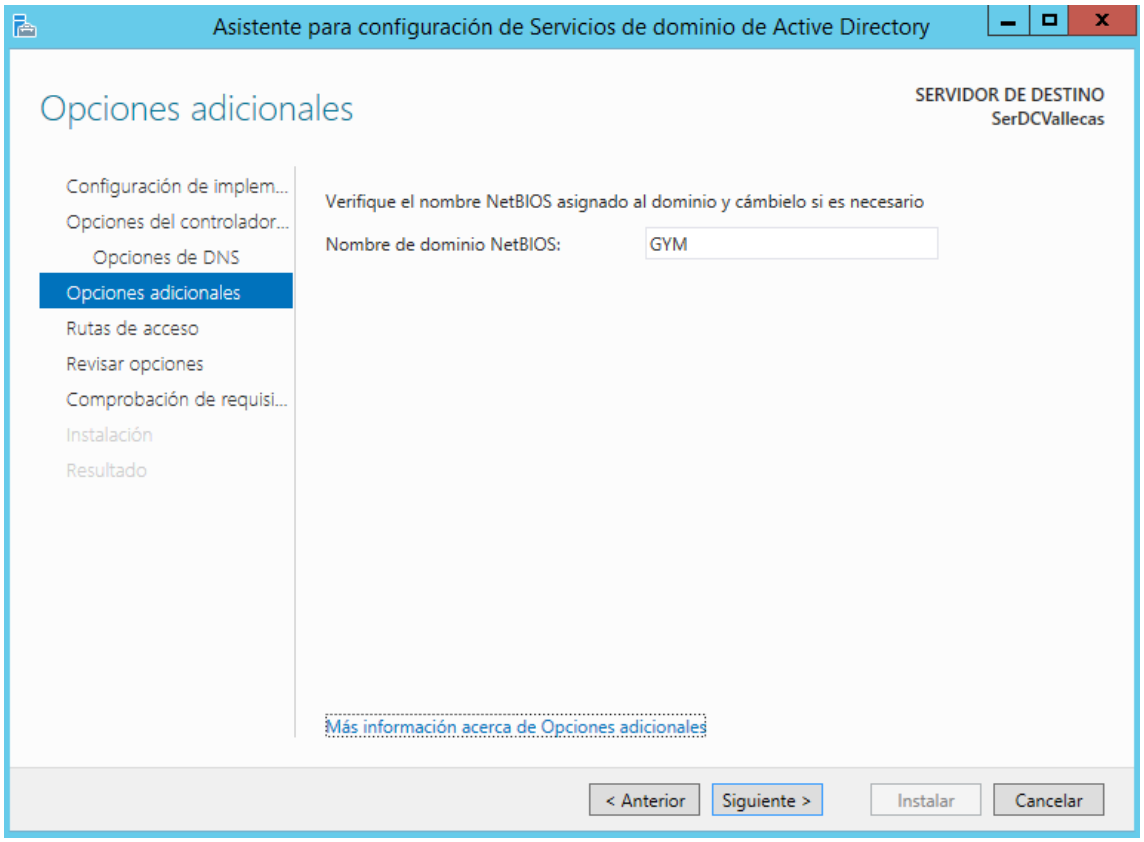

Figura 26. Nombre de dominio NetBIOS.

Como en la Figura 27, se mostrarán opciones en la pestaña de “Rutas de acceso” a la que no haremos cambios, dando a siguiente.

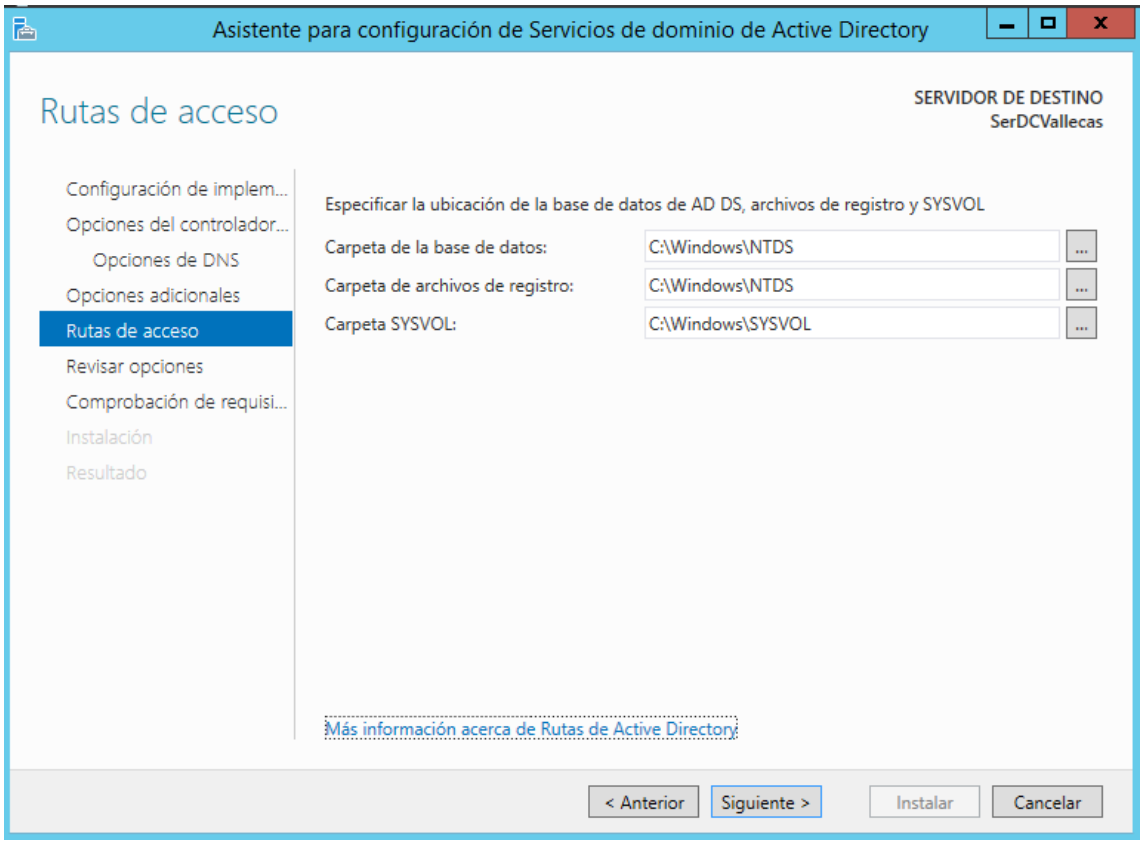

Figura 27. Ubicaciones para la ruta de acceso.

Nos mostrará una ventana como en la Figura 28. Se trata de un resumen de las opciones que hemos elegido para la configuración. Pulsaremos siguiente.

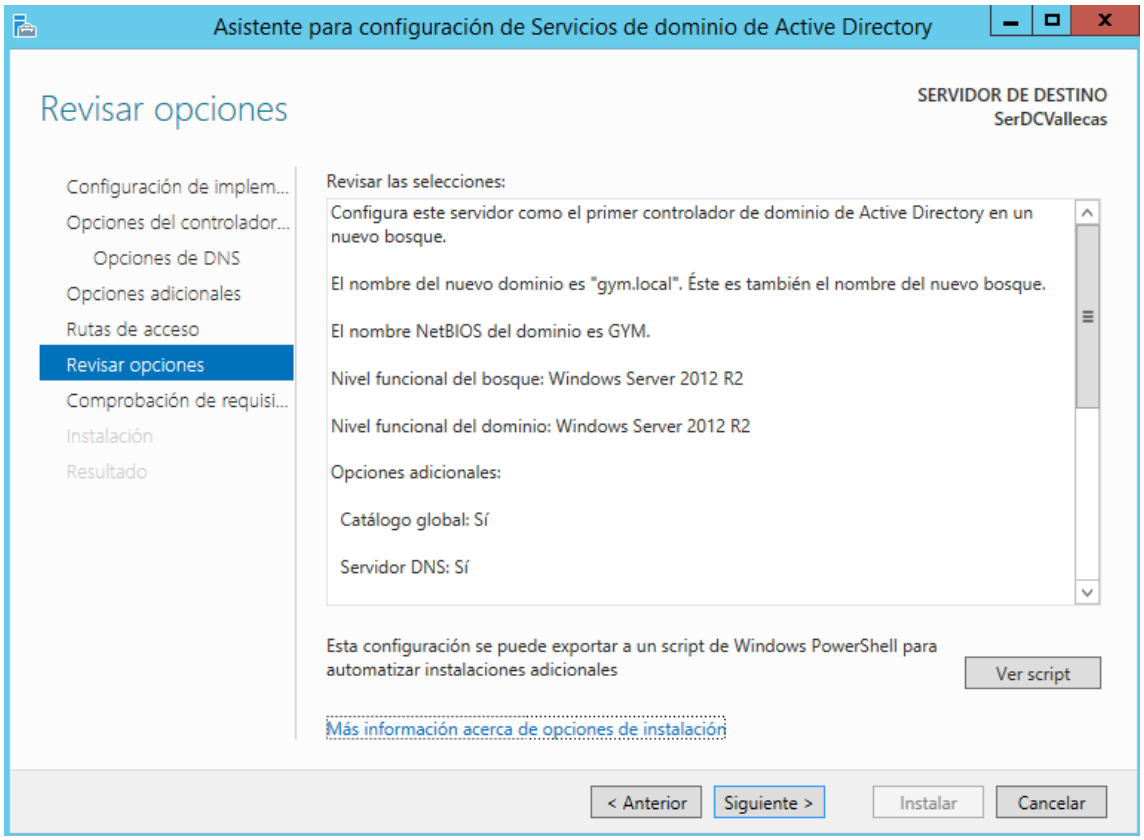

Figura 28. Resumen de las opciones.

Se comprobará que se los requisitos se cumplen para la configuración que hemos elegido, pudiendo mostrar alguna advertencia como vemos en la Figura 29, pero permitiendo continuar clicando la opción de instalar.

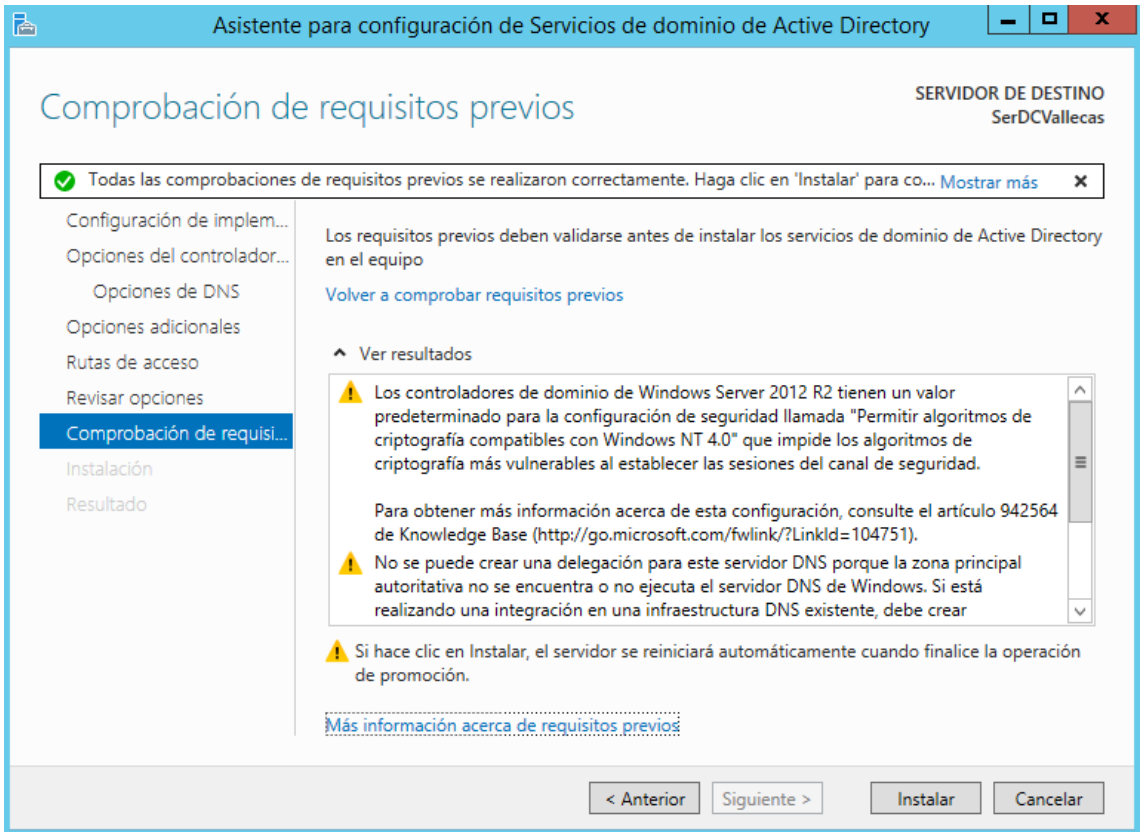

Figura 29. Comprobación de requisitos.

Comenzará el proceso de instalación y cuando concluya será necesario reiniciar.

Una vez reiniciado, ya tendremos creado nuestro controlador de dominio, mostrando el administrador por defecto al arrancar como muestra la Figura 30.

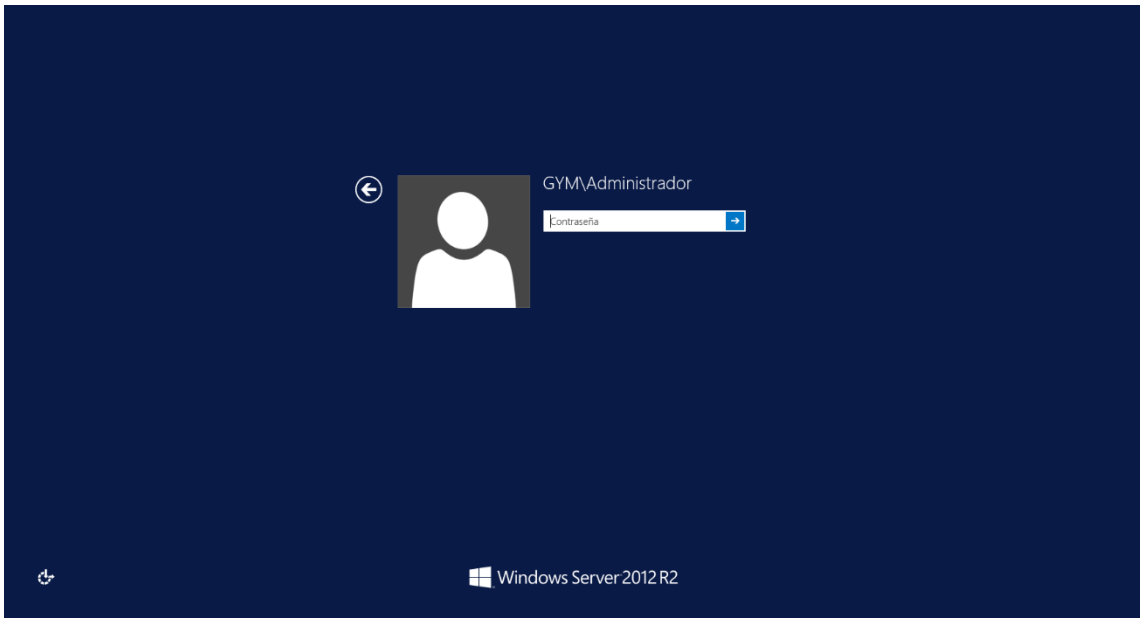

Figura 30. Usuario administrador al reiniciar.

Una vez creado nuestro dominio lo que haremos será crear una zona inversa para resolver nombres.

Para ello nos vamos a Herramientas-> DNS mostrándose una pestaña como la Figura 31.

Una vez dentro de DNS lo que haremos será hacer click en el botón derecho en zona inversa y seleccionaremos Zona Nueva.

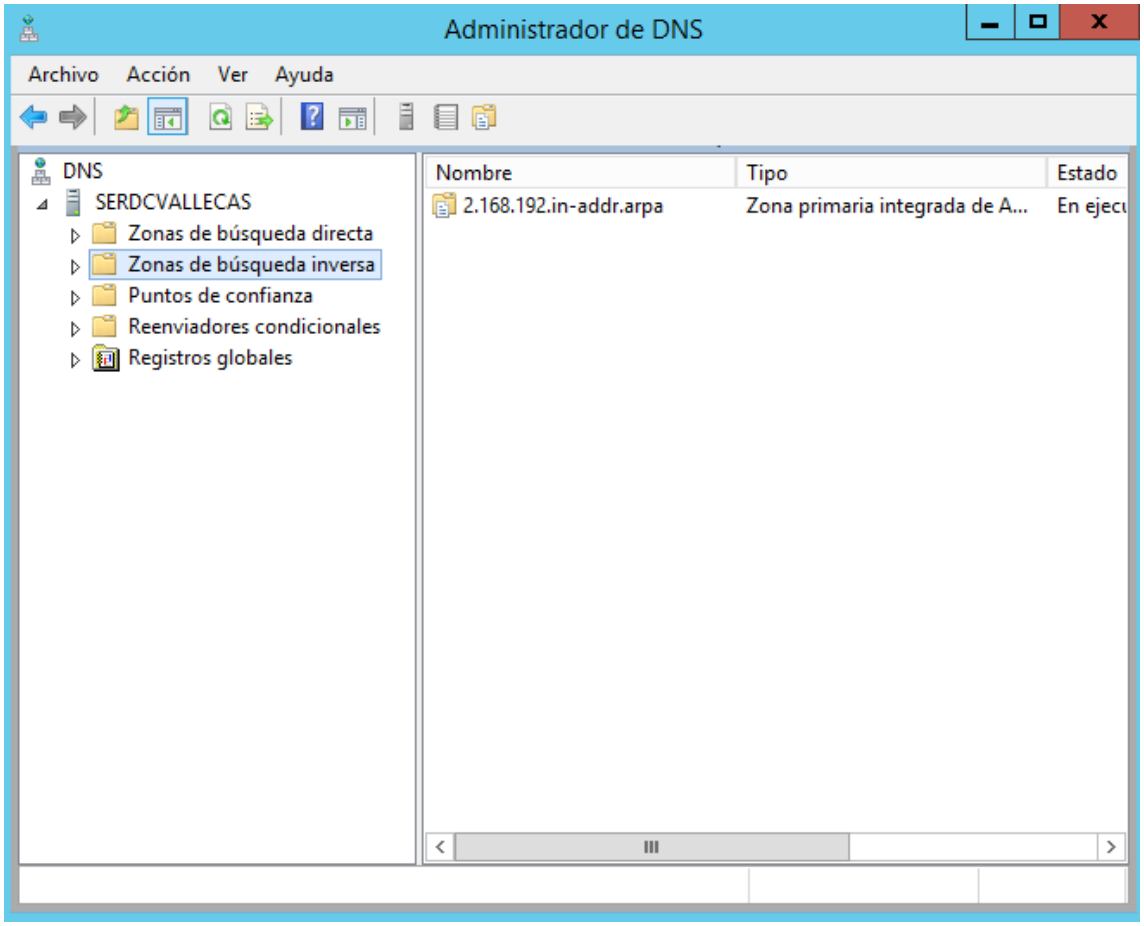

Figura 31. Zonas de búsqueda inversa.

Pulsaremos siguiente hasta que el asistente nos solicite la Id de la red, que pondremos la de nuestra lan correspondiente de cada sede, como vemos en la Figura 32 para la de Vallecas.

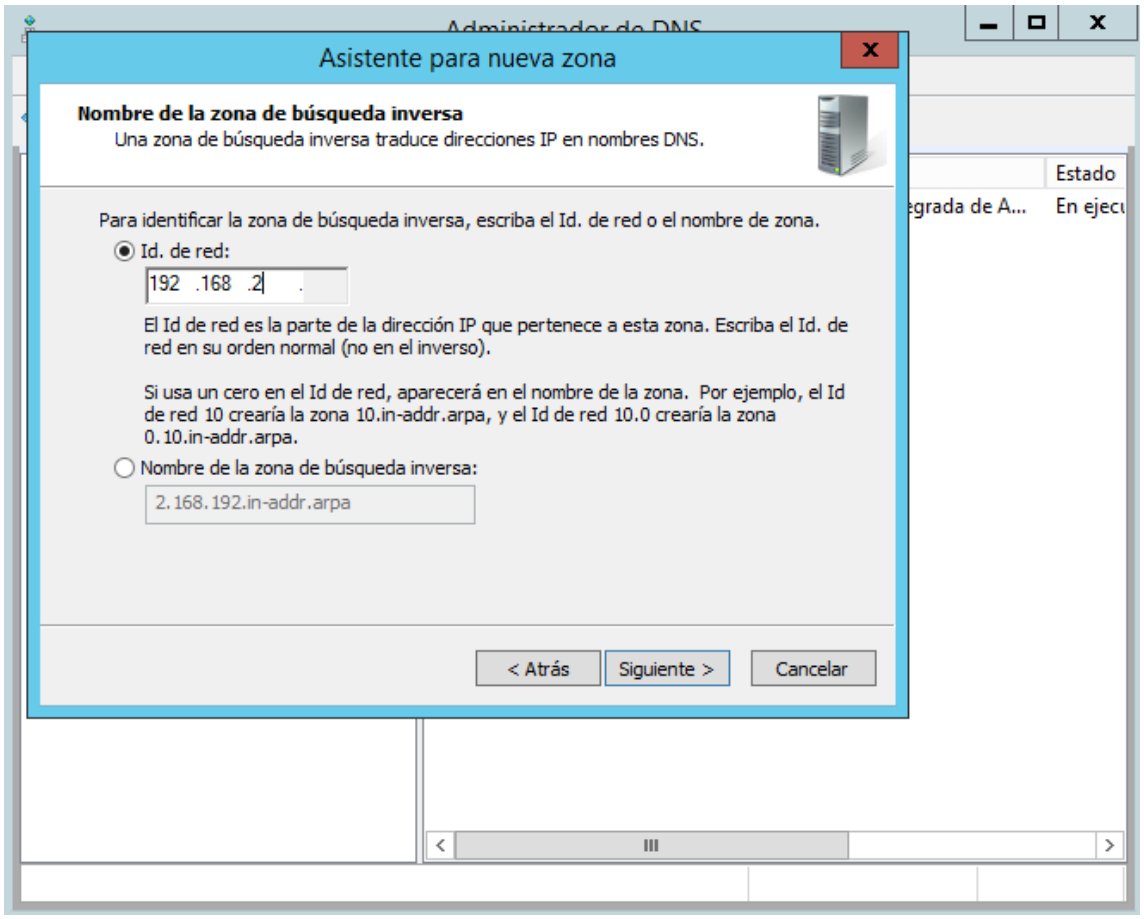

Figura 32. Creación de nueva zona inversa.

Le daremos siguiente hasta finalizar.

Por último, en gym.local en la zona de búsqueda directa pulsaremos el botón derecho del ratón en nuestro servidor y buscaremos en propiedades.

Seleccionaremos actualizar el PTR para finalizar quedando la configuración como la mostrada en la Figura 33.

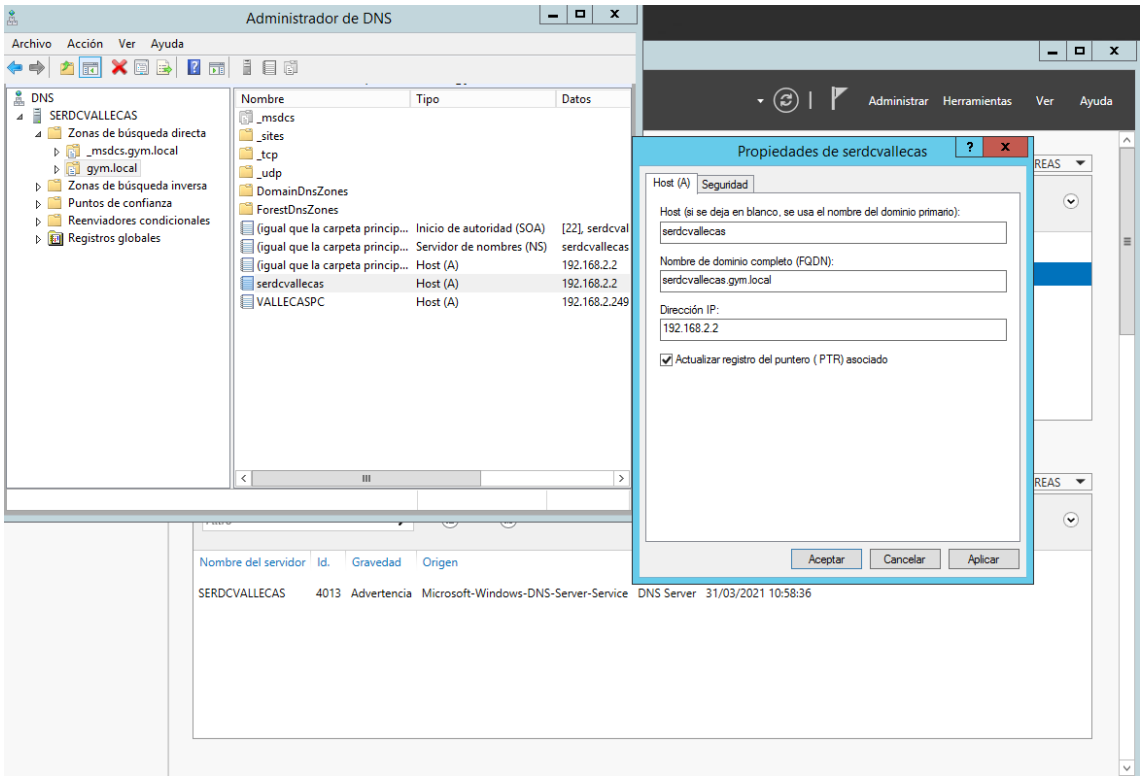

Figura 33. Actualización del puntero PTR.

6.1.5 Añadir los equipos al dominio

Es importante que para que todo funcione correctamente, todos los equipos que conforman la red pertenezcan al mismo dominio.

Así de forma que, cuando un usuario se identifique con su nombre y su contraseña, el controlador del dominio será quien valide o no el acceso.

Para añadir al dominio a los clientes de cada sede tenemos que hacer lo siguiente.

Dentro de cada cliente nos dirigimos al Panel de Control, Sistema y cambiar el nombre de este equipo (avanzado) como apreciamos en la Figura 34.

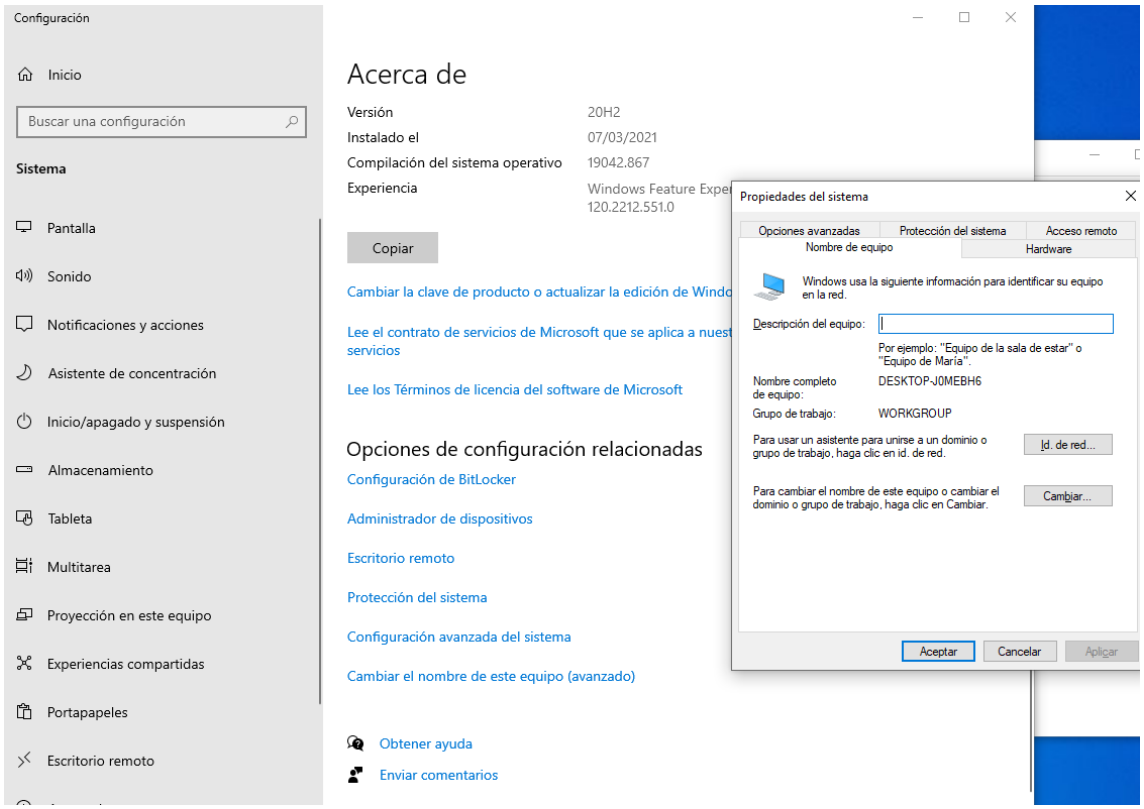

Figura 34. Cambiar el nombre del equipo.

Pulsaremos la opción Cambiar, pondremos el nombre del equipo y el dominio al que queremos pertenecer. Nos solicitará el usuario y la contraseña del administrador como muestra la Figura 35.

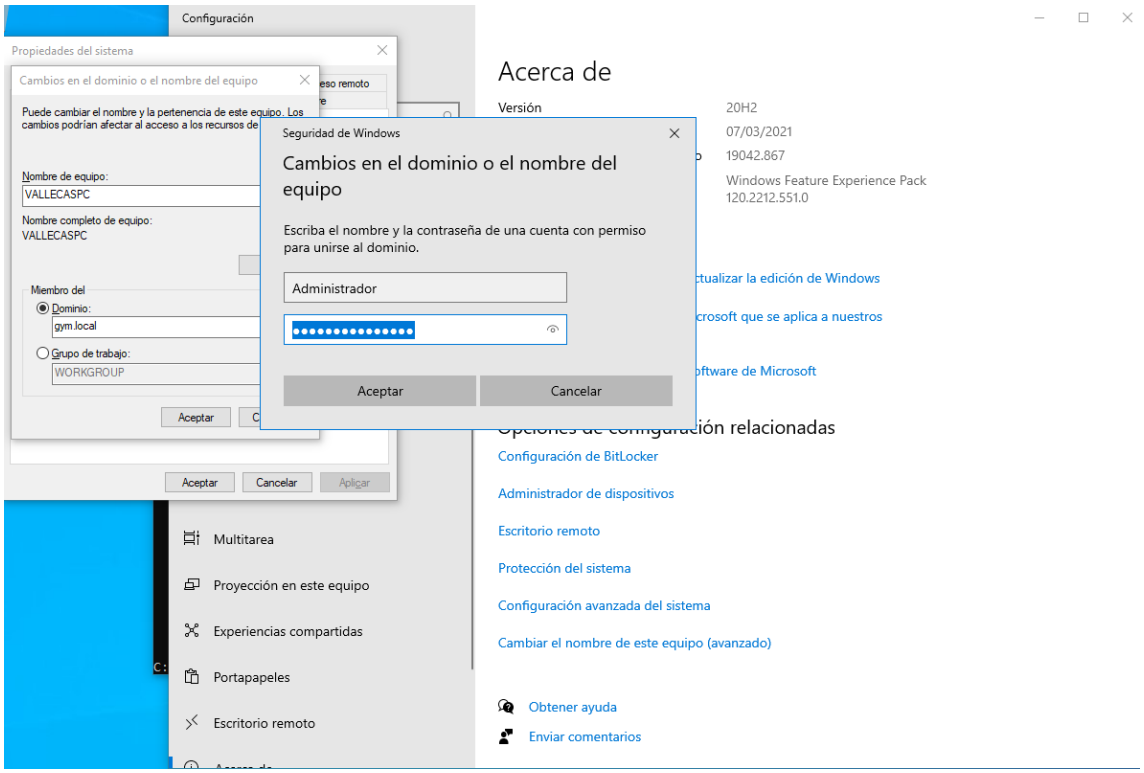

Figura 35. Solicitud de credenciales de administrador.

Por último se reiniciará el equipo para aplicar las configuraciones.

6.2 Instalación y configuración de Routers Mikrotik

En el siguiente apartado vamos a utilizar los Routers de la compañía Mikrotik.

Como se describe en el blog de Citelia [6], el principal motivo de utilizar estos routers o es la gran relación calidad/precio. Productos profesionales a bajos precios si lo comparas con otras marcas.

Con estos routers pretendemos dotar a nuestro sistema de seguridad gracias al firewall que lleva integrado, filtrando paquetes para administrar el flujo de datos que pasa por él.

Este hardware, acompañado del soporte software, nos va a permitir crear una conexión entre las sedes a través de una VPN. De esta forma podemos disponer de todos los recursos, aunque los equipos no se encuentren físicamente juntos, que es nuestro principal escollo para la comunicación.

También nos permitirá gestionar cada red Lan, asignando direcciones a los equipos que se encuentren dentro de la red y sus tiempos dentro de ellas.

A continuación se pasa a describir su instalación y configuración para nuestras necesidades.

6.2.1 DHCP y FIREWALL.

Nuestro Mikrotik de cada sede será nuestro servidor DHCP, que será el encargado de asignar automáticamente las direcciones IPs, puertas de enlace, así como otros parámetros de red que necesitemos en cada sede.

La forma de configuración será válida para ambas sedes, pero teniendo en cuenta que cada sede tendrá rangos de IPs y DNS distintas debido a que son redes Lan diferentes.

Para ello lo vamos a configurar de la siguiente forma:

Lo primero será descargarnos de la página del fabricante (https://mikrotik.com/download) el fichero VMDK la versión stable de Cloud Hoster Router más reciente para añadir la máquina virtual a nuestro VMWare.

Una vez añadida, descargamos también en la web del fabricante el programa de gestión Winbox para configurarlo.

Para configurarlo tiene que ser visible en nuestra red, por lo que tendrá un adaptador de red en modo bridge en VMWare. También conectaremos un adaptador de red para estar conectado a la red Lan de cada sede como se indica en la figura IPS

Una vez visible abrimos el programa de gestión y en la ventana Neighbors marcamos la dirección MAC y conectamos con nuestro Mikrotik. Por defecto el login será admin y la contraseña estará vacía.

Lo primero que haremos será asignar en la pestaña Quick Set una Ip estática, la máscara de red y la puerta de enlace para nuestro router, según corresponda a nuestra sede guiándonos por la Tabla 3.

ROUTER	RED LAN	IP RED LAN	MASCARA	RED WAN	IP RED WAN	VLAN
MIKROTIC Vallecas	192.168.2.0	192.168.2.1	255.255.255.0	192.168.1.0	192.168.1.100	192.168.4.1
MIKROTIC Coslada	192.168.3.0	192.168.3.1	255.255.255.0	192.168.1.0	192.168.1.101	192.168.4.2

Tabla 3. Direcciones de Routers Mikrotik (Fuente: propia).

Además daremos la dirección de nuestro router para nuestra lan, tal y como muestra la Figura 36.

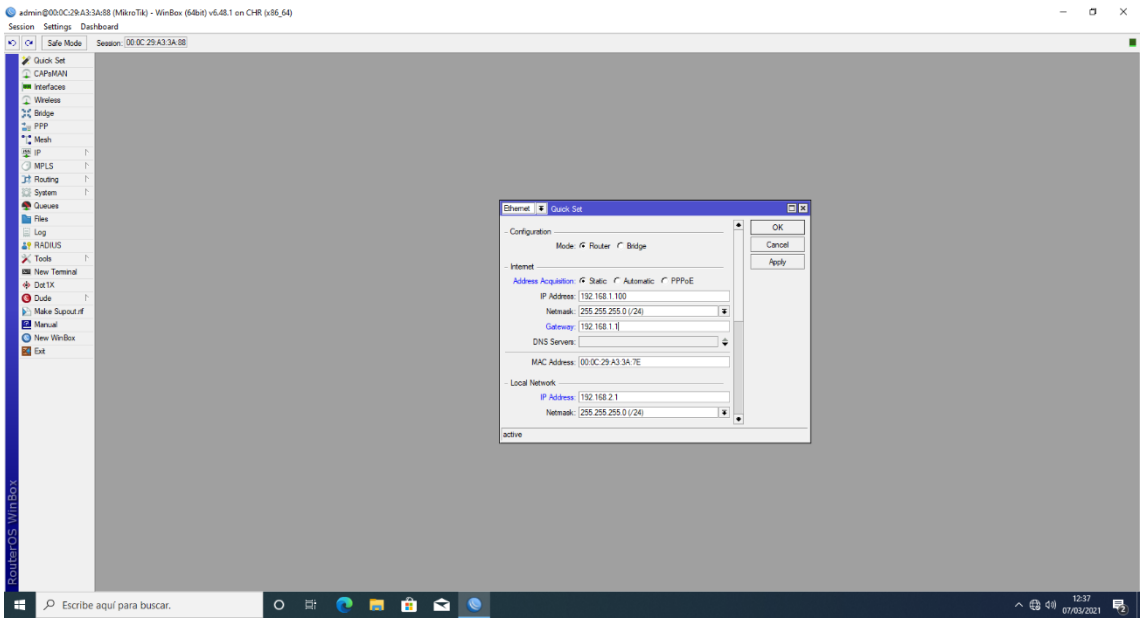

Figura 36. Configuración Quick Set en Mikrotik.

Además, pondremos un nombre a cada los router para diferenciarlos quedando como en la Figura 37 para el Mikrotik de Vallecas.

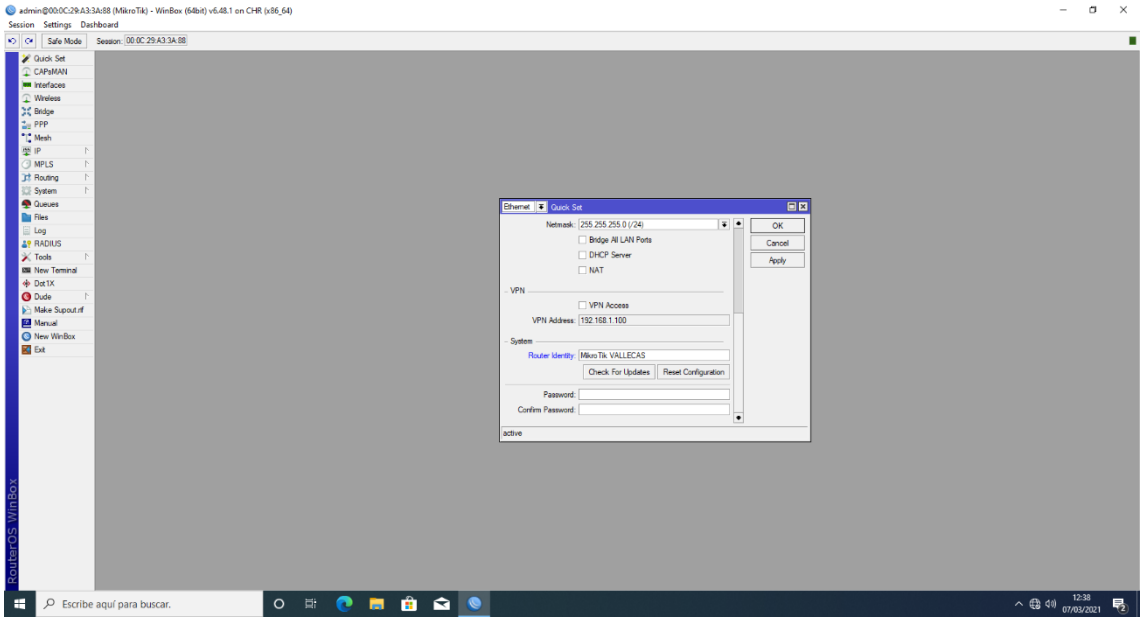

Figura 37. Asignación de nombre a Router Mikrotik.

Lo siguiente será nombrar a cada red para diferenciarlas en posibles configuraciones futuras. Para ellos nos situaremos en interfaces y nombraremos las dos redes según corresponda.

Para la red externa será wan como muestra la Figura 38.

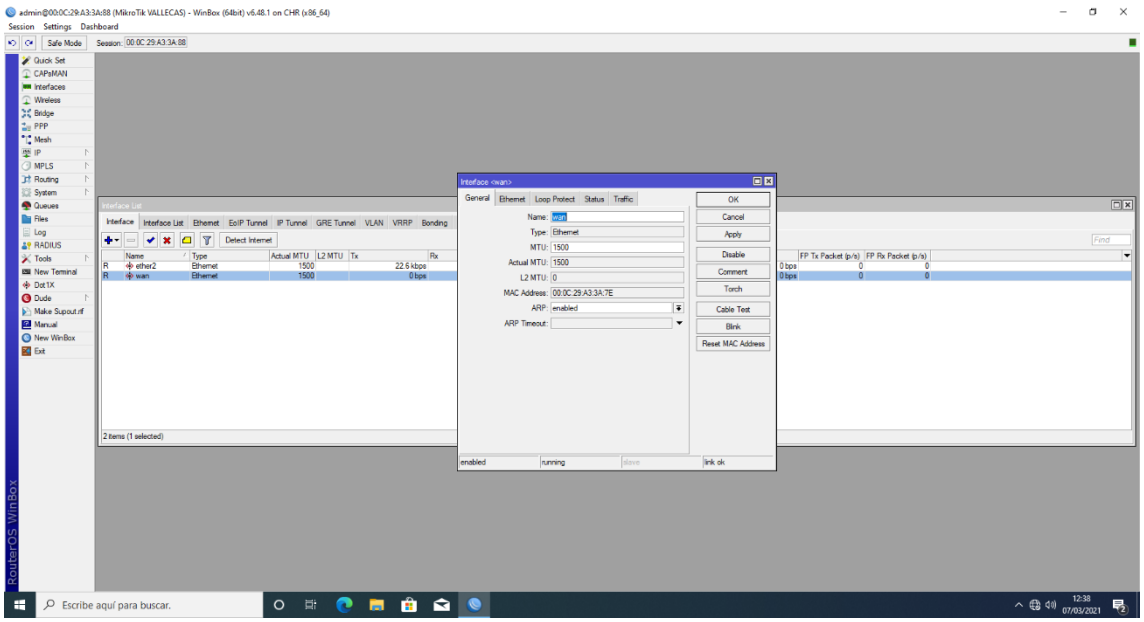

Figura 38. Asignación de nombre a la red wan.

Y para la red interna será lan según corresponda por la sede. Para el Mikrotik de Vallecas quedaría como en la Figura 39.

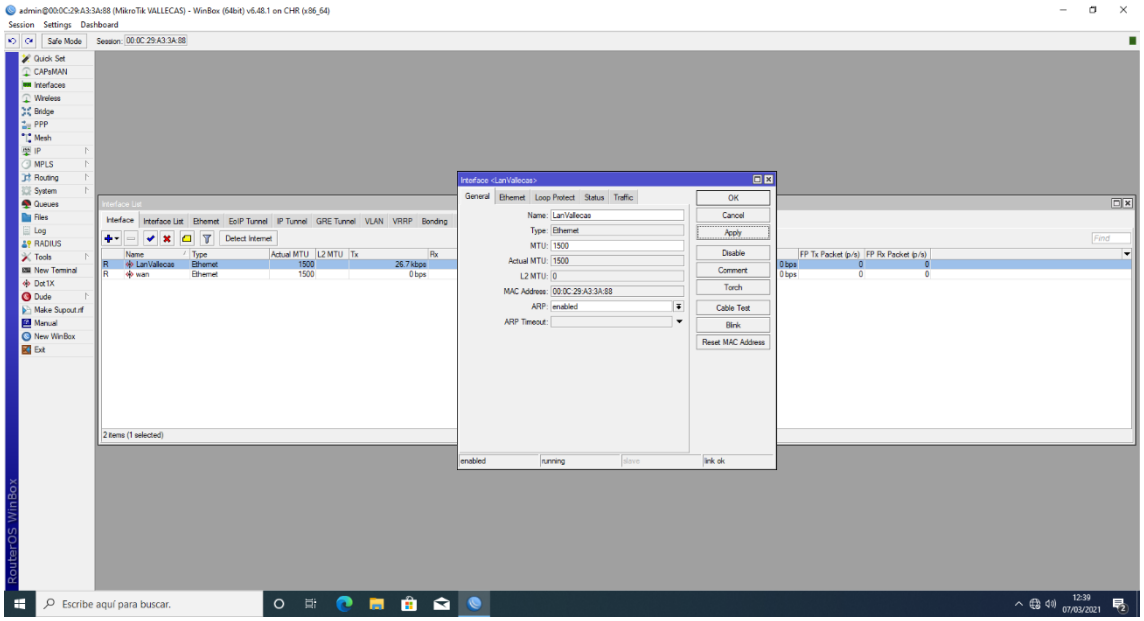

Figura 39. Asignación de nombre a la red lan.

Por si en Quick Set no se hubiera configurado bien la dirección del Mikrotik en la cada sede, accedemos a Ip->Addresses y añadimos la dirección Ip del Mikrotik que ocupará en cada red, como en la Figura 40.

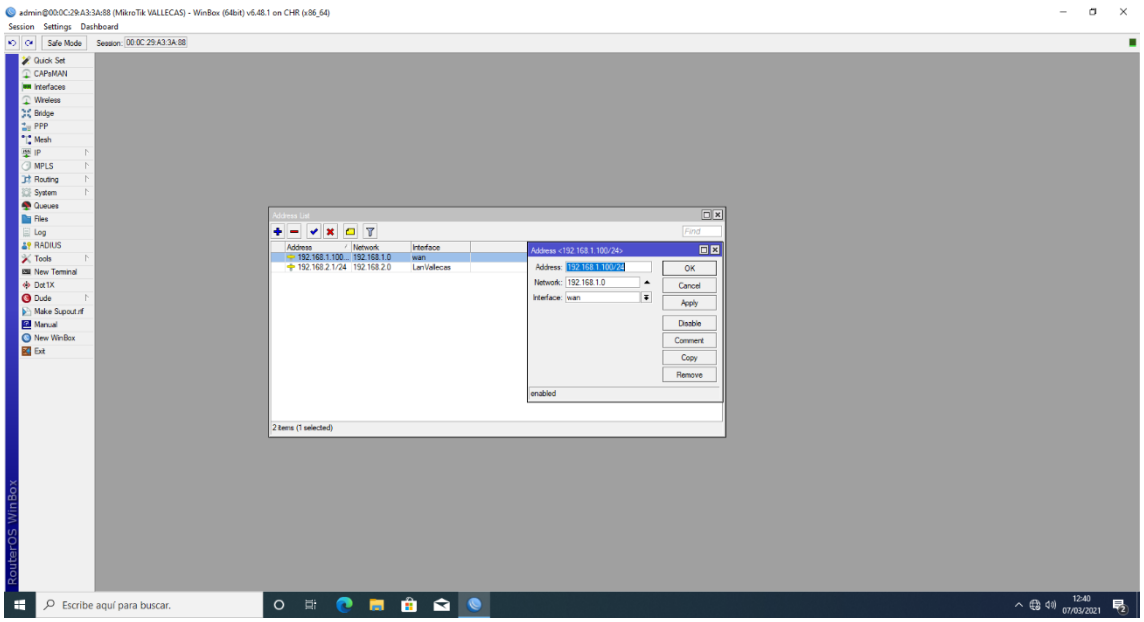

Figura 40. Asignación de IP del Mikrotik.

El siguiente paso será dar salida a internet desde la lan configurando las reglas en el firewall.

Para ello vamos a IP->Firewall y en la pestaña NAT le damos a +.

En la nueva ventana, como vemos en la Figura 41, en la pestaña general, seleccionaremos srcnat en chain .

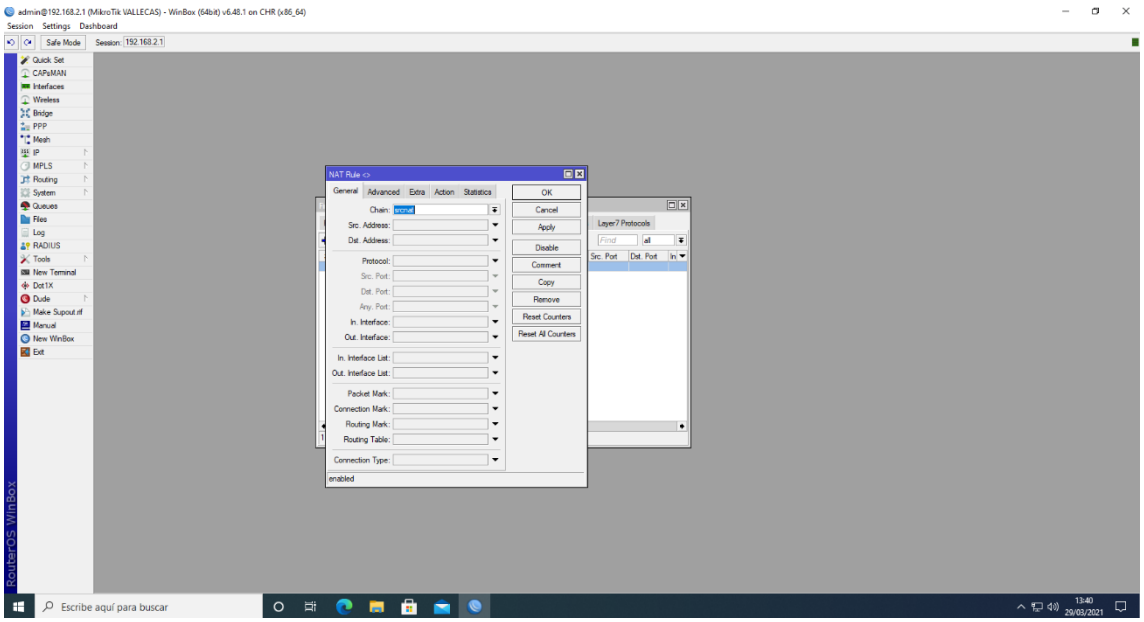

Figura 41. Creación de regla de firewall.

Y en la pestaña Action, como en la Figura 42, seleccionaremos masquerade.

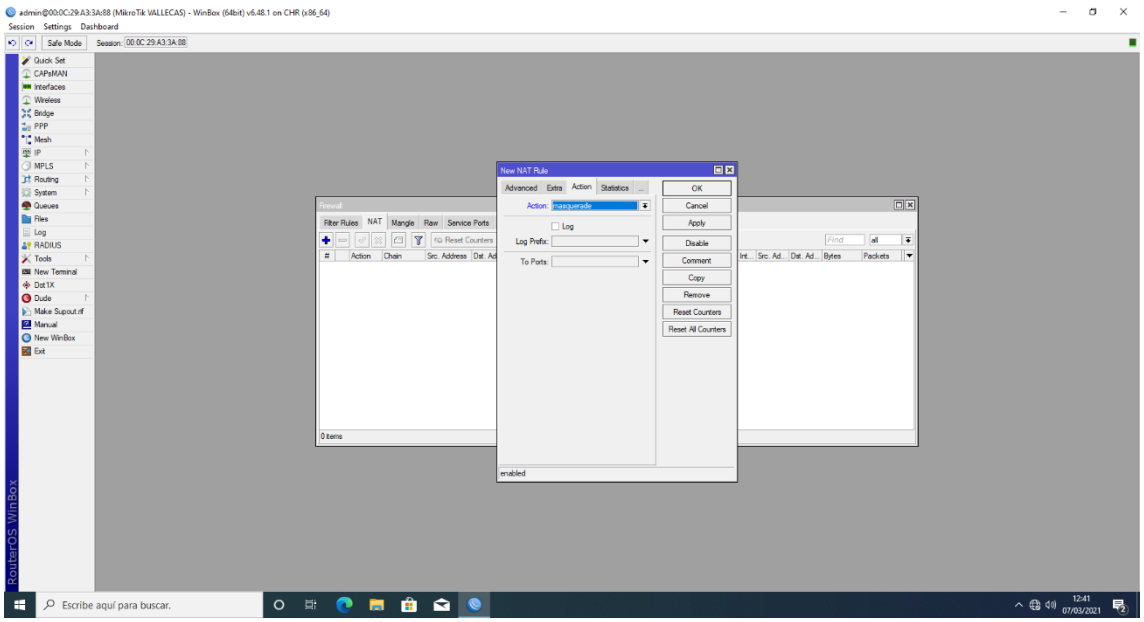

Figura 42. Selección de masquerade.

Una vez configurados estos parámetros, vamos a configurar el servidor DHCP.

Iremos al apartado IP->DHCP Server.

En la ventana que se despliega daremos a DHCP Setup para introducir los parámetros.

Como vemos en la Figura 43, primeramente nos solicita la interface en la que queremos que actúe, que en nuestro caso será la lan que corresponda según la sede.

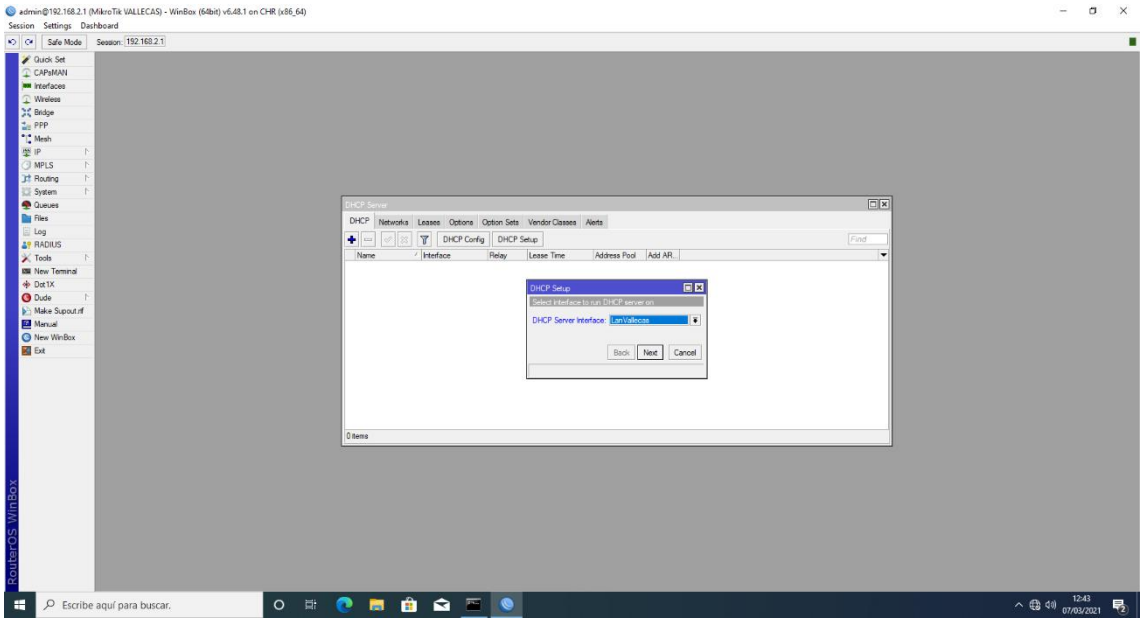

Figura 43. Selección de interface.

El siguiente punto será introducir la dirección de la red y la máscara en la que queremos que actúe, como la mostrada en la Figura 44.

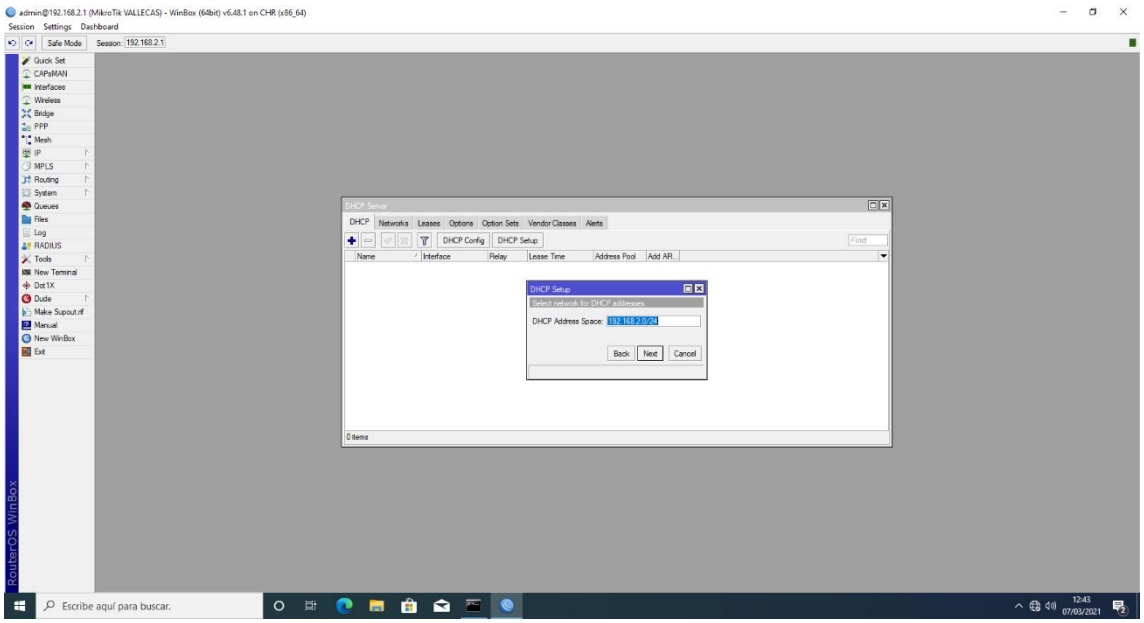

Figura 44.Introducción de dirección y máscara de la red.

En la Figura 45, vemos que en el siguiente paso nos solicita la puerta de enlace que asignará.

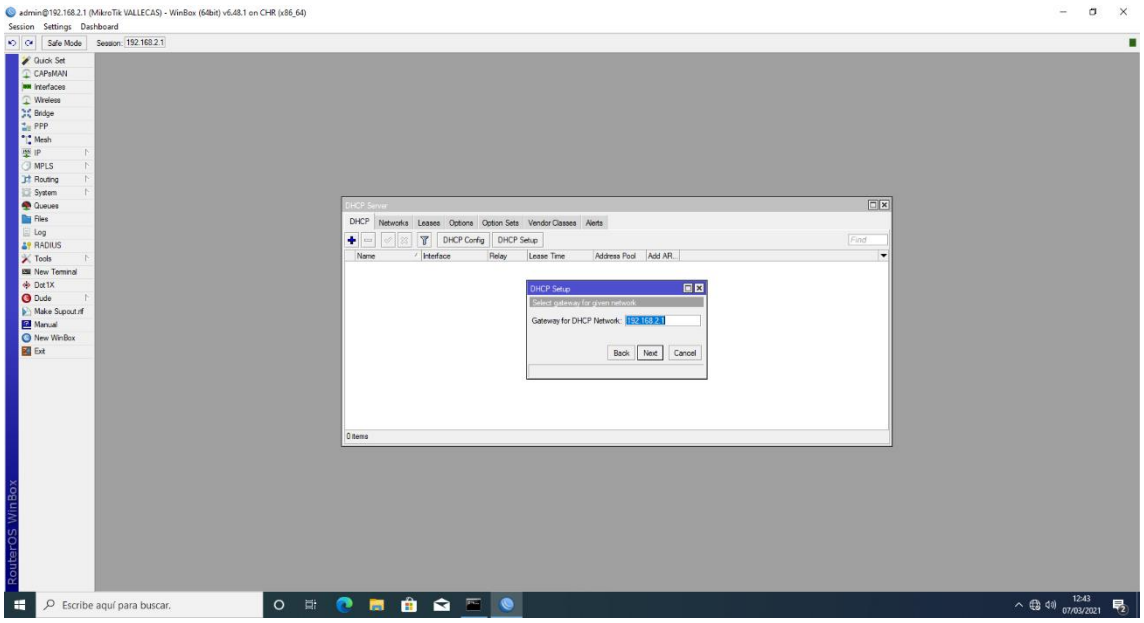

Figura 45. Introducción de la puerta de enlace.

Posteriormente nos solicita el rango de direcciones que queremos asignar. Vamos a asignar direcciones desde la 192.168.X.50/24 hasta la 192.168.X.254/24 para dejar

libres las primeras 50 direcciones para servidores y otros recursos que necesitemos, siendo X la sede según corresponda. Lo podemos ver en la Figura 46.

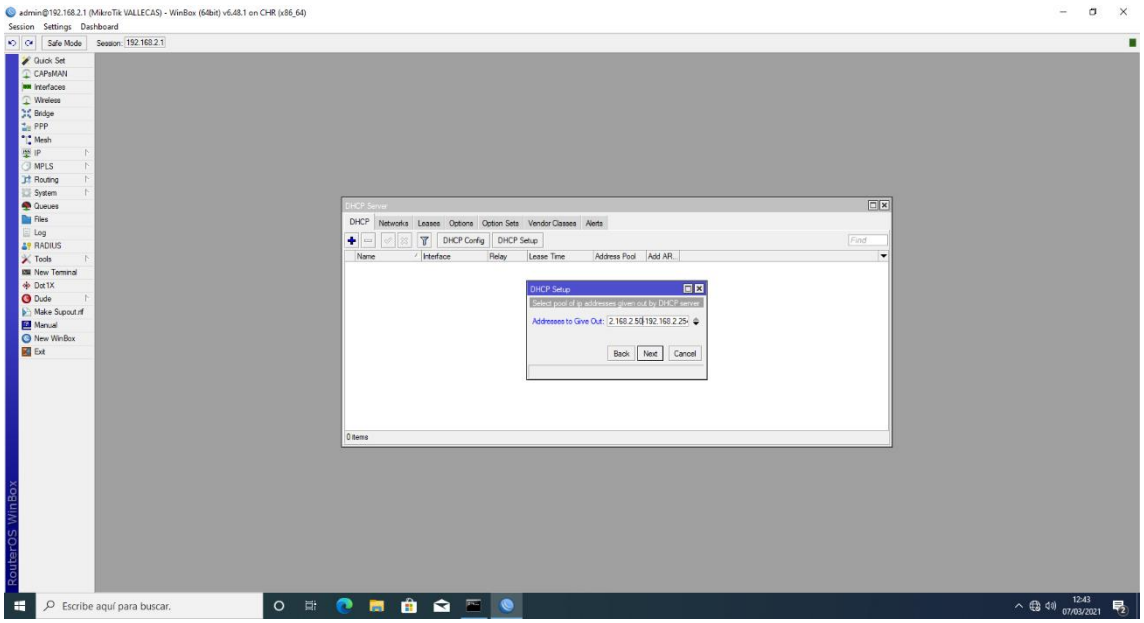

Figura 46. Rango de direcciones.

Una vez introducido el rango, como muestra la Figura 47, introducimos la dirección del servidor según corresponda en cada sede.

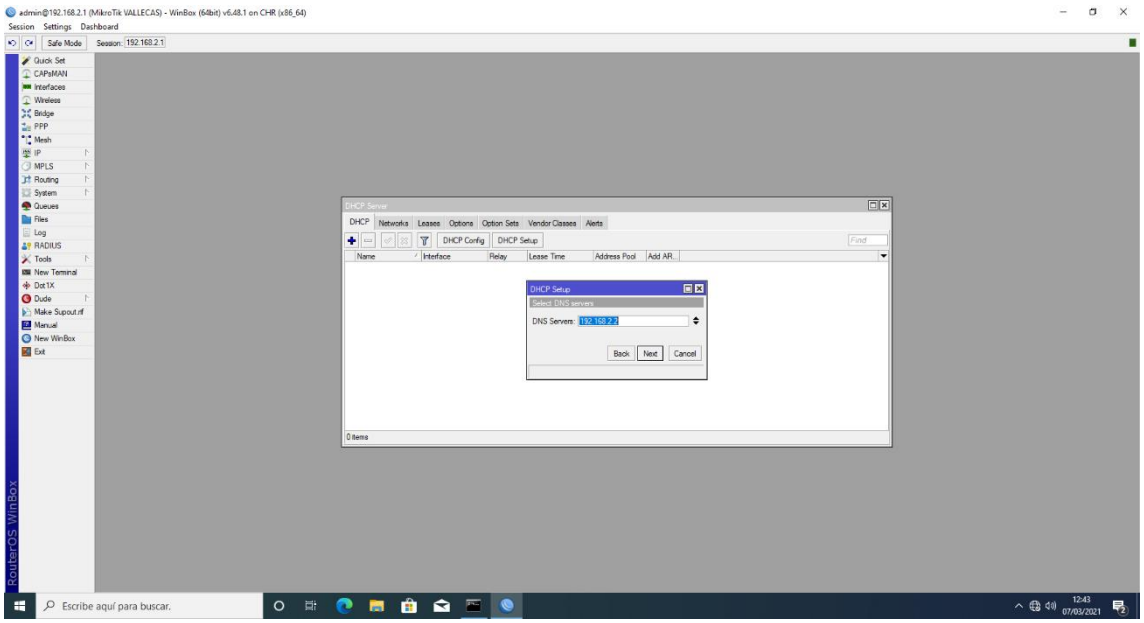

Figura 47. Selección de DNS

Por último, en la Figura 48, nos solicita el tiempo de concesión que tendrá cada solicitud.

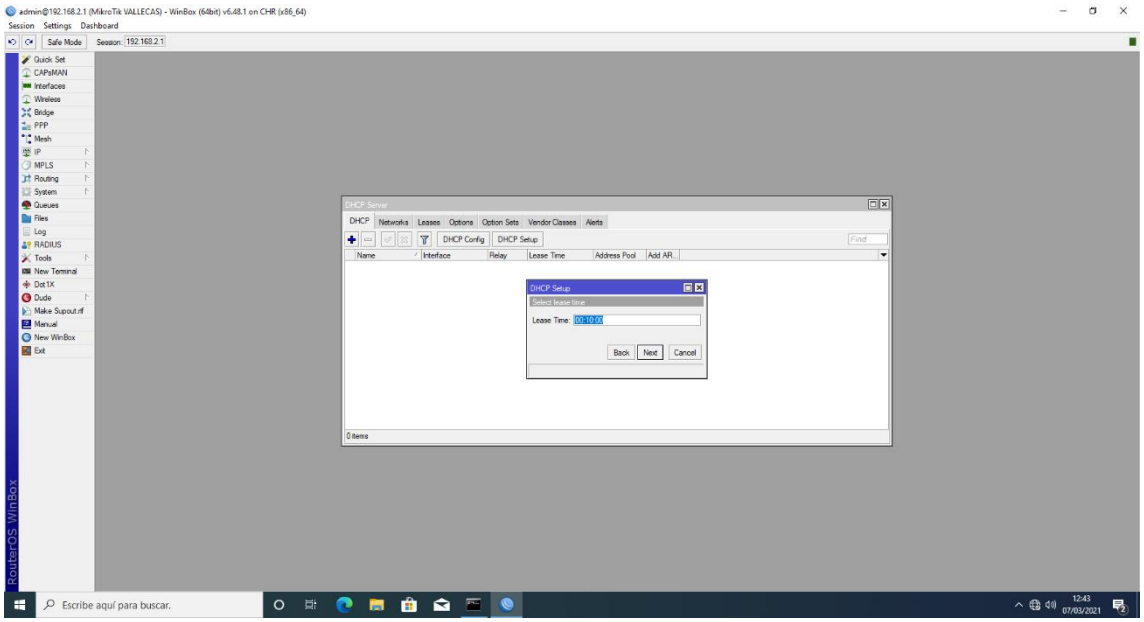

Figura 48. Tiempo de concesión de dirección.

Nos queda configurar las direcciones reservadas en cada sede, que en nuestro caso serán los servidores, aunque ya están asignadas en cada servidor al tenerlas fijas.

Para ello averiguaremos la dirección MAC de cada servidor y en leases le asignaremos la IP estática que le asignará a cada servidor según su MAC, quedando como muestra la Figura 49.

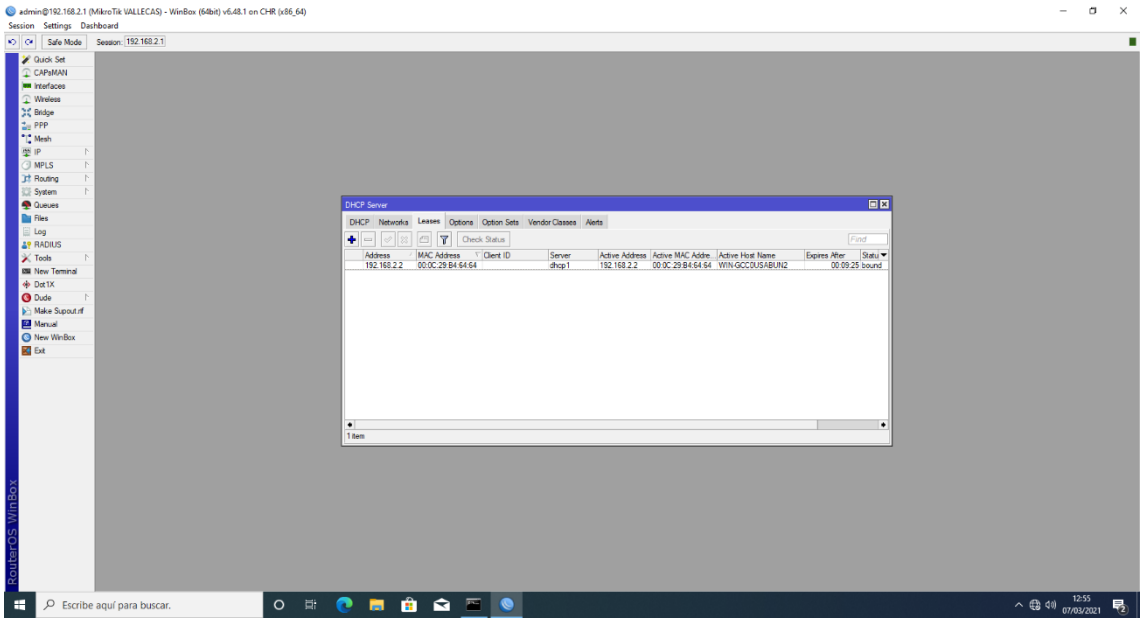

Figura 49. Reservas de direcciones.

6.2.2 VPN

En este apartado vamos a crear un túnel site to site de Mikrotik a Mikrotik vía OpenVPN, apoyándonos en la información que nos brindan en mikrotiklabs[5]

Queremos conseguir que nuestras redes locales se extiendan a través de la red pública mediante túneles virtuales cifrados.

Con este tipo de conexiones proporcionamos a nuestro sistema una capa de seguridad adicional, cifrando los datos que viajan de un lado a otro evitando intrusismo.

Existen diferentes protocolos para conseguir este objetivo como PPTP, Ipsec, OpenVPN, etc.

Dentro de los diferentes protocolos que disponemos para llevar a cabo nuestra VPN, hemos optado por OpenVPN.

Este protocolo en materia de seguridad establece la máxima encriptación, añadiendo una capa extra de seguridad. Además, es el protocolo más estable y con mejor rendimiento, ofreciendo velocidades elevadas.

Con OpenVPN, será necesario crear claves secretas y certificados para poder realizar la conexión entre las sedes.

A continuación, pasamos a detallar probablemente la configuración más importante para el correcto funcionamiento del negocio, haciendo uso de ambos routers, ya que sin ésta no se podrá llevar a cabo la replicación del servidor ni acceder a la web ni al servidor Owncloud.

Mikotik Vallecas

Para ello nuestro router de la sede de Vallecas va a actuar como router principal el cual va a manejar nuestro OpenVPN servidor.

Primeramente, tenemos que crear los certificados.

El primer certificado que vamos a crear va a ser la autoridad certificadora.

Para ello vamos a System y accedemos a Certificates. Pulsamos el icono +, y le llamaremos CA, tanto en Name como en Common Name quedando como vemos en la

Figura 50. En la pestaña Key Usage, seleccionamos Key cert. Sign y crl sing como en la Figura 51 y hacemos clic en Apply.

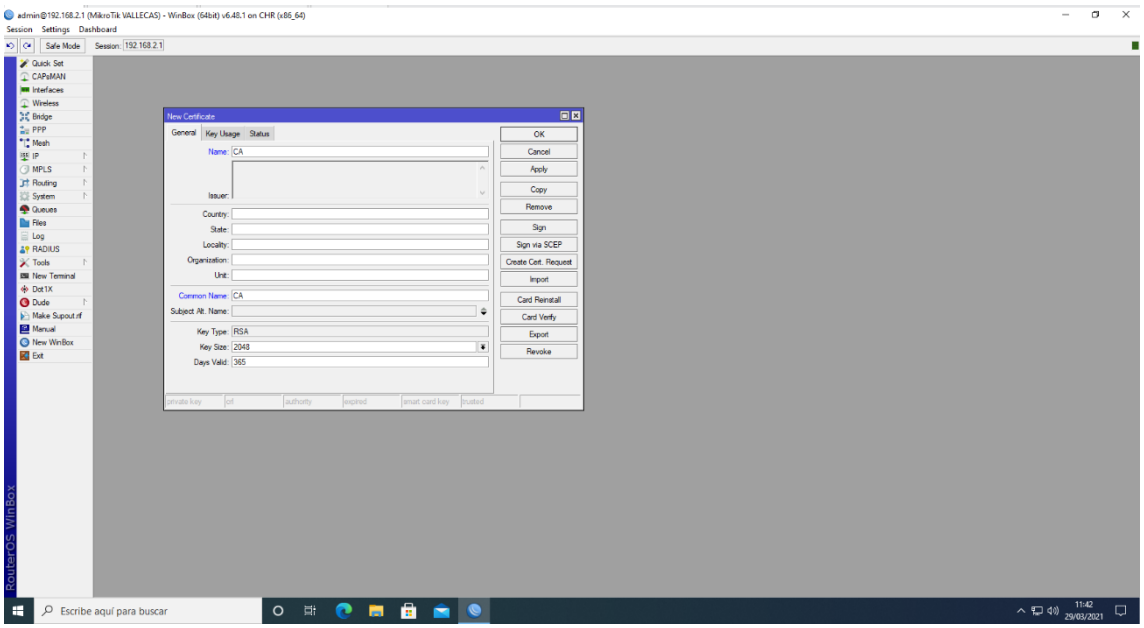

Figura 50. Nombre del certificado.

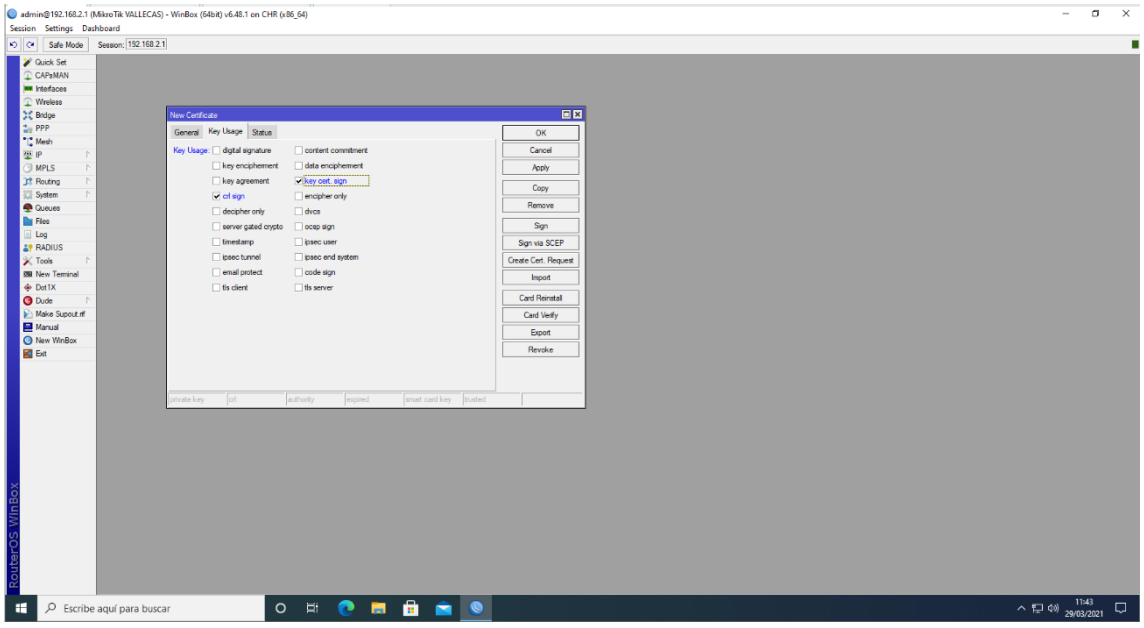

Figura 51. Selección en Key Usage.

Lo siguiente será firmar el certificado. Para ello pulsamos Sign y firmamos nuestro certificado con nuestra IP pública, quedando como en la Figura 52. En este caso para virtualizarlo le asignamos la dirección IP estática que hemos escogido para nuestro Router (192.168.1.100).

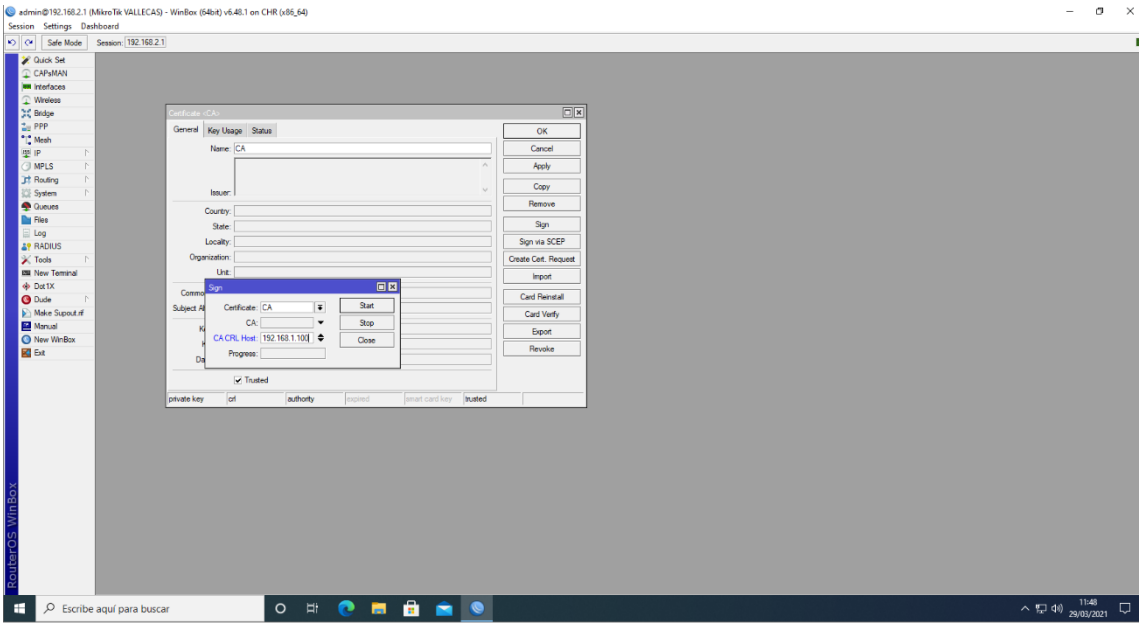

Figura 52. Firma del certificado CA.

Una vez creado el certificado de la autoridad certificadora, lo que vamos a crear es el certificado del servidor. Al igual que antes nos vamos a System y accedemos a Certificates. Pulsamos el icono +, y le llamaremos Server, tanto en Name como en Common Name y en la pestaña Key Usage seleccionamos key encipherment y data encipherment para decir que la llave y los datos son encriptados. Además, seleccionaremos tls server y aplicamos la configuración pulsando Apply.

Pulsamos Sign y firmaremos el certificado con el CA anteriormente creado, como vemos en la Figura 53.

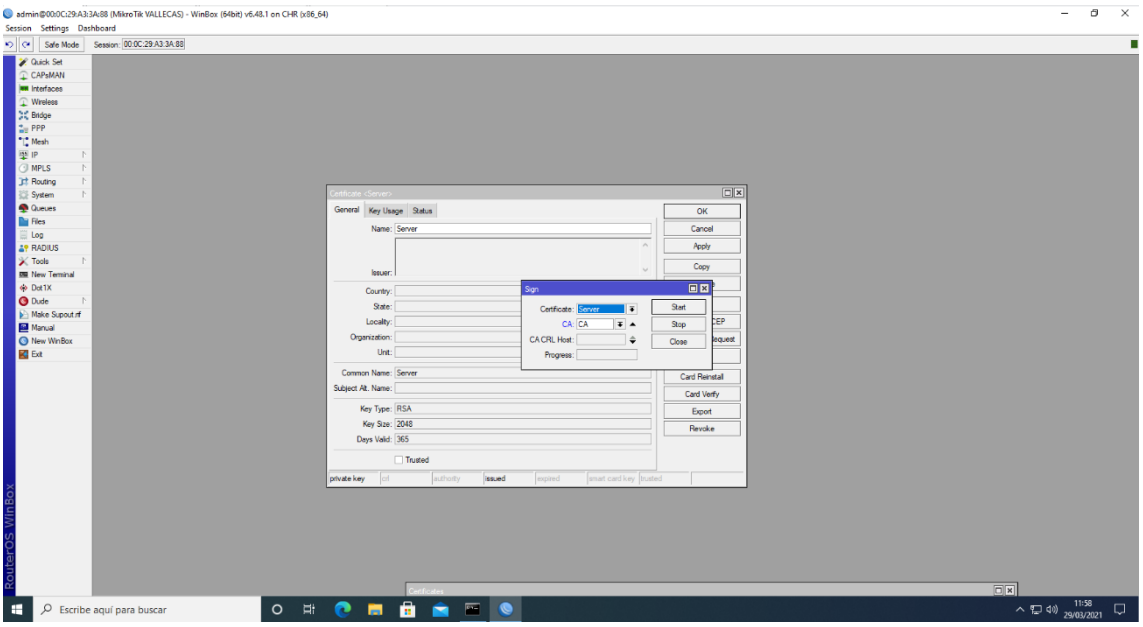

Figura 53. Firma del certificado Server.

Por último, crearemos el certificado cliente. Si hubiera más sedes tendríamos que crear uno por cada sede.

Vamos a System y accedemos a Certificates. Pulsamos el icono +, y le llamaremos Server, tanto en Name como en Common Name y en la pestaña Key Usage seleccionamos tls client y aplicamos la configuración pulsando Apply.

Pulsamos Sign y firmaremos el certificado con el CA anteriormente creado.

El siguiente paso es irnos a la ventana PPP y crearemos el Profile. Utilizaremos el default-encryption en donde vamos a configurar el local address. En nuestro caso utilizaremos el direccionamiento 192.168.4.1 para que esa sea nuestra ip del Mikrotik en el túnel VPN, como lo mostrado en la Figura 54.

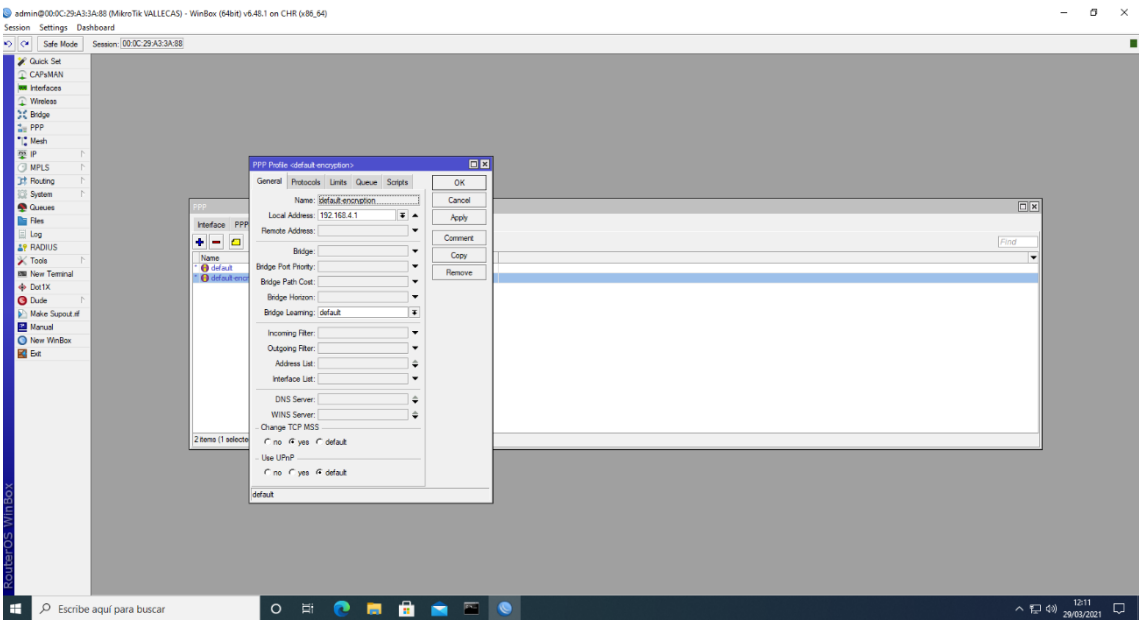

Figura 54. Profile de PPP.

Una vez creado el Profile, habilitaremos el OVPN Server en PPP. Lo configuramos con el default-encryption y el certificado Server que habíamos creado anteriormente. Además seleccionaremos sha1 y aes256 como se muestra en la Figura 55.

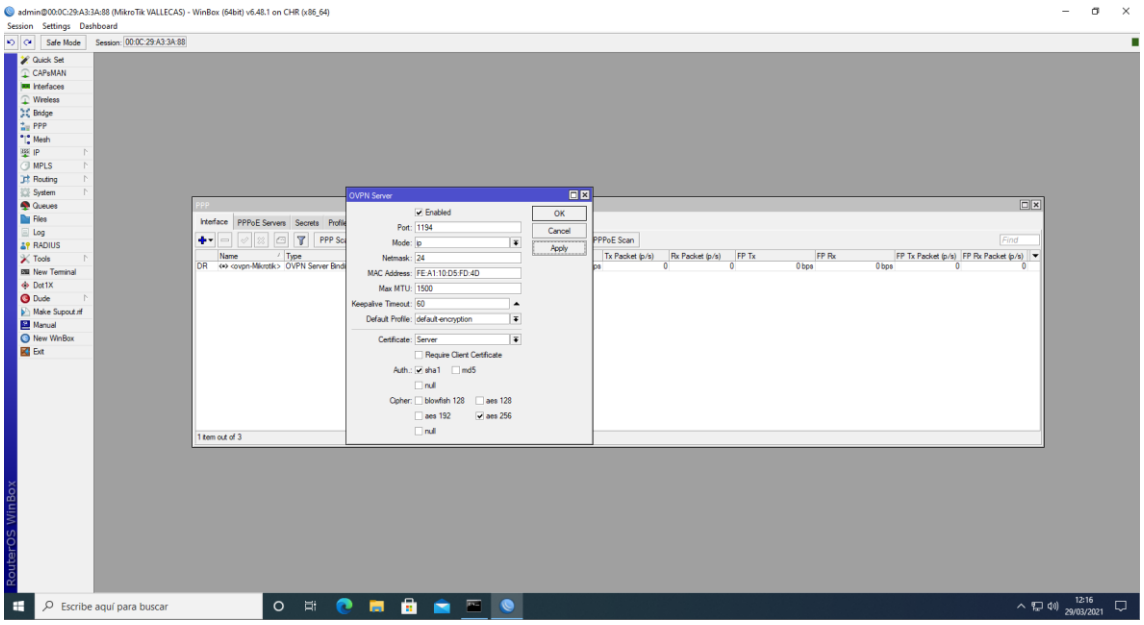

Figura 55. Habilitación de OVPN Server.

Crearemos nuestro usuario en la pestaña Secret. Le llamaremos Mikrotik y le asignaremos una contraseña. Además utilizaremos el default-encryption como Profile y el servicio será ovpn.

Como muestra la Figura 56, le asignaremos el direccionamiento 192.168.4.2 que será la Ip del Mikrotik del cliente en el túnel VPN.

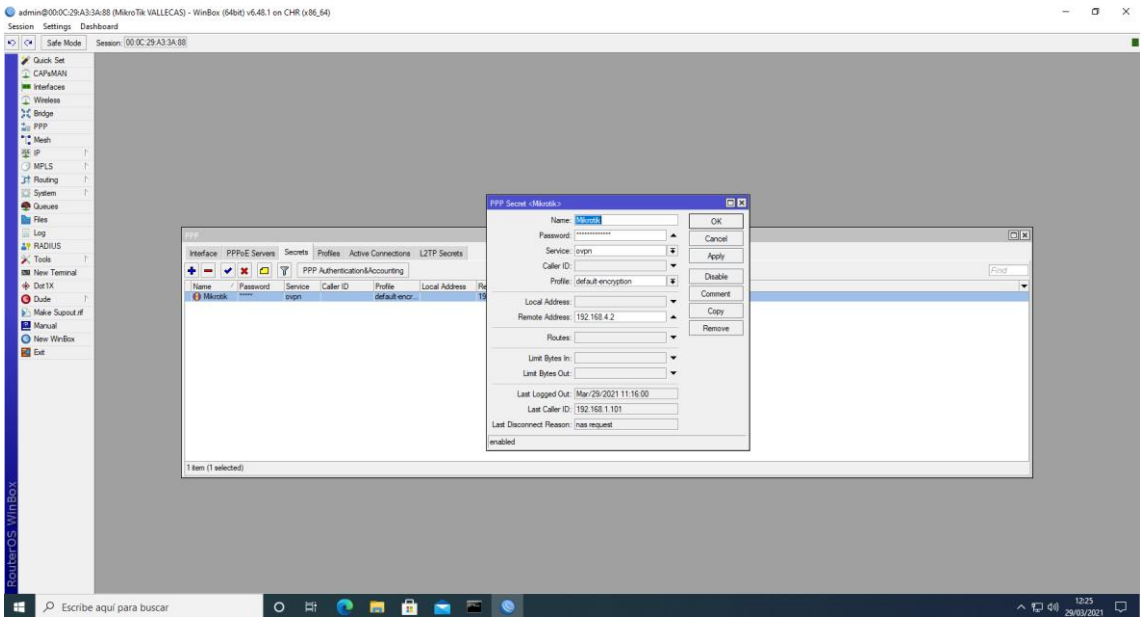

Figura 56. Creación del Secret.

Por último, exportaremos los certificados CA y cliente de Mikrotik server a Mikrotik cliente. En el certificado cliente crearemos una contraseña que necesitaremos para cuando lo importemos.

Mikrotik Coslada

Lo primero que haremos será importar los certificados en hemos creado en el otro mikrotik, añadiéndolos a la lista de archivos del Mikrotik de Coslada, como vemos en la Figura 57.

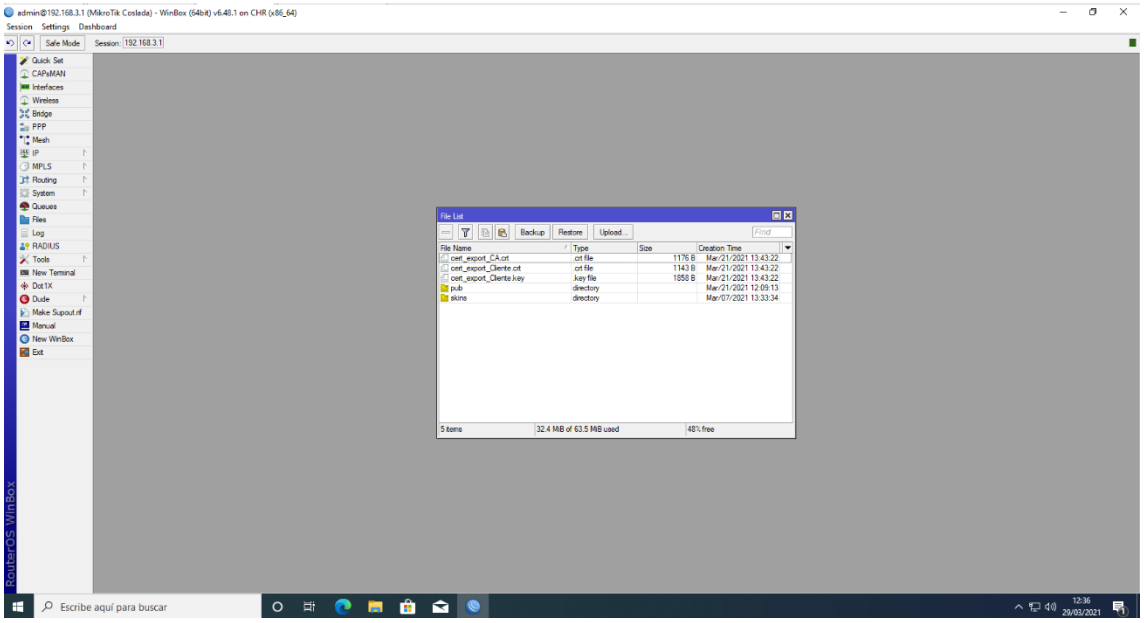

Figura 57. Listado de archivos.

Lo que haremos será irnos a System->Certificates.

Una vez dentro daremos a Import y selecionaremos el certificado cert_export_CA.crt.

Seguidamente cert_export_Cliente.crt, y por último la llave de este certificado cert_export_Cliente.key en el que tendremos que poner la contraseña que pusimos al exportar, como se muestra en la Figura 58.

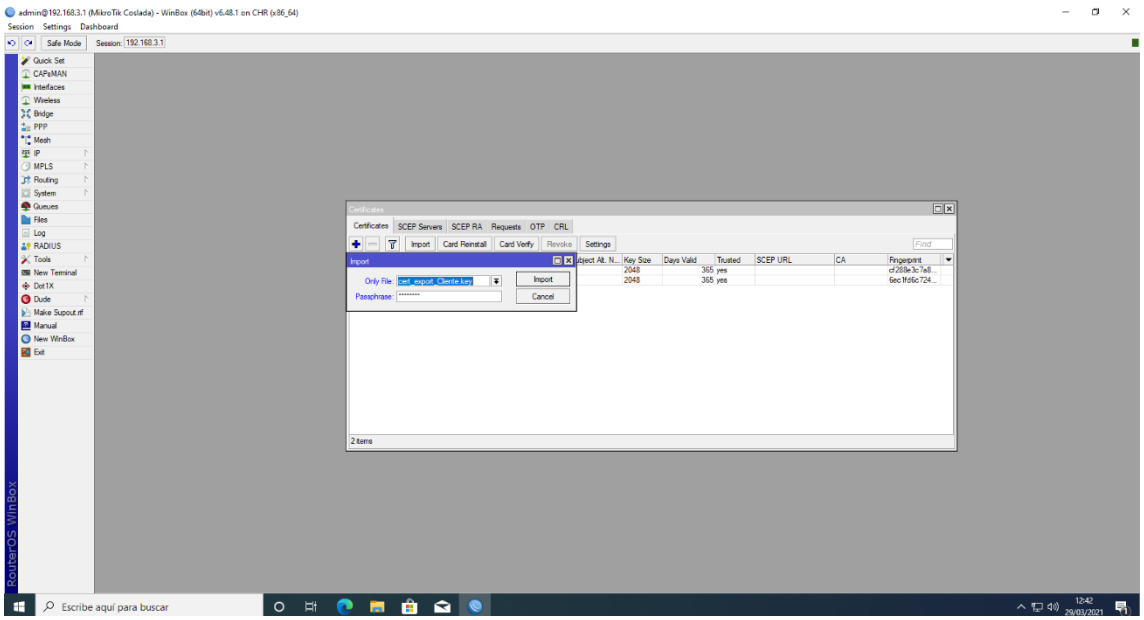

Figura 58. Importación de certificados.

El siguiente paso será crear el Ovpn Client. Para ello iremos a PPP y en la pestaña + buscaremos el OVPN client.

Le vamos a llamar ovpn-remote en la pestaña General.

En la pestaña Dial Out, en Connect to pondremos la ip pública de nuestro Mikrotik servidor, que en nuestro caso al virtualizarlo será 192.168.1.100.

En User y Password pondremos el secret que habíamos creado en el Mikrotik de Vallecas con su debida contraseña y en el certificate pondremos cert_export_Cliente.crt_0. Seleccionaremos sha1 y aes 256 como anteriormente, quedando como lo moestrado en la Figura 59.

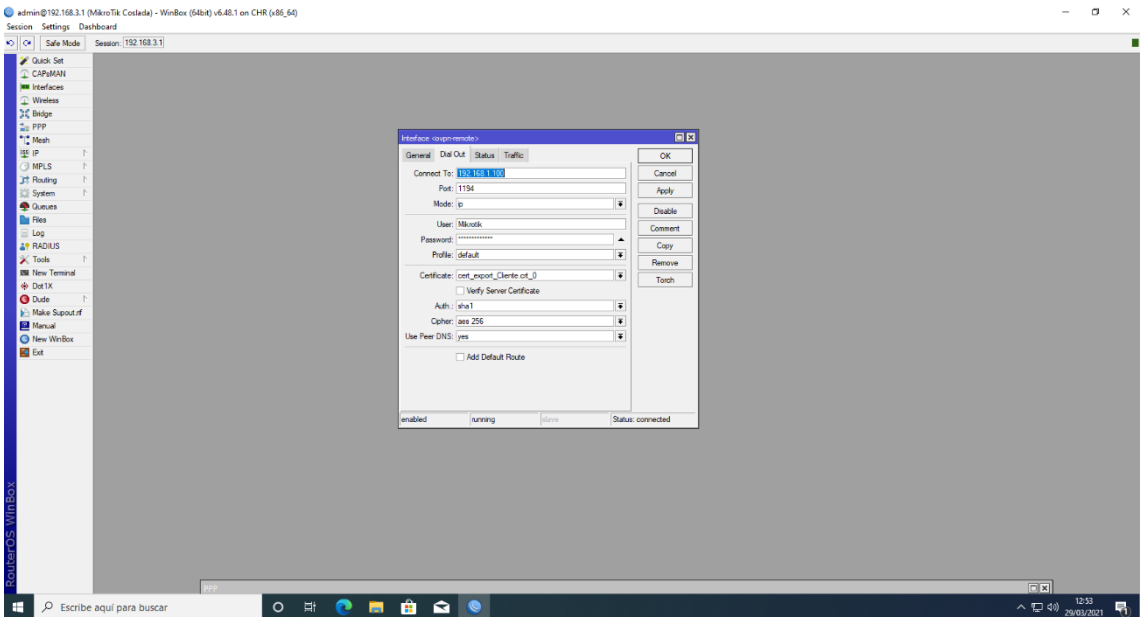

Figura 59. Creación OVPN Client.

Para que los recursos de una sede sean disponibles desde cualquier sede, debemos crear una ruta estática.

Para Coslada crearíamos la ruta como muestra en la Figura 60 en el Mikrotik de Coslada.

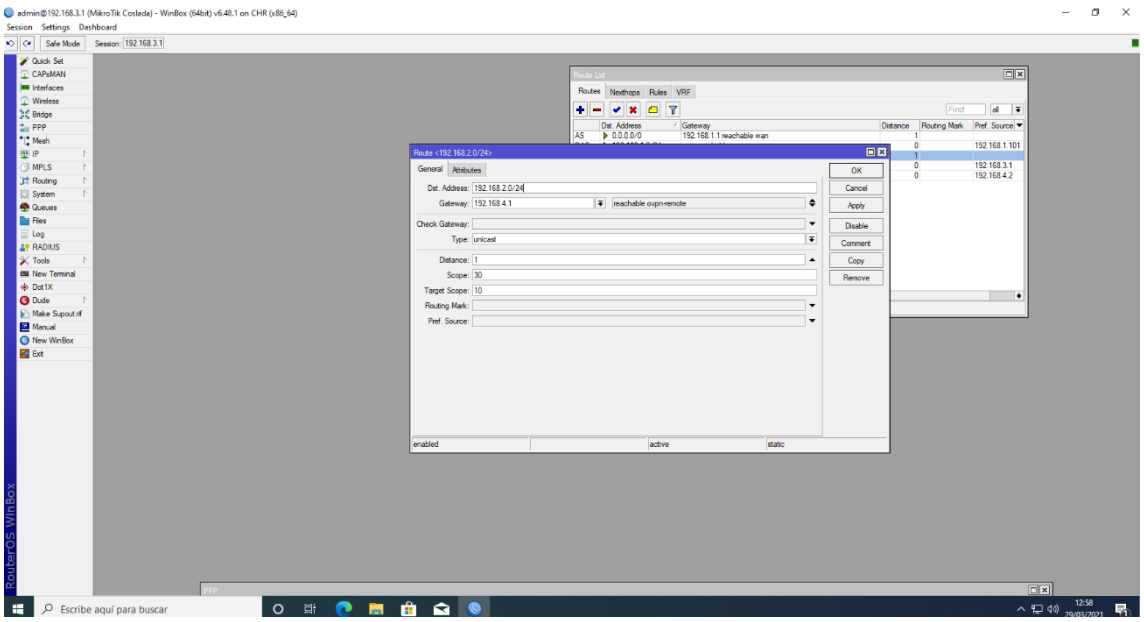

Figura 60. Ruta para la sede de Coslada.

Para Vallecas crearíamos la ruta con los parámetros como muestra la Figura 61 en el Mikrotik de Vallecas.

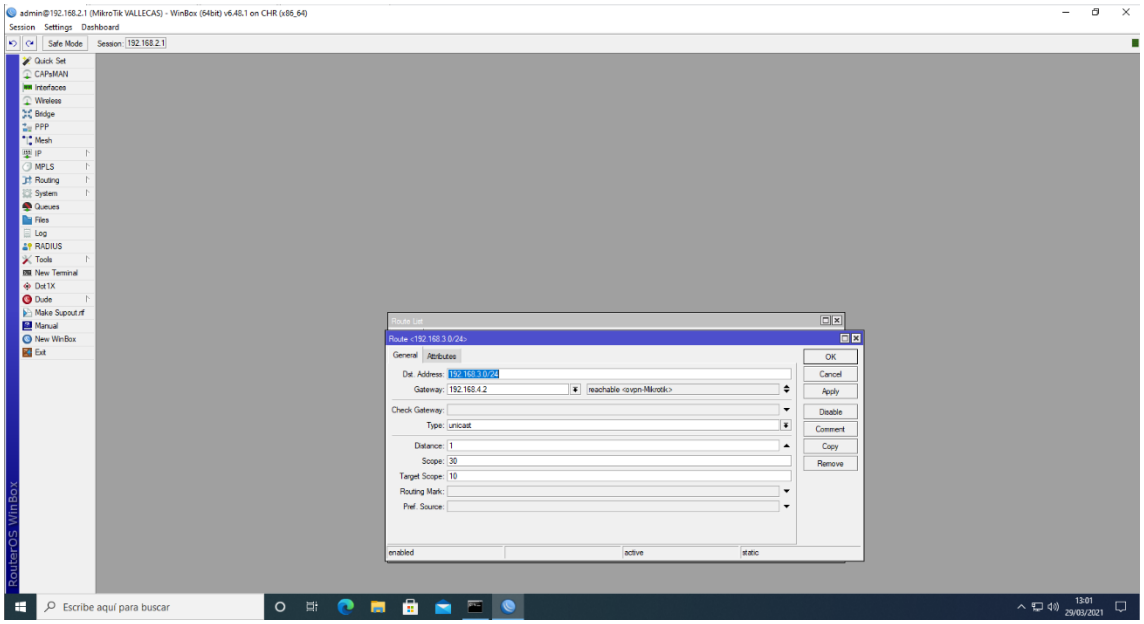

Figura 61. Ruta para la sede de Vallecas.

Por último, solo necesitaríamos comprobar a través del comando ping en cmd si se ven ambas redes desde un host a la dirección del otro.

En la Figura 62 podemos ver que tienen conexión.

También con el comando tracert podemos ver que está configurado correctamente visualizando la ruta que lleva de extremo a extremo.

```
C:\Users\VALLECASPC>ping 192.168.3.254

Haciendo ping a 192.168.3.254 con 32 bytes de datos:
Respuesta desde 192.168.3.254: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.3.254: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.3.254: bytes=32 tiempo=2ms TTL=126
Respuesta desde 192.168.3.254: bytes=32 tiempo=2ms TTL=126

Estadísticas de ping para 192.168.3.254:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms

C:\Users\VALLECASPC>
```

Figura 62. Comprobación del correcto funcionamiento de la VPN.

6.3 Instalación y configuración Servidor replicado

En el siguiente apartado vamos a llevar a cabo la replicación del servidor.

De este modo haremos réplicas de la información que contiene el principal, siendo una copia fiel de la original. Con ello evitaremos pérdida de datos por fallo o mal funcionamiento.

Esta replicación es muy ventajosa, ya que en caso en de que caiga alguno, el otro puede reemplazarlo sin detener el servicio.

También con esta replicación repartimos el tráfico entre los servidores, permitiendo aligerar la carga de procesamiento, no como en el caso de tener un único servidor.

Por todo ello, vamos a desarrollar su configuración e instalación para su correcto funcionamiento.

Primeramente aplicaremos el paso 6.1.2 y 6.1.3 para nuestro servidor que queremos replicar y lo nombraremos según la tabla 1.

Deberemos tener en cuenta que el DNS será el mismo que el DNS primario para que pueda pertenecer al dominio y así poder replicarlo posteriormente.

El siguiente paso será pertenecer al dominio creado en el servidor primario. Para ello aplicaremos los mismos pasos que en el punto 6.1.5

En siguiente punto, iremos a las notificaciones (triangulo amarillo de advertencia) y daremos a promover el servidor de dominio.

Nos desplegará un asistente. Tendremos que seleccionar Agregar un controlador de dominio a un dominio existe.

Como vemos en la Figura 63, por defecto aparecerá el dominio gym.local ya que ya pertenecemos a dicho dominio.

También nos pedirá las credenciales del administrador para realizar la operación.

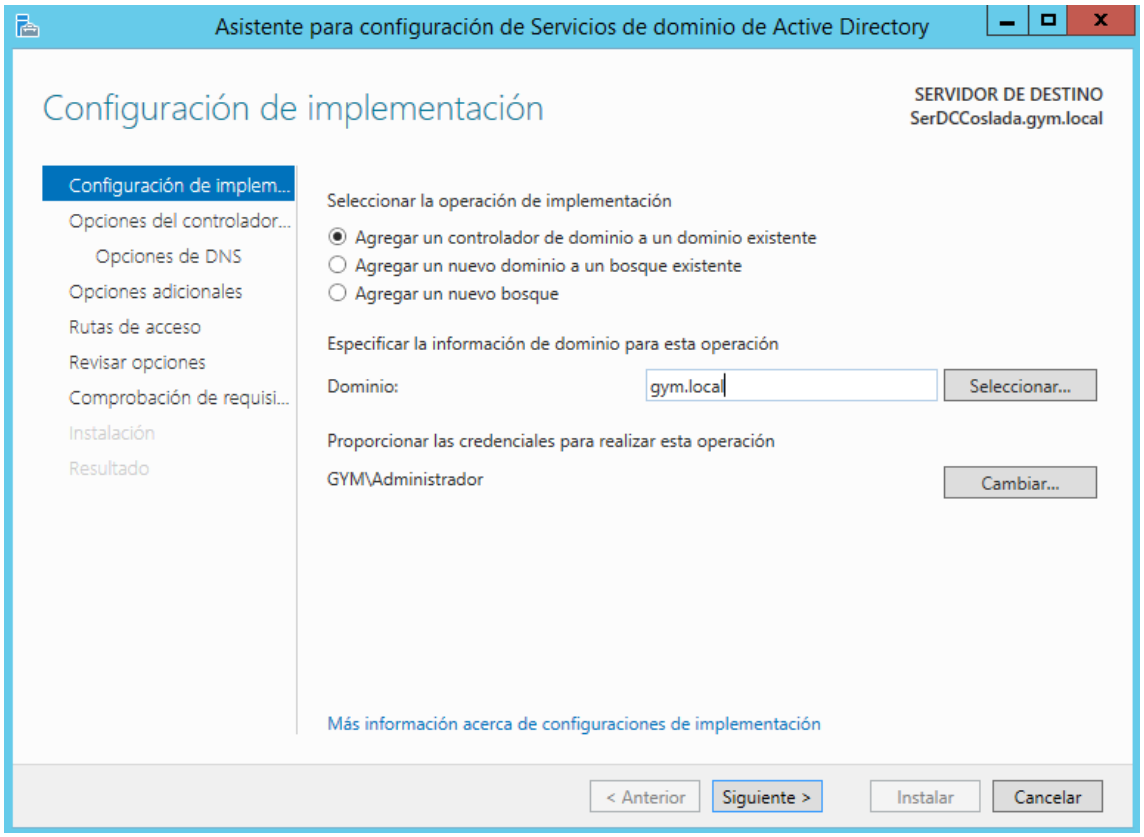

Figura 63. Agregamos el controlador al dominio ya existente.

Daremos a siguiente, y como muestra la Figura 64, nos solicitará una contraseña por si tuviéramos que entrar por un problema de corrupción del sistema, no siendo necesario que sea la misma. Pulsaremos siguiente.

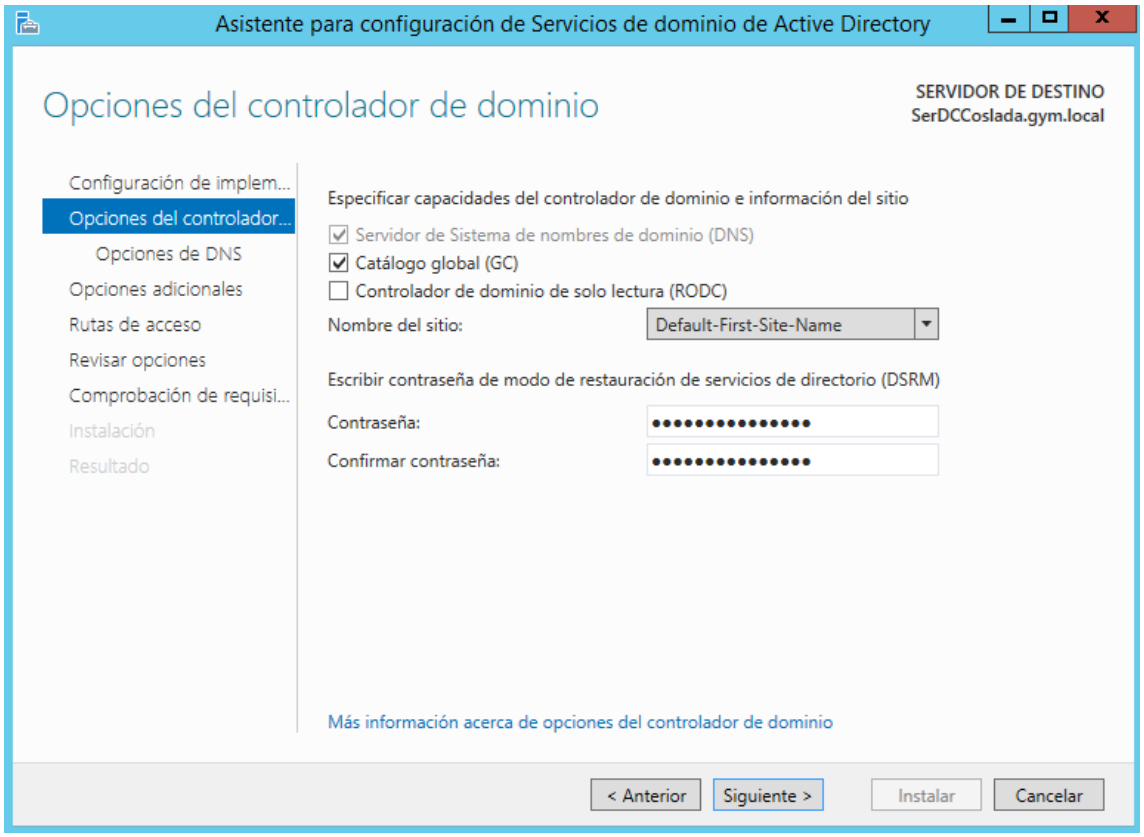

Figura 64. Solicitud de contraseña.

La siguiente opción que debemos configurar es de donde queremos replicar, que elegiremos el maestro de operaciones de la sede de Vallecas.

Le daremos a siguiente hasta que aparezca instalar. Pulsaremos y empezará el proceso de promoción de esta réplica a controlador de dominio adicional.

Una vez finalice se reiniciará el servidor y podemos comprobar que se ha realizado correctamente, visualizando como en la Figura 65 que ambos son los controladores del dominio.

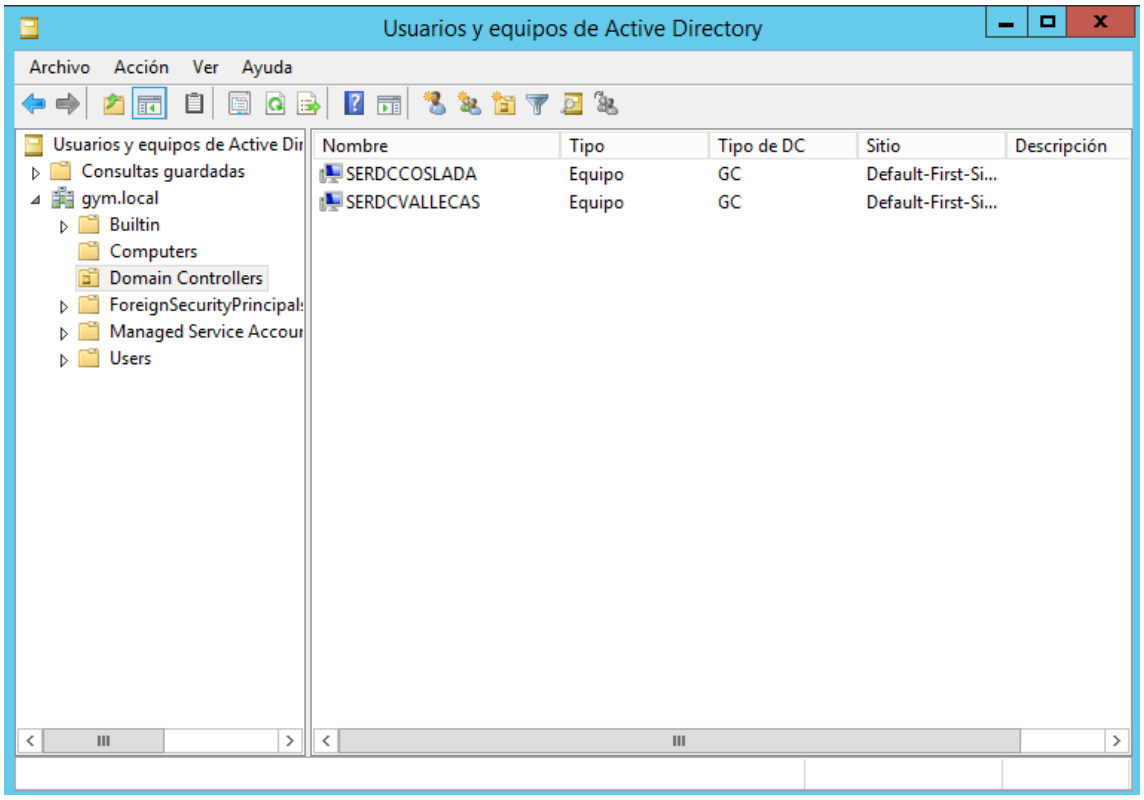

Figura 65. Controladores de dominio replicados.

Para terminar, configuraremos el DNS del servidor replicado para que primero resuelva el servidor replicado y después el maestro de operaciones, quedando como muestra la Figura 66.

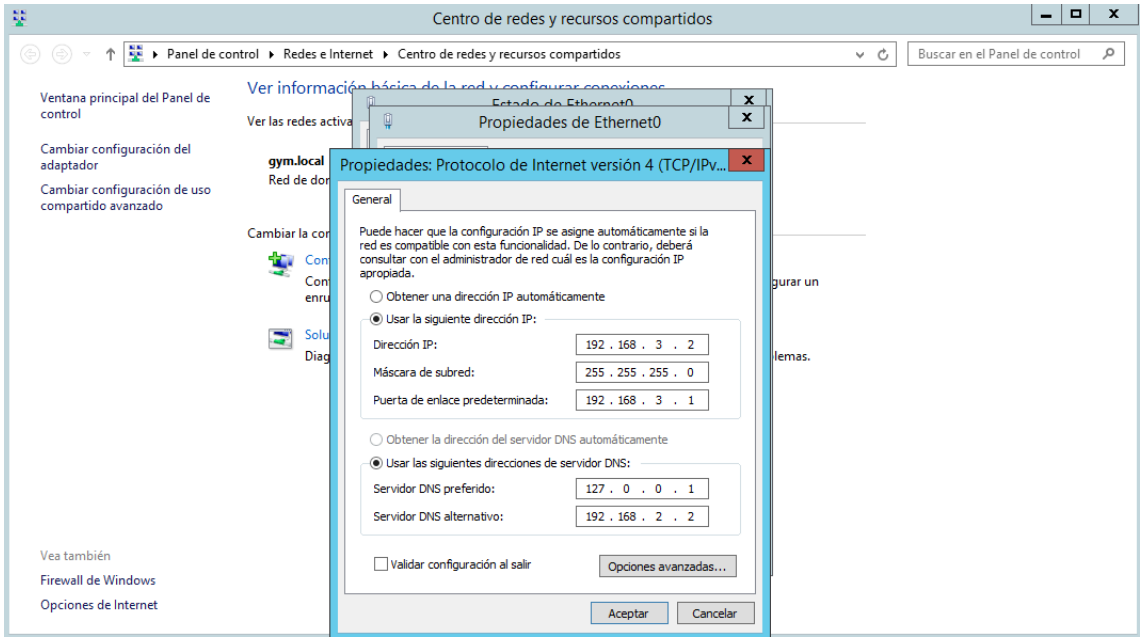

Figura 66. Configuración de DNS.

6.4 Instalación y configuración Servidor Web/WordPress

Para poder llevar a cabo nuestro objetivo de la página web, es necesario trabajar con los CMS.

Un CMS es un sistema de gestión de contenidos, en el que a través de esta herramienta se permite la creación de un sitio web sin recurrir a recursos técnicos avanzados, con un uso sencillo en cuanto a su gestión y mantenimiento en el tiempo.

Existen diversos tipos de CMS, como Blogger, Joomla, Drupal, etc. pero en nuestro caso vamos a utilizar WordPress.

WordPress es un CMS orientado a blogs. Es el más extendido actualmente debido a su facilidad de uso y tiene la gran ventaja de ser gratuito.

Este CMS trabaja con plugins que son unas aplicaciones que corre a la par del WordPress para facilitar diversas tareas dependiendo del plugin que estemos hablando. Existen plugin gratuitos y de pago, pudiendo adaptarse a cualquier necesidad que se nos pueda surgir en un futuro.

Por todo ello hemos decidido su utilización para el proyecto.

Para su instalación necesitamos seguir una serie de directrices que vamos a detallar.

Antes de realizar cualquier paso, instalamos un host con Windows Server 2012 como en el apartado 6.1.1 y según la Tabla 2, le asignamos la IP estática, la máscara, la puerta de enlace y el DNS correspondiente.

También haremos que pertenezca al dominio como en el punto 6.1.5

6.4.1 Instalación XAMPP y WORDPRESS

Para la instalación de WordPress, he decidido utilizar el paquete de software libre XAMPP, el cual incluye las herramientas necesarias para poder alojar el WordPress en nuestro servidor creado para tal causa.

XAMPP es un servidor independiente de plataforma de código libre que nos permite instalar Apache, MySQL, PHP y phpMyAdmin convirtiendo nuestro equipo en un componente perfecto para el desarrollo de nuestra web.

Para su instalación accedemos a la página web https://www.apachefriends.org/es/index.html, descargamos la última versión y comenzamos con la instalación.

Aparecerá una ventana de bienvenida en la que sólo hay hacer clic en el botón Next.

En la siguiente pantalla se puede elegir los componentes que quieres utilizar. Por defecto dejaremos todos como muestra la Figura 67, aunque sólo será necesario Apache, MySQL, PHP y phpMyAdmin.

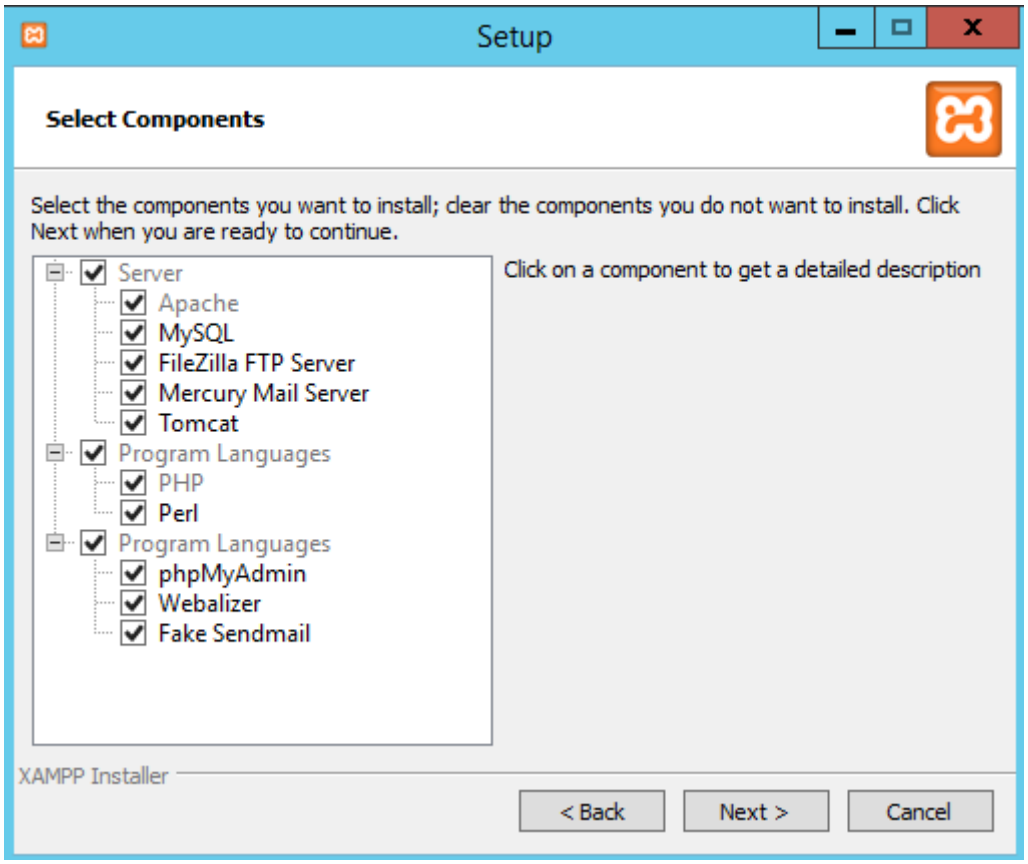

Figura 67. Instalación de XAMPP

En la siguiente configuración nos solicita la carpeta donde se instalará, que dejaremos por defecto la que viene que es C:\xampp.

Elegiremos el lenguaje que viene por defecto y daremos next hasta que comience la instalación.

Una vez instalado arrancamos XAMPP y como muestra la Figura 68, seleccionaremos los módulos a utilizar y haremos clic en START tanto en el módulo de Apache como en el de MySQL. Con el primero arrancamos el servidor Apache, y con el segundo arrancamos el gestor de base de datos.

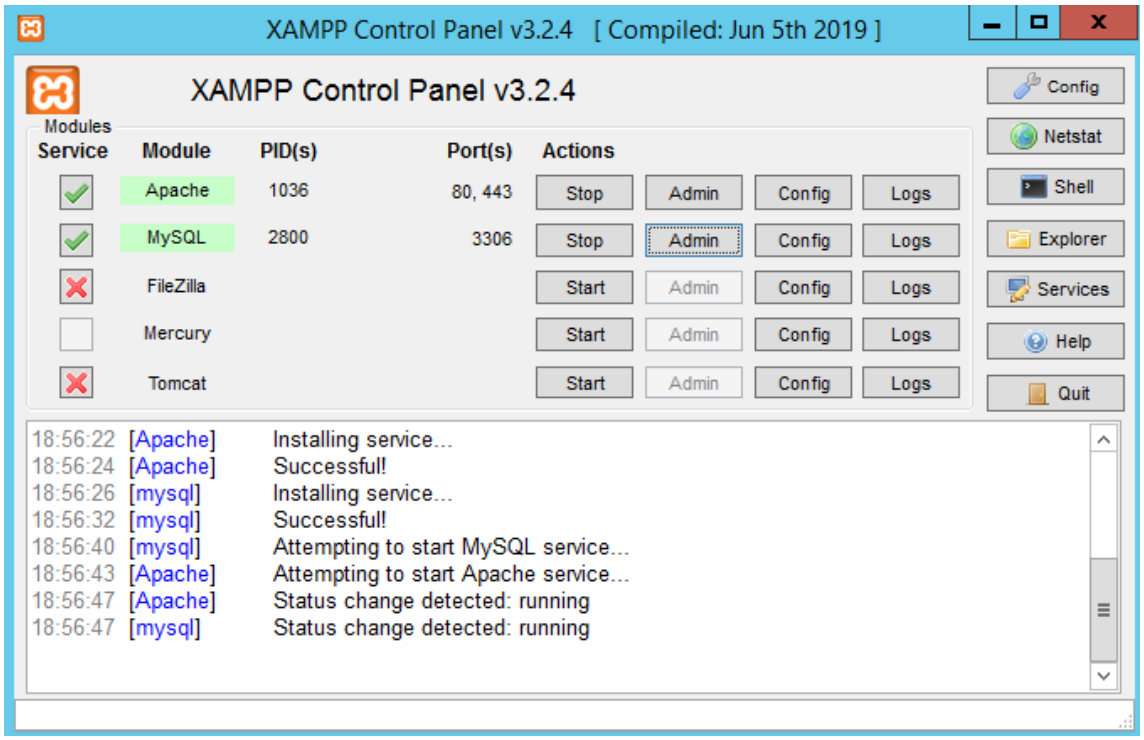

Figura 68. Panel de Control de XAMPP.

Una vez instalado XAMPP, necesitamos crear una base de datos nueva a través de phpMyAdmin.

Para entrar a phpMyAdmin se puede hacer desde el panel de control de XAMPP haciendo clic en el botón Admin de MySQL, o puedes entrar directamente desde el navegador a http://localhost/phpmyadmin/

Al abrir el gestor de base de datos, podemos ver a la izquierda de la ventana las bases de datos creadas por defecto en el servidor con el que estamos trabajando.

En ese mismo punto haceros clic en Nueva, y a la derecha pondremos el nombre de nuestra base de datos (gymbd) con la opción utf8_general_ci. Daremos clic al botón Crear.

A la izquierda aparecerá nuestra base de datos creada como apreciamos en Figura 69.

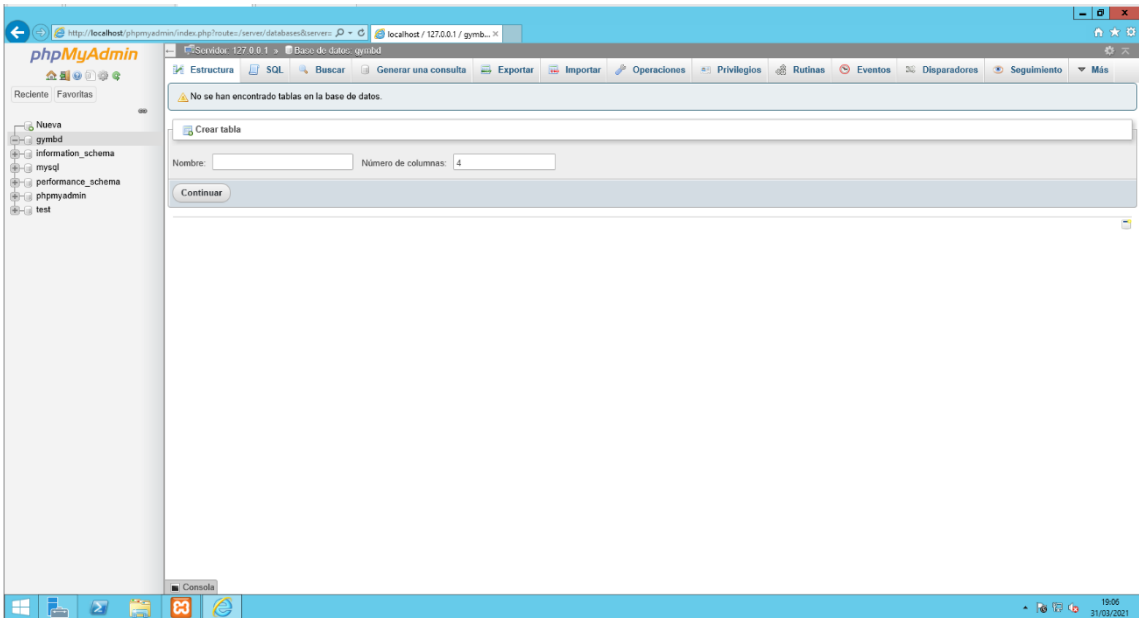

Figura 69. Base de datos gymbd creada en phpMyAdmin.

Una vez con la base de datos creada y el servidor arrancado, necesitamos descargarnos el fichero .zip de Wordpress de la página https://es.wordpress.org/download/ , concretamente la versión 5.7.

Descargaremos los archivos descomprimidos en C:\xampp\htdocs como muestran la Figura 70 y la Figura 71, y entraremos en http://localhost/wordpress/ desde el navegador.

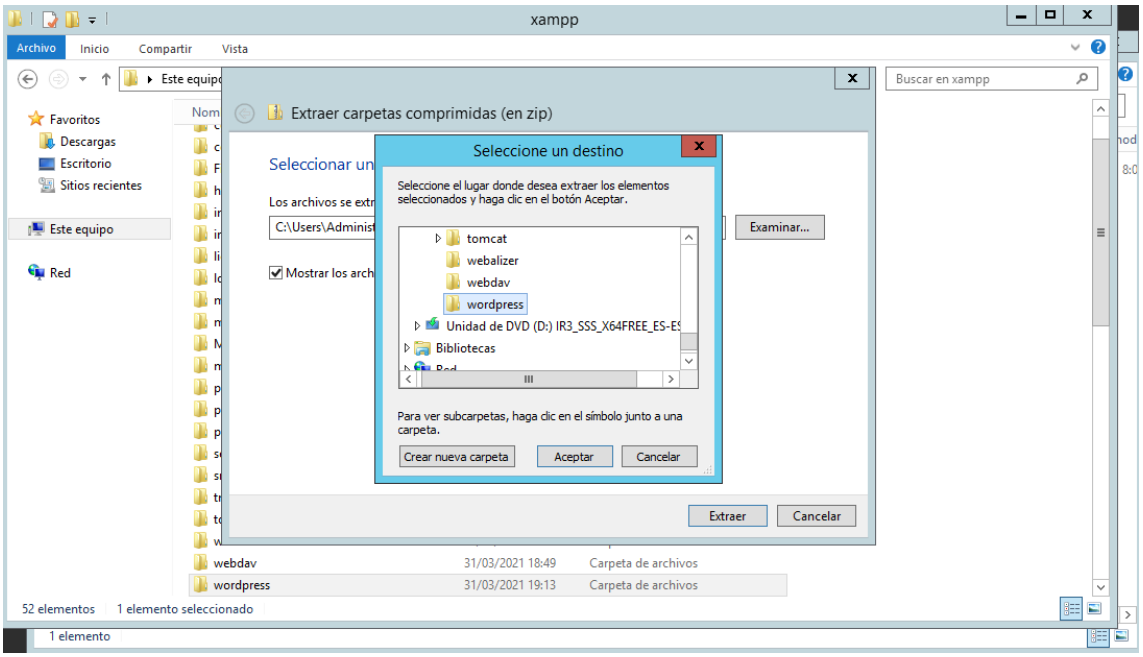

Figura 70.Descomprimir el archivo descargado.

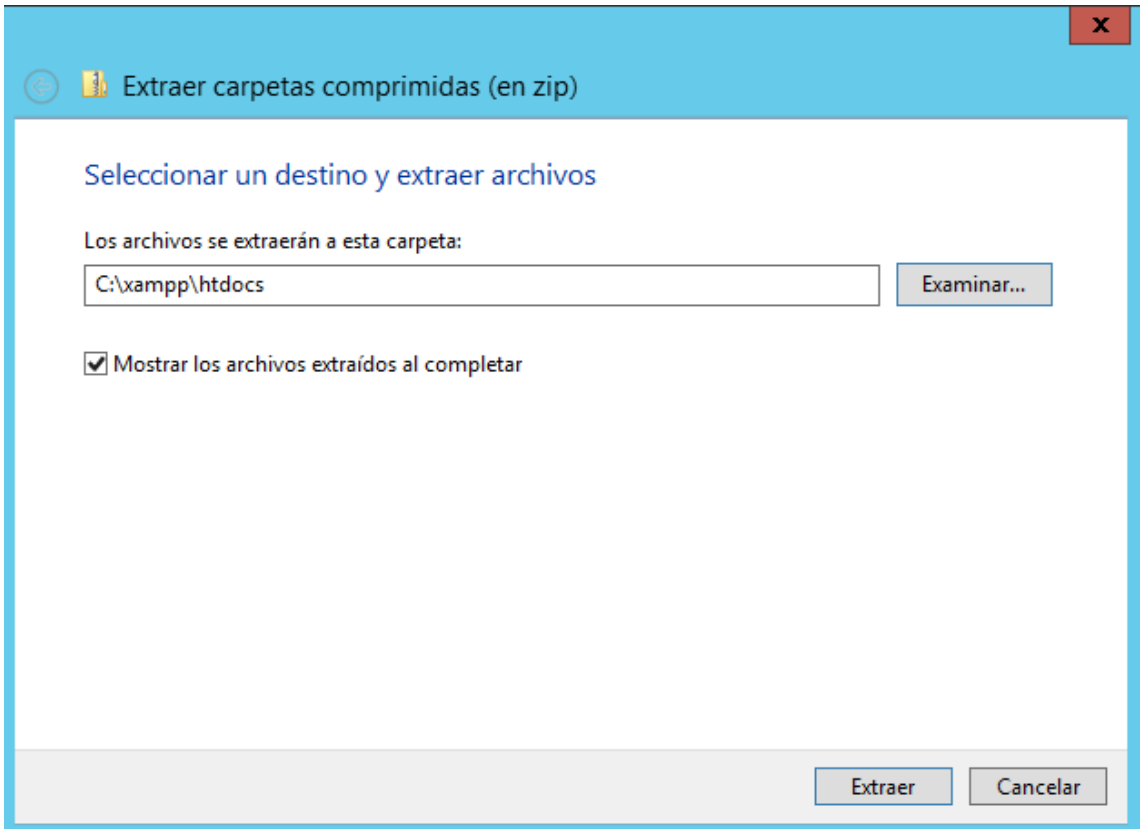

Figura 71. Selección del destino de la carpeta WordPress.

Como vemos en la Figura 72, aparece una pantalla de bienvenida para empezar la instalación y configuración de WordPress. Haremos clic en el botón ¡Vamos a ello!

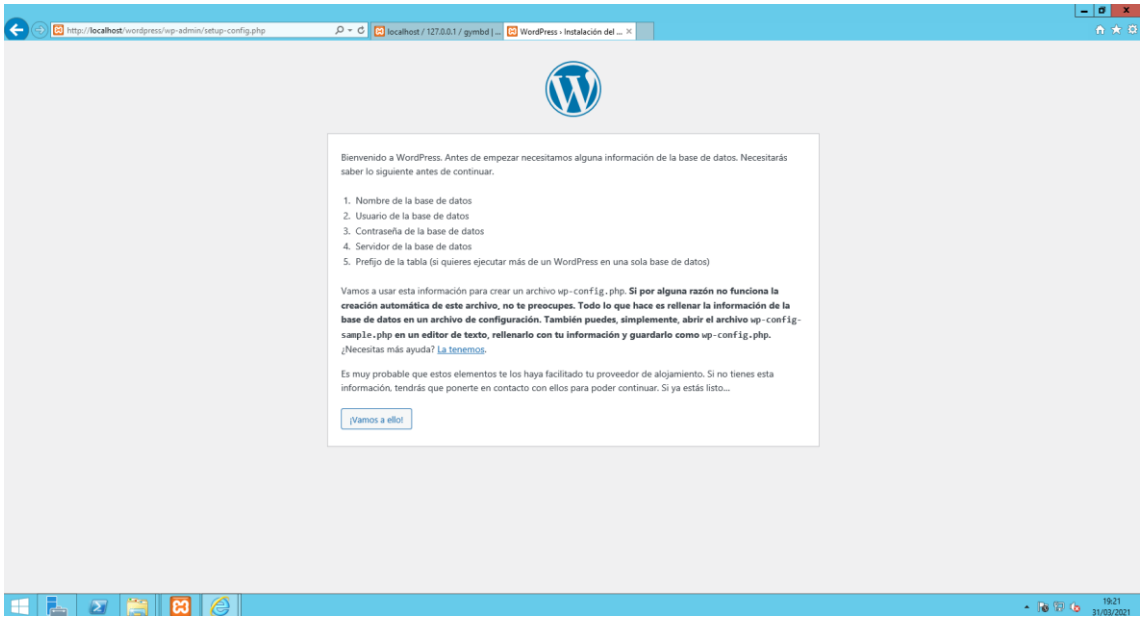

Figura 72. Inicio del asistente de instalación.

En la pantalla siguiente tenemos que meter los datos de la base de datos creada anteriormente. El usuario será root y no tiene contraseña, aunque lo podemos modificar. Completamos los datos como en la Figura 73 y le damos a enviar.

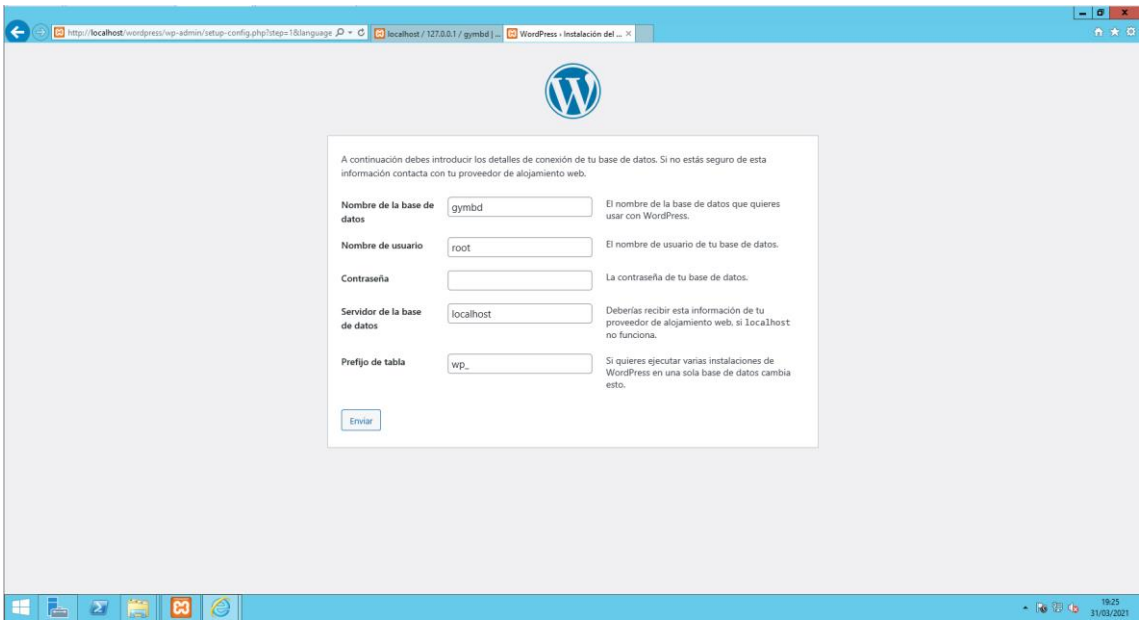

Figura 73. Datos sobre la base de datos creada.

Saldrá una ventana que comentará que hemos terminado parte de la instalación y haremos clic a Ejecutar la instalación como observamos en la Figura 74

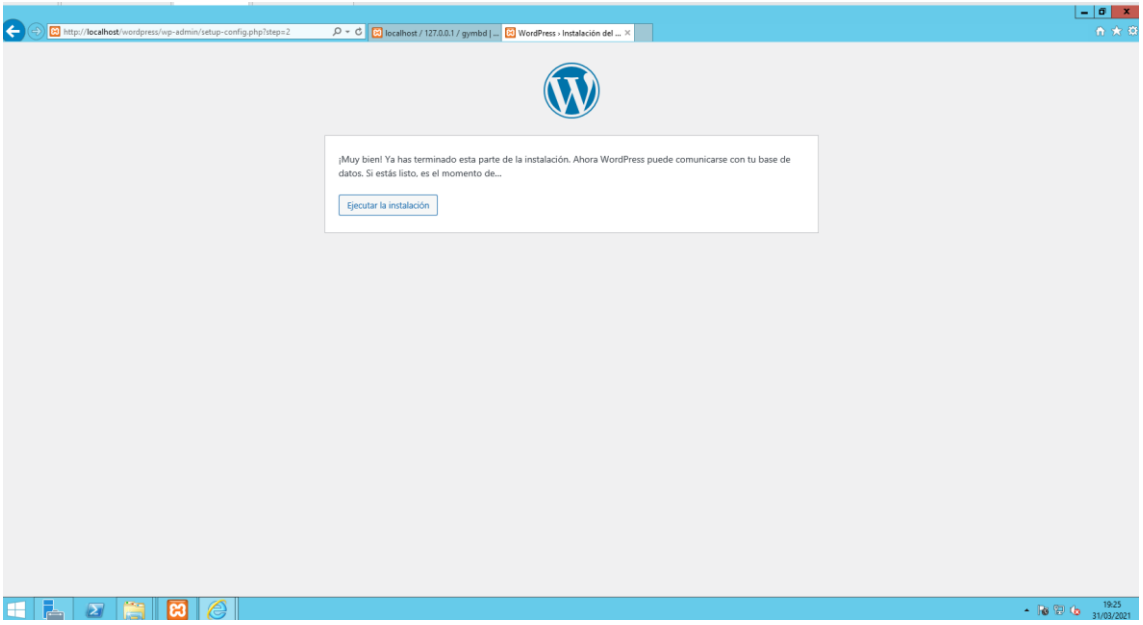

Figura 74. Ventana de ejecución de instalación.

Si nos fijamos en la Figura 75, en la siguiente ventana tenemos que rellenar los datos para la instalación de WordPress, como el título del nuevo sitio, el nombre del usuario utilizarás para administrarlo, la contraseña, etc. Una vez rellenado los datos haremos clic a Instalar WordPress.

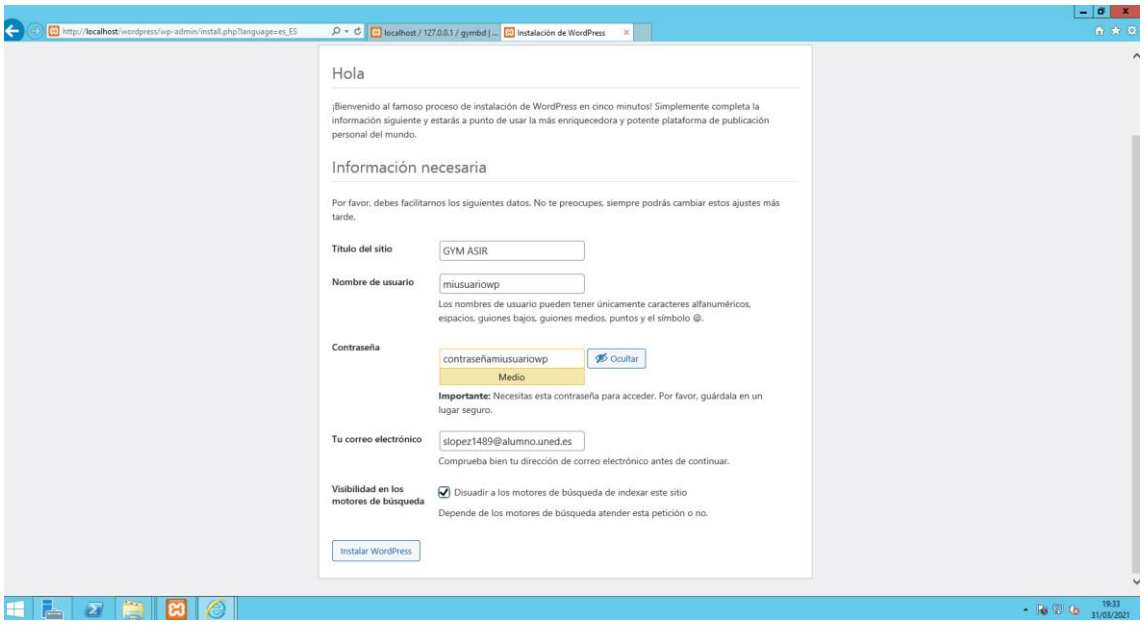

Figura 75. Datos a introducir sobre nuestro WordPress.

Ya lo tenemos instalado. Haremos clic en el botón Acceder para ir a la ventana de login del WordPress. Usamos el nombre de usuario y la contraseña que elegimos antes. Haremos clic en el botón Acceder y entraremos al escritorio del WordPress.

Para acceder y ver cómo queda el sitio lo haremos desde http://localhost/wordpress/

Para acceder al escritorio y configurarlo a nuestro gusto lo haremos desde http://localhost/wordpress/wp-login.php

6.4.2 Puerto 80, URL y CNAME

Una vez instalado, tenemos que abrir el puerto 80 del firewall de nuestro servidor web para que podamos visualizarlo desde cualquier host de nuestra red lan.

Para ello accederemos a Panel de control\Sistema y seguridad\Firewall de Windows y haremos clic en configuración avanzada.

Una vez dentro, daremos a nueva regla desplegando la ventana como la que aparece en la Figura 76 y seleccionaremos la opción puerto.

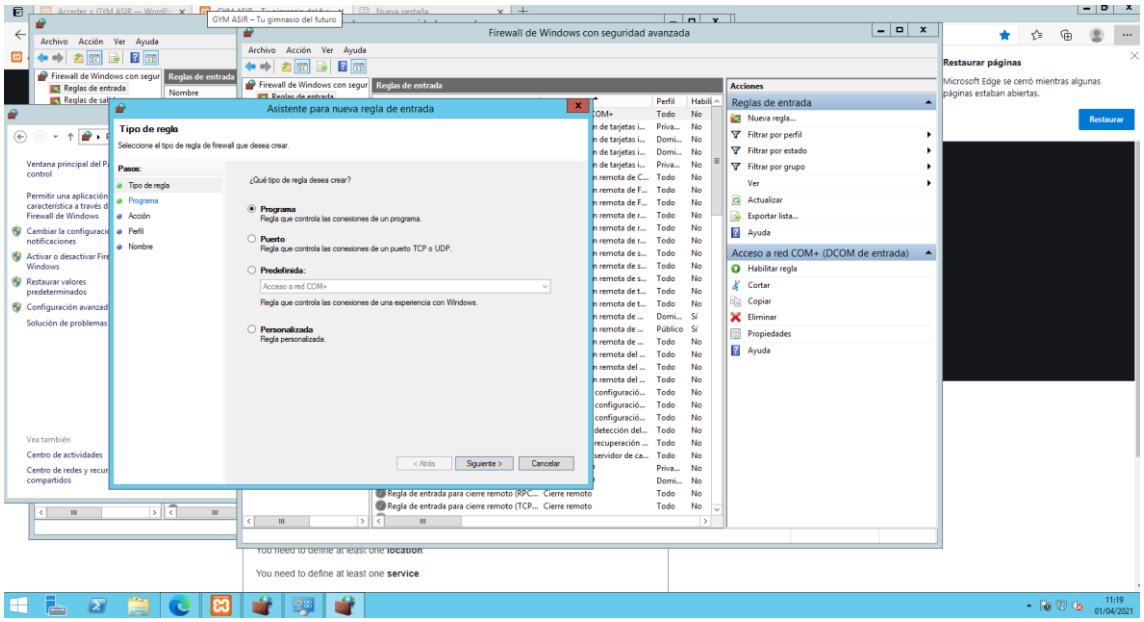

Figura 76. Asistente de regla de entrada.

En la siguiente ventana seleccionaremos TCP, pondremos 80 en los puertos locales específicos como muestra Figura 77 y daremos a siguiente.

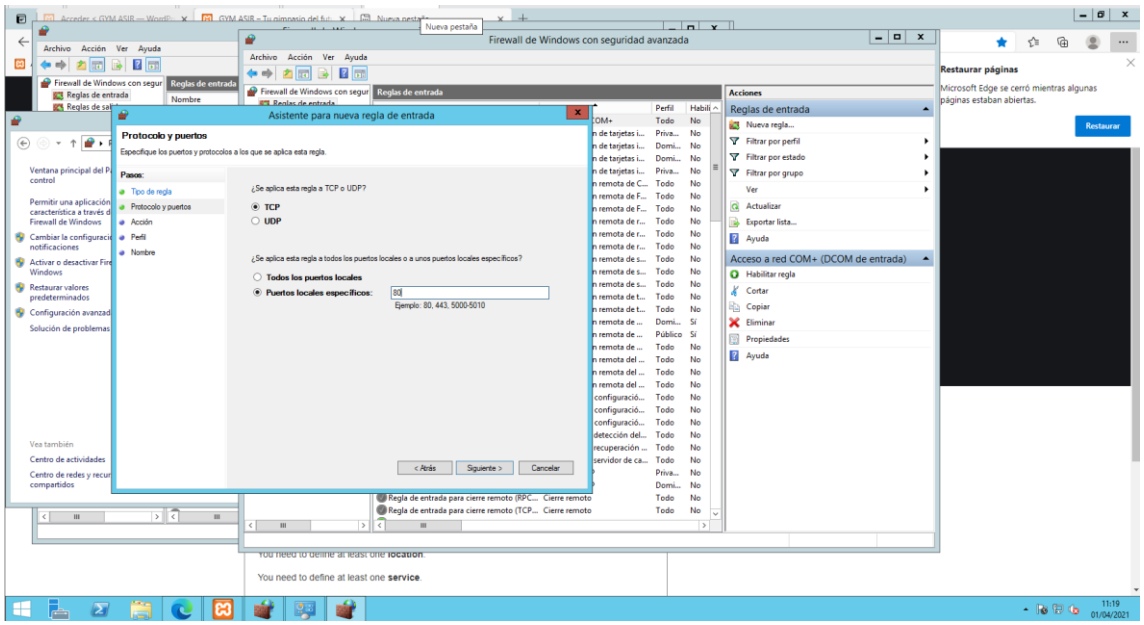

Figura 77. Selección de TCP/UDP.

Al igual que lo que muestra la Figura 78, aparecerá la siguiente opción y daremos a permitir la conexión y siguiente.

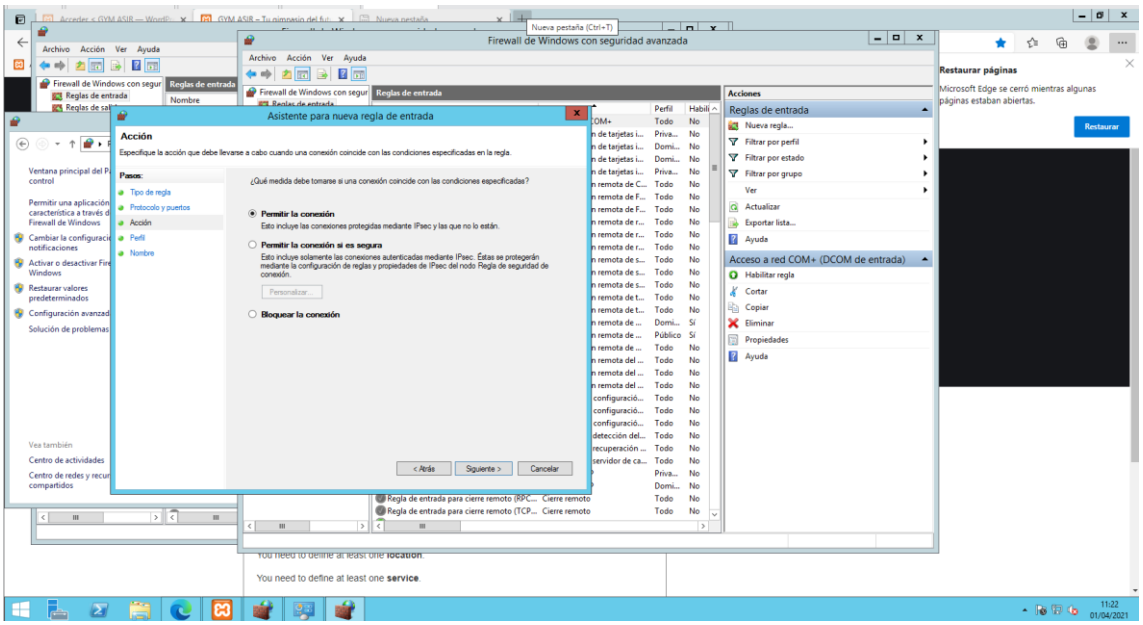

Figura 78. Selección de acción.

En la siguiente opción seleccionaremos las opciones dominio y privado. Haremos clic en siguiente.

Nos solicitará un nombre y una descripción, en el que pondremos puerto 80 para tener localizada la regla de entrada y le daremos a finalizar.

La siguiente opción que queremos es que accedamos desde cualquier host únicamente con la dirección http://reservas

Para ello vamos a realizar los siguientes cambios:

Moveremos los archivos que se encuentran en la dirección C:\xampp\htdocs\wordpress a la dirección C:\xampp\htdocs y eliminando la subcarpeta.

En nuestro servidor controlador de dominio iremos a Administrador del Servidor->Herramientas->DNS.

En la barra de la izquierda desplegaremos el servidor y las zonas de búsqueda directa.

Como muestra la Figura 79, haremos clic en el botón derecho del ratón en gym.local y seleccionaremos Alias Nuevo (CNAME).

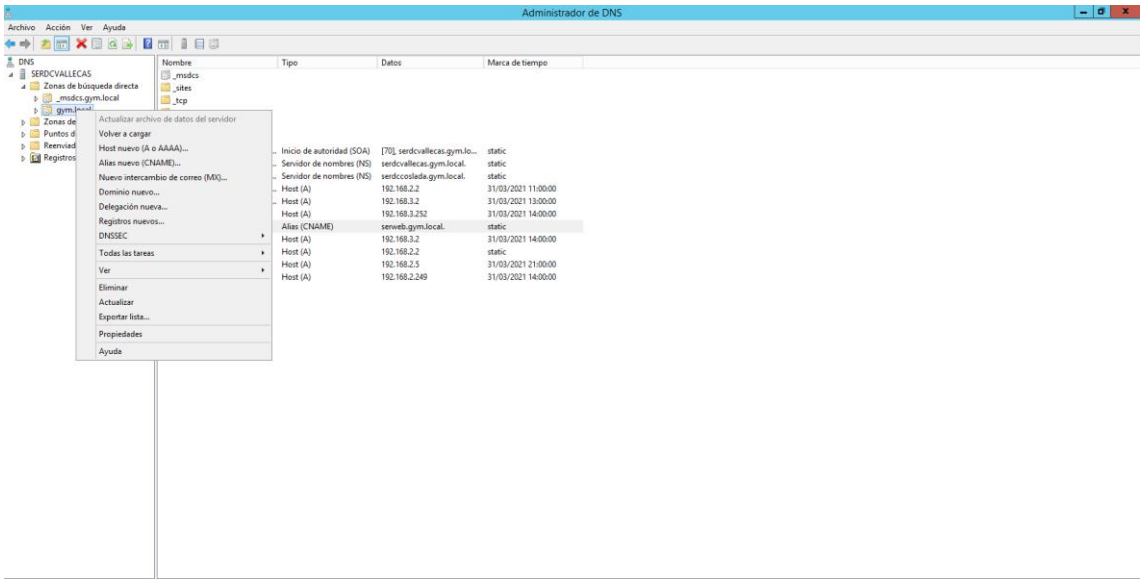

Figura 79. Zona de búsqueda directa en el DNS.

En la ventana siguiente lo configuraremos con los datos que refleja la Figura 80.

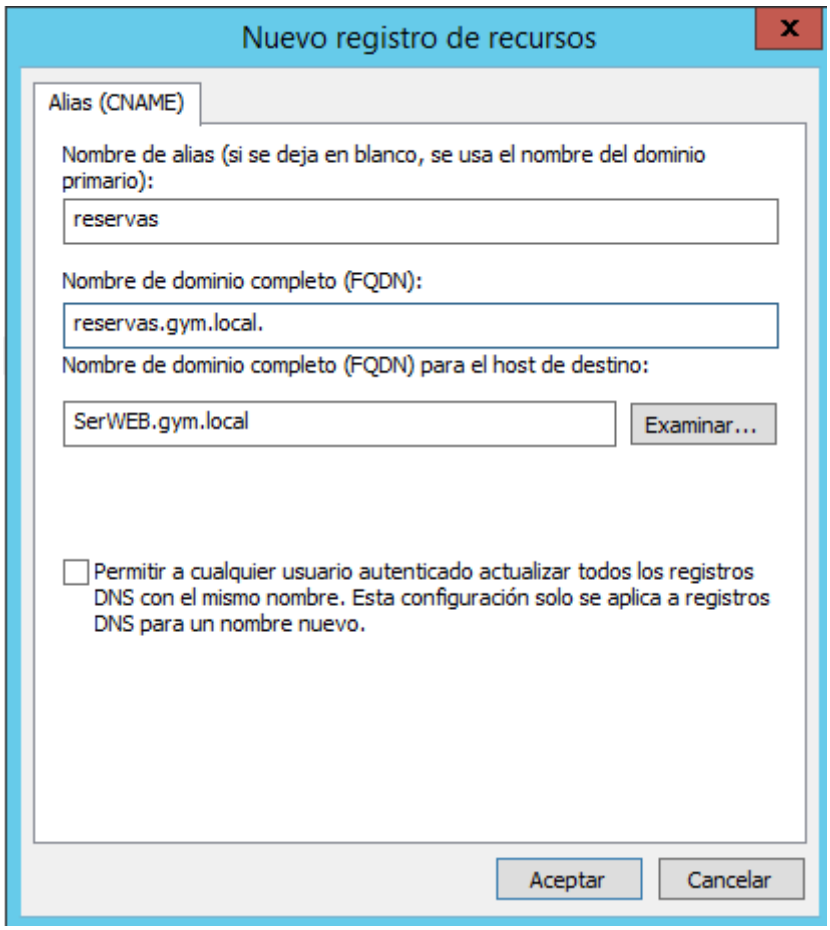

Figura 80. Creación del registro CNAME.

Nos queda cambiar la URL desde el WordPress. Para ello accedemos a http:// localhost/wordpress/wp-admin/ entramos en nuestro escritorio de WordPress.

Una vez dentro, en ajustes->general vamos a modificar los datos como se muestra en la Figura 81 y le damos a guardar. Con estos pasos ya estaría cambiado.

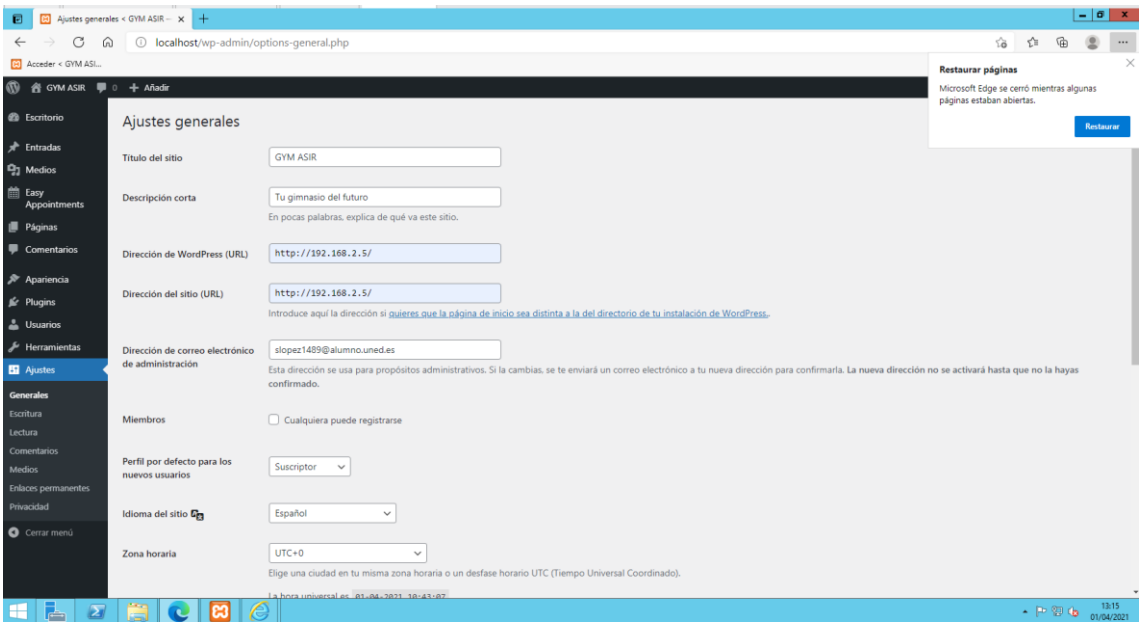

Figura 81. Cambio de URL.

A partir de ahora, para acceder y ver cómo queda el sitio lo haremos desde http://reservas

Para acceder al escritorio y configurarlo a nuestro gusto lo haremos desde http://reservas/wp-login.php

6.4.3 Apariencia de la página web y reserva de citas

Una vez terminada de instalar nuestra página, nos centraremos en la apariencia y configuración de dicha página.

Para ello lo primero que vamos a realizar es gestionar los temas.

Los temas son plantillas estéticas que determinan su apariencia y su funcionalidad.

En el caso concreto de esta página se ha elegido el tema Hiero por su gratuidad y por ser sencillo a la hora de trabajar con él.

Para ello, una vez dentro de nuestro escritorio de WordPress, lo que haremos será acceder a apariencia->temas visualizando lo mismo que la Figura 82. Haremos clic a añadir nuevo, lo buscaremos y le daremos a instalar. Una vez instalado lo activaremos para que surjan efecto los cambios.

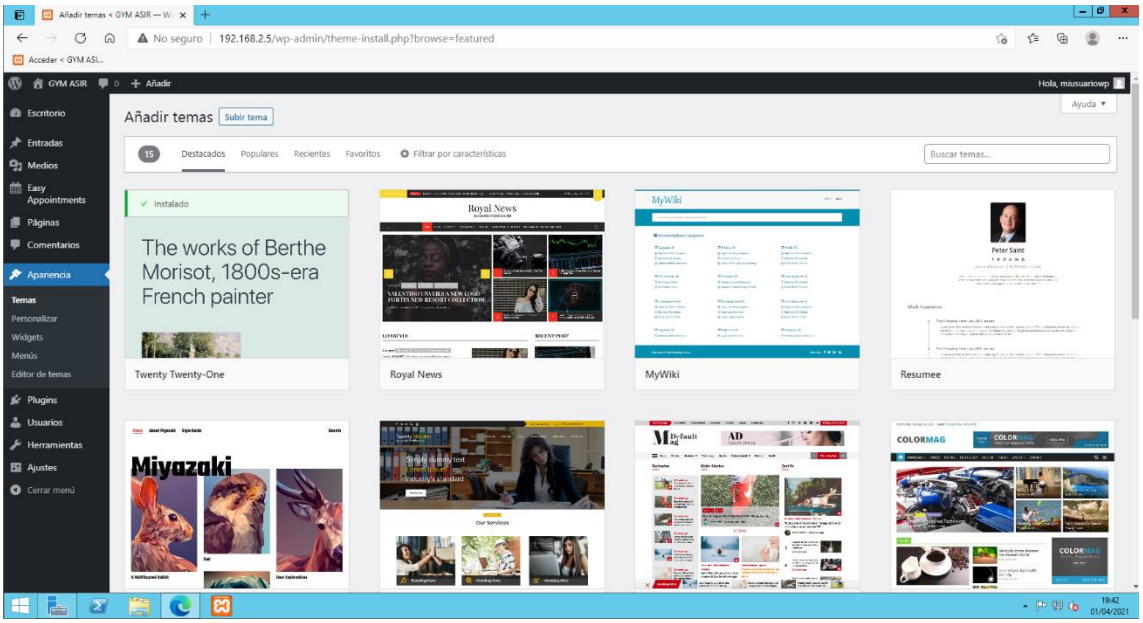

Figura 82. Temas de WordPress.

Una vez introducidos los cambios descargaremos el plugin para la reserva de las salas.

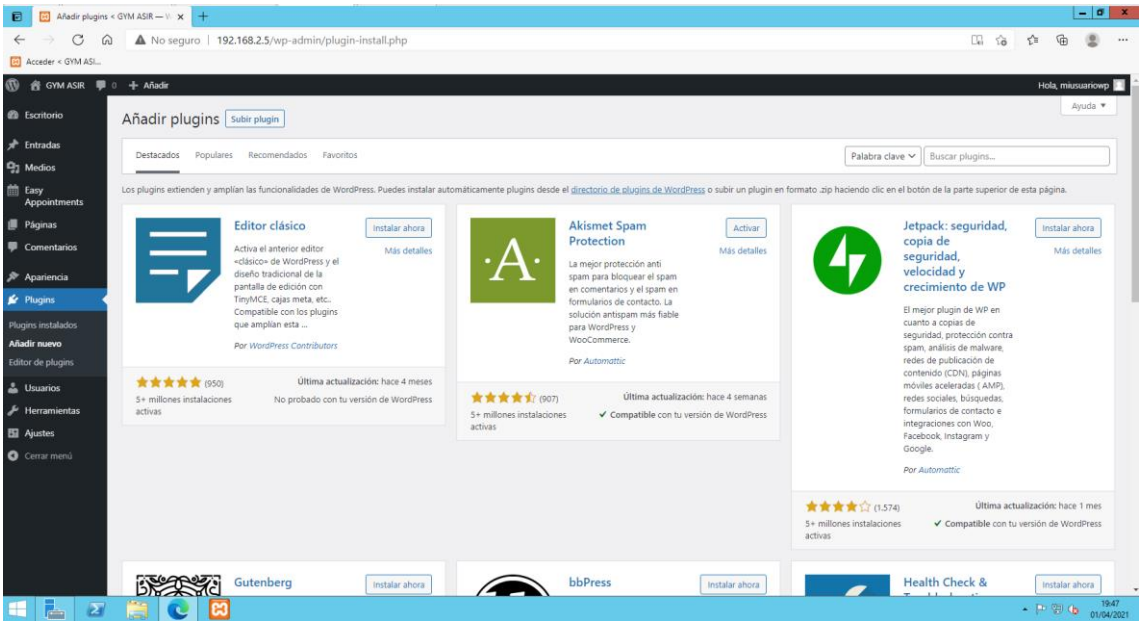

Figura 83. Plugins de WordPress.

En nuestro caso hemos elegido el plugin Easy Appointments.

Para ello iremos a Plugins->Añadir nuevo visualizando algo similar a lo que muestra la Figura 83. Lo buscaremos y le daremos a instalar ahora. Una vez instalado lo activaremos como vemos en la Figura 84 y aparecerá en la parte izquierda de la pantalla el menú para configurarlo.

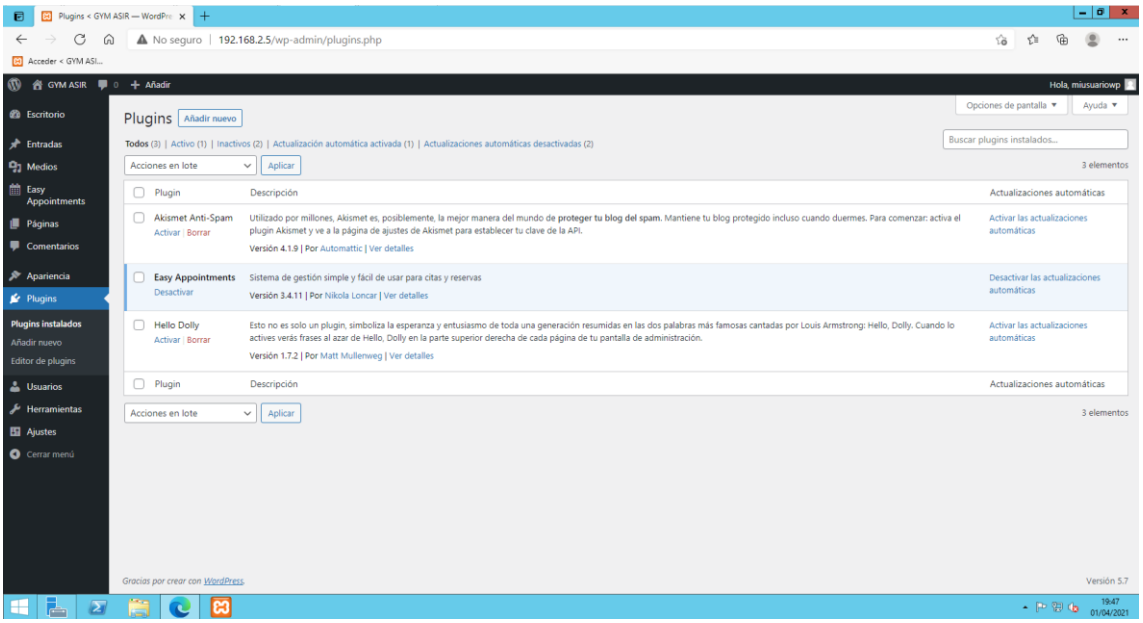

Figura 84. Activación/Desactivación de Plugins.

Como muestra la Figura 85, lo configuraremos con todos nuestros datos. Tanto de trabajadores, ubicaciones, máximo de reservas, etc.

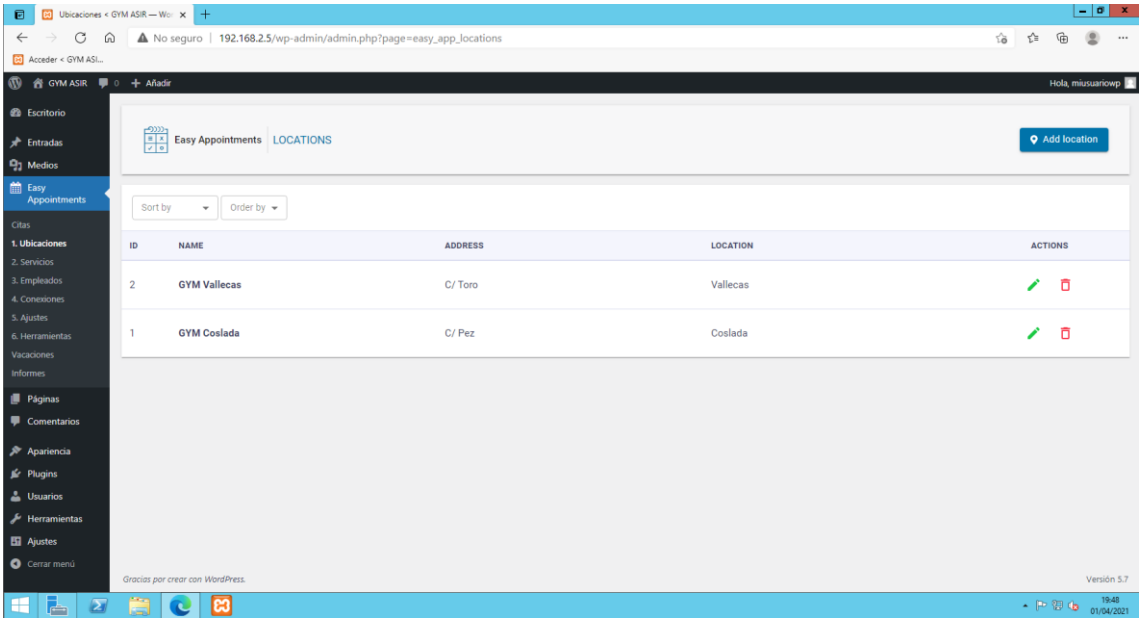

Figura 85. Configuración de Easy Appointment.

También existe posibilidad de configurarlo para que envíe correos de confirmación a los usuarios y a los empleados, aunque no se configurará en este proyecto.

Una vez configurado los parámetros, iremos a páginas y haremos clic a añadir una nueva página.

Configuraremos la página a nuestro gusto como vemos en la Figura 86, pero tendremos que añadir el comentario [ea_bootstrap width=»800px» scroll_off=»true» layout_cols=»2”] para poder visualizar nuestro pluging de citas.

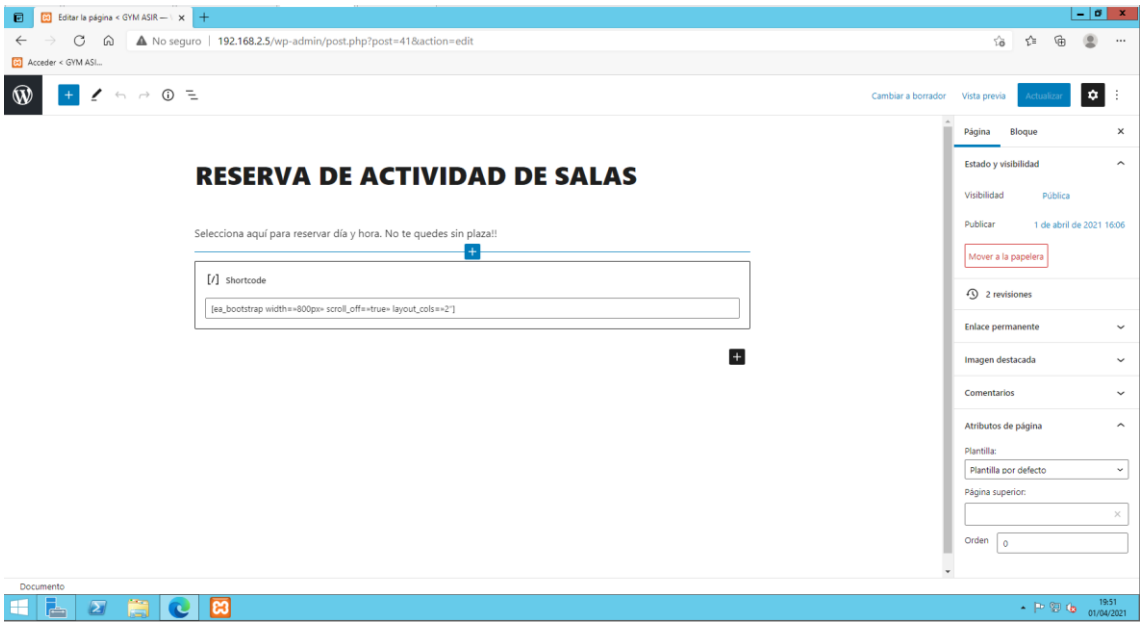

Figura 86. Creación página principal.

Una vez creada la página, lo que haremos será establecer nuestra página de una manera estática para que sea lo que muestra nuestra página de inicio. Para ello nos iremos a Ajustes-> Lectura y estableceremos como portada nuestra página creada igual que en la Figura 87.

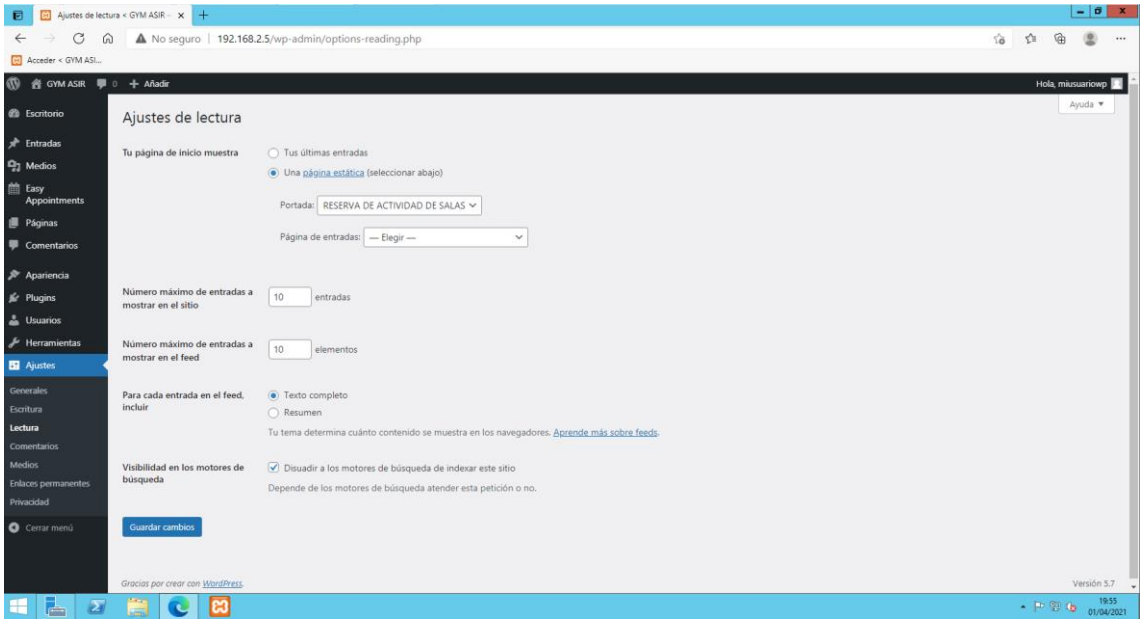

Figura 87. Asignación de página estática.

Por último, ajustaremos nuestra página a nuestro gusto, introduciendo alguna imagen o color. Para realizarlo, tendremos que ir a Apariencia->Personalizar, modificando lo que queremos visualizar quedando como en la Figura 88.

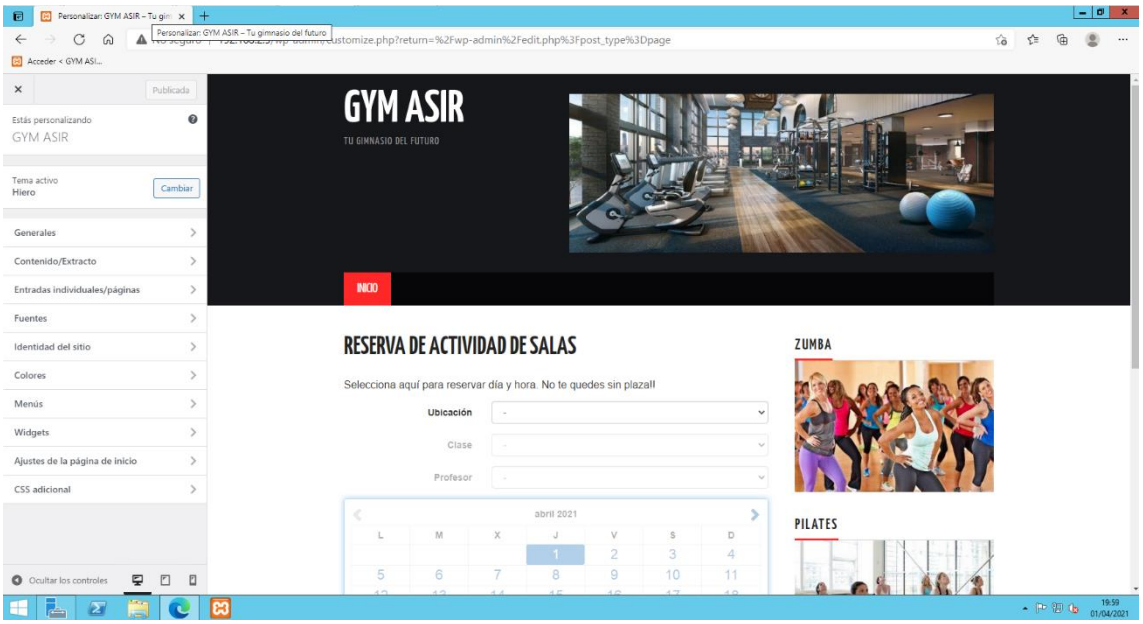

Figura 88. Personalización de nuestro WordPress creado.

Si quisiéramos visualizar las citas, tendríamos que entrar en Easy Appointment en el apartado citas y filtrar según queramos ver.

Esas visualizaciones con las citas se pueden exportar por si quisiéramos entregárselo a los monitores de cada actividad.

6.5 Instalación y configuración Servidor OwnCloud

Para poder gestionar las tablas de los usuarios y sus rutinas necesitamos en servicio que pueda almacenarlas y compartirlas con los usuarios que necesitemos para cada caso.

Esta gestión se podría llevar a cabo a través de variadas y múltiples herramientas que hay disponibles en el mercado, como por ejemplo Dropbox.

Para este proyecto se ha decido utilizar el servicio de OwnCloud.

A diferencia de Dropbox, Owncloud se instala en nuestro propio servidor, garantizando así la privacidad y la seguridad, con total independencia de servicios externos.

Además, OwnCloud cuenta con diversos módulos para implementar mejoras pudiendo compartir contenido con URL públicas si fuera necesario.

Para su correcta implantación será necesario realizar dos pasos: Instalar el servidor de OwnCloud y, a través de un administrador, configurar correctamente los usuarios y demás administradores que pudiéramos necesitar.

A continuación, se detallan los dos pasos a seguir.

6.5.1. Instalación OwnCloud Server

Para este apartado vamos a utilizar la máquina virtual que tiene el desarrollador para implementar este servidor en máquina virtuales. Bastará con descargar el archivo para VMWARE como muestra la Figura 89 desde la página https://owncloud.com/es/descarguese-el-servidor/

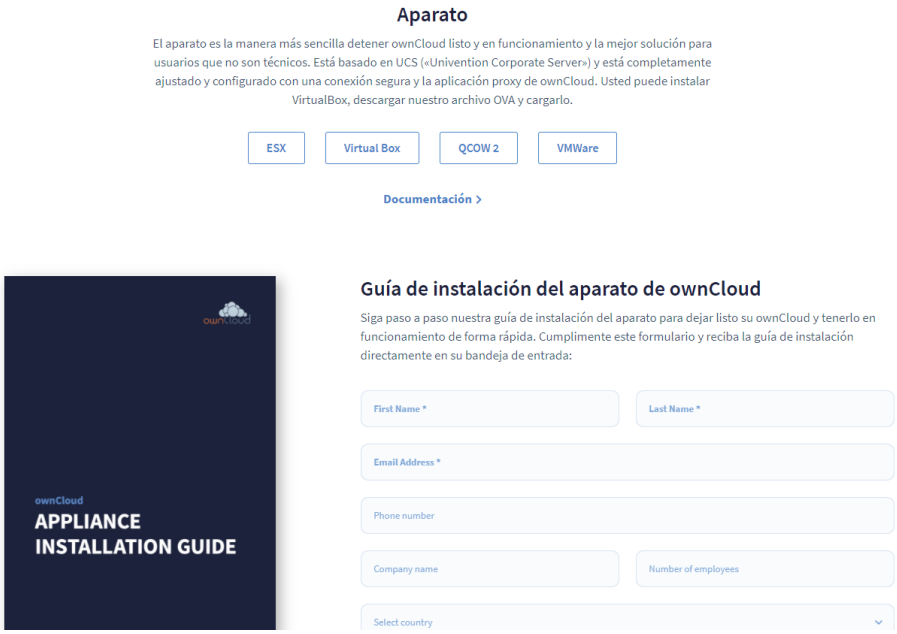

Figura 89. Página de OnwCloud para realizar la descarga.

Una vez alojada en nuestra máquina virtual, arrancaremos la máquina y empezaremos a configurarlo con nuestros parámetros.

La primera ventana que nos aparece tendremos que seleccionar el idioma y nuestra ciudad. Lo dejaremos como la Figura 90 y haremos clic en siguiente.

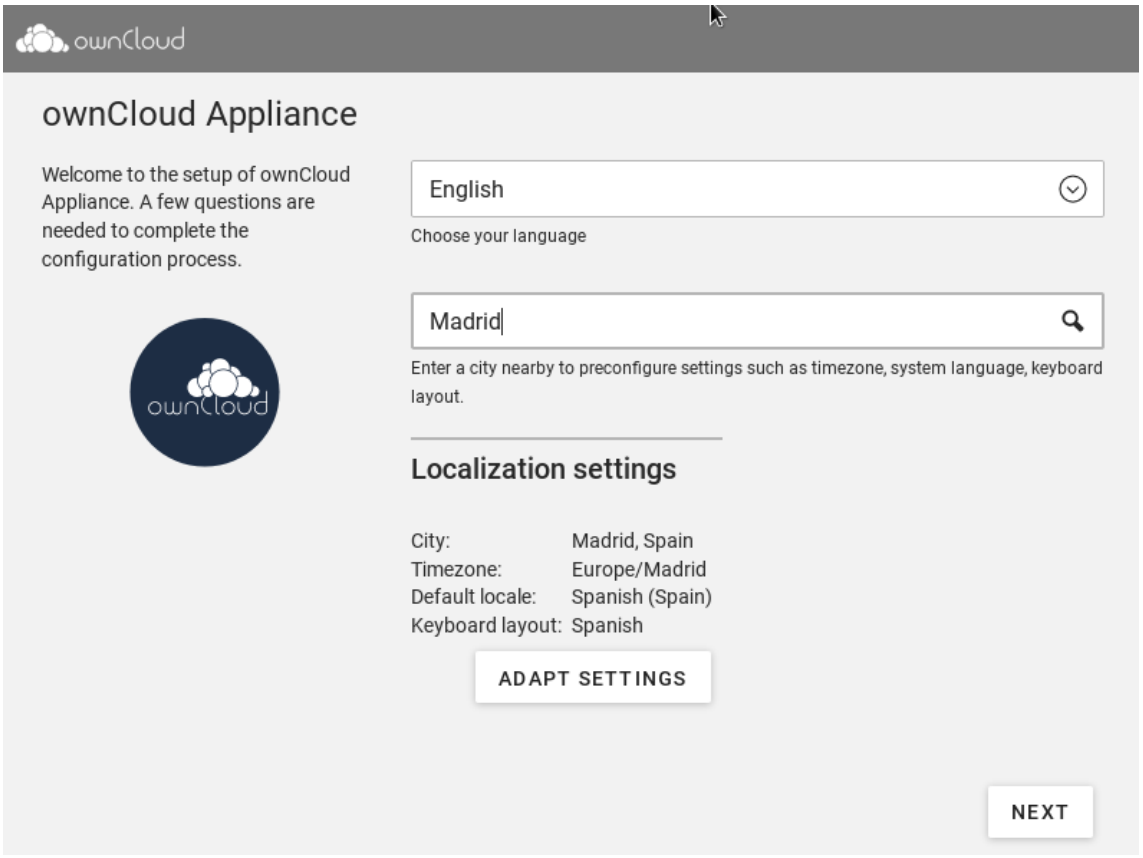

Figura 90. Selección de idioma y ciudad.

En la siguiente ventana, deshabilitaremos la opción obtener la dirección IP automáticamente por DCHP y asignaremos la que nosotros queremos, añadiendo la máscara, la puerta de enlace y los servidores DNS que queremos para nuestro sistema, quedamos como en la Figura 91. Daremos a next.

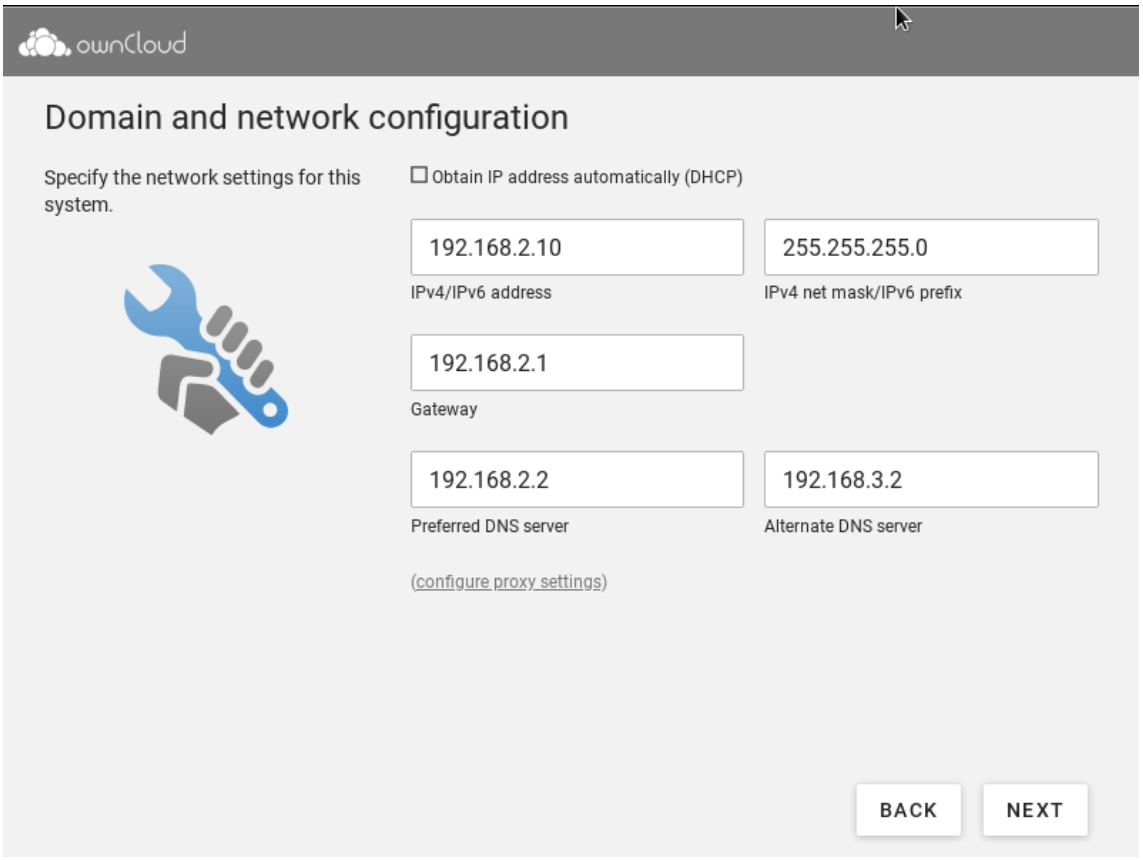

Figura 91. Configuración de IP, máscara, puerta de enlace y DNS.

En la siguiente pantalla nos solicitará las opciones del dominio como muestra la Figura 92. Nosotros seleccionaremos unirnos a un dominio existente de Microsoft Active Directory. Pulsaremos Next.

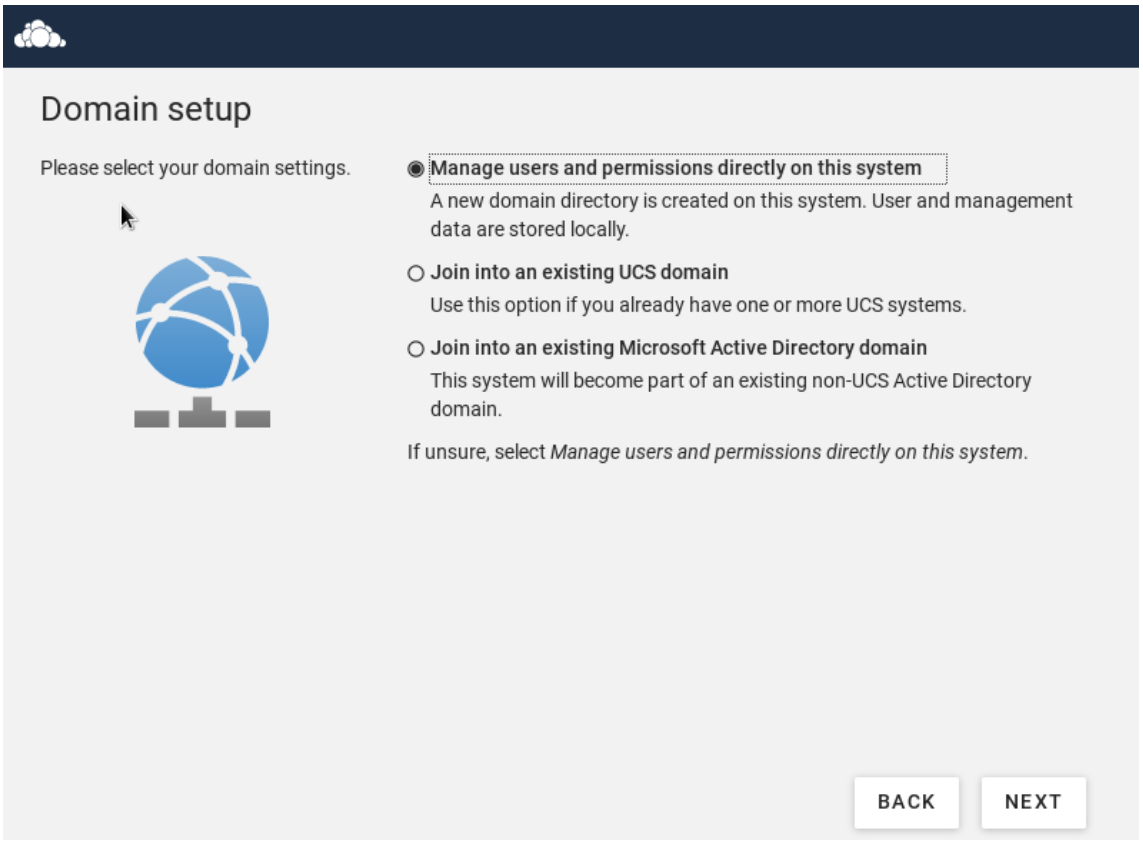

Figura 92. Selección de las opciones de dominio.

Seguidamente nos solicitará el nombre del dominio y unas credenciales de Administrador para poder ingresar en dicho dominio. Como en la Figura 93, rellenamos y pulsamos siguiente.

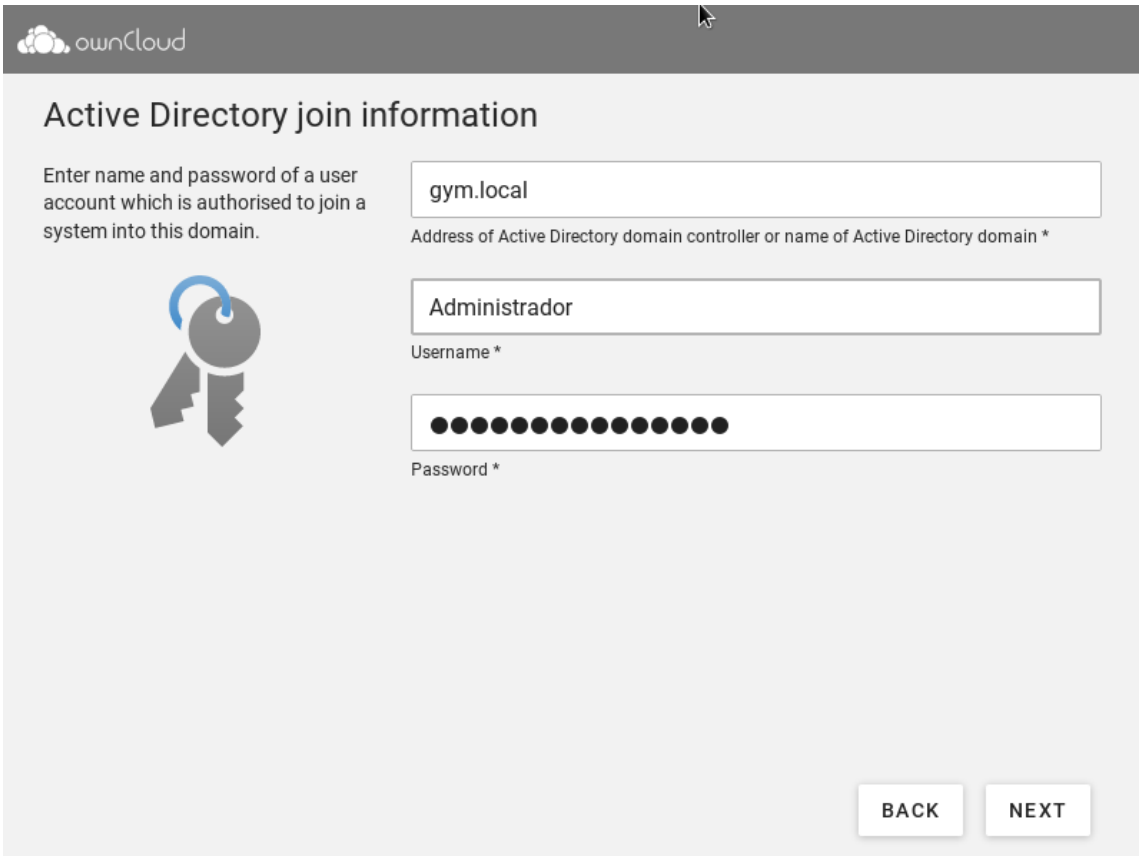

Figura 93. Introducción de dominio, usuario y contraseña.

Nos solicitará el nombre para nuestro nuevo servidor y una contraseña para el local root. Como en la Figura 94, introduciremos los datos y haremos clic en Netx.

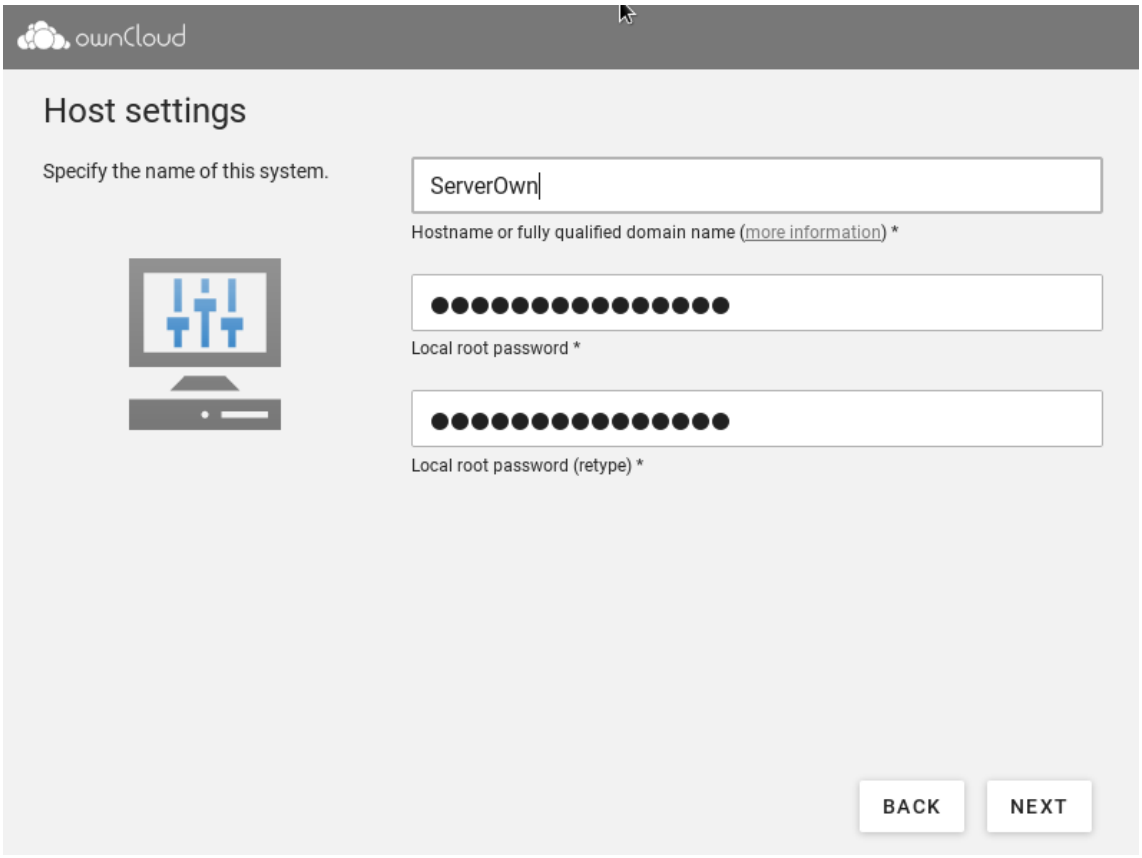

Figura 94. Nombre de nuestro servidor y contraseña.

Por último, se visualizará un resumen con todas las opciones que hemos completado. Le daremos a configure system y empezará el proceso de configuración del servidor como vemos en la Figura 95.

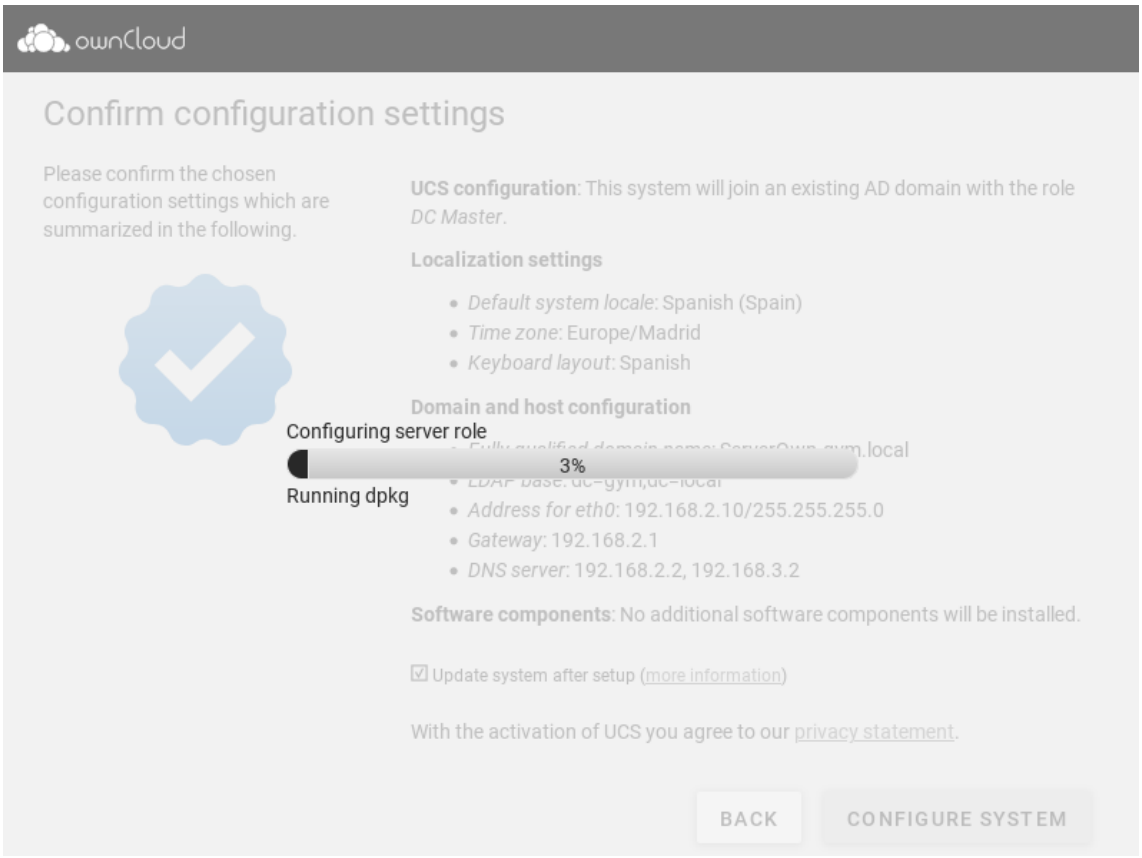

Figura 95. Proceso de configuración.

Cuando haya terminado nos mostrará una pantalla diciendo que el proceso ha sido válido idénticamente a lo mostrado en la Figura 96.

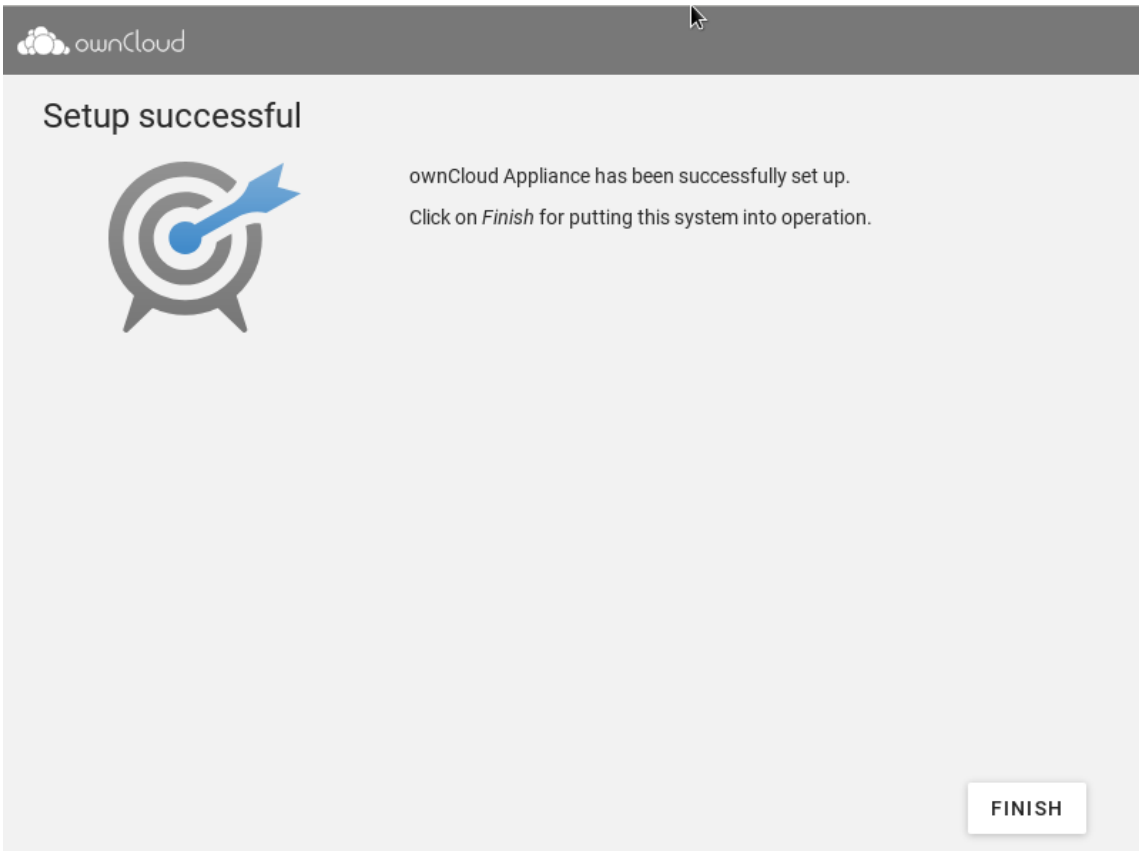

Figura 96. Finalización correcta de la configuración.

Al hacer clic en finish, desplegará una ventana para darnos las instrucciones de como acceder al OwnCloud. Como vemos en la Figura 97, tendremos que introducir la dirección del servidor.

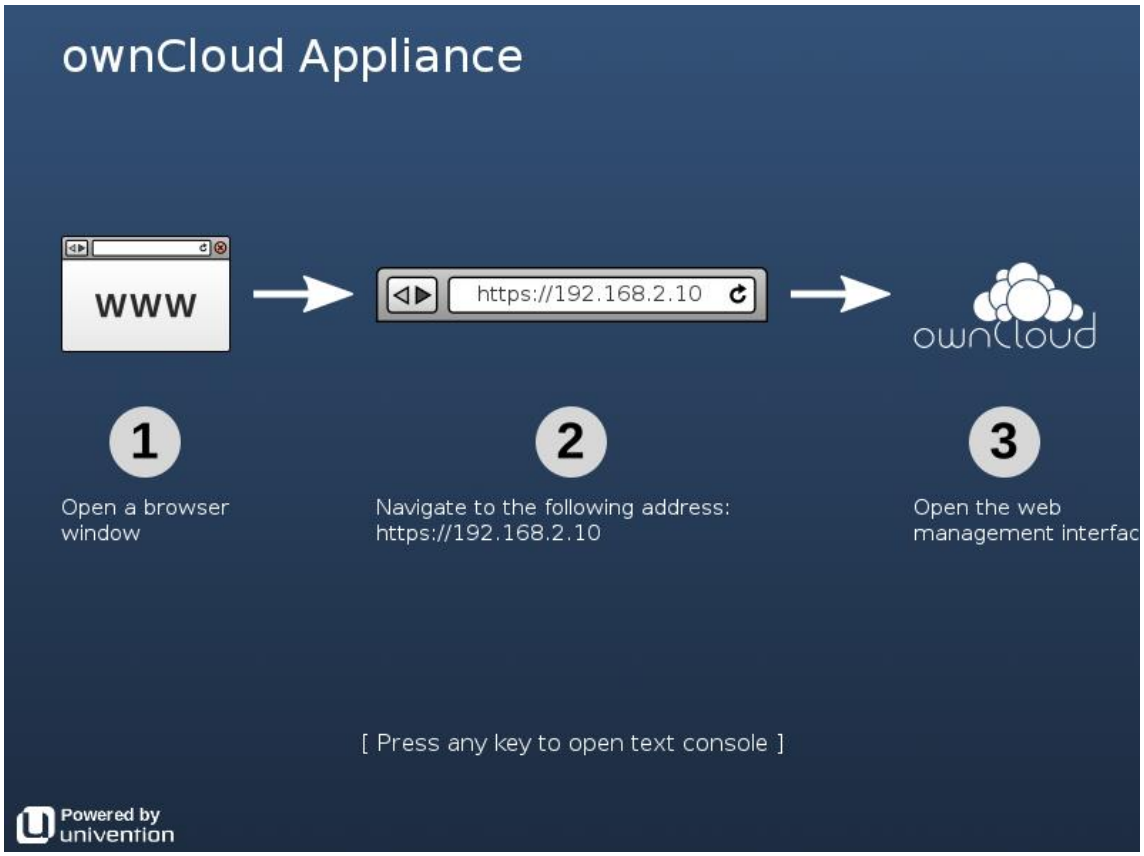

Figura 97. Instrucciones finales para acceder.

El siguiente paso, será irnos a un host. Abrimos nuestro navegador e introducimos la dirección donde se encuentra alojado el servidor OwnCloud. Nos solicitará un correo electrónico para poder activarlo como lo mostrado en la Figura 98.

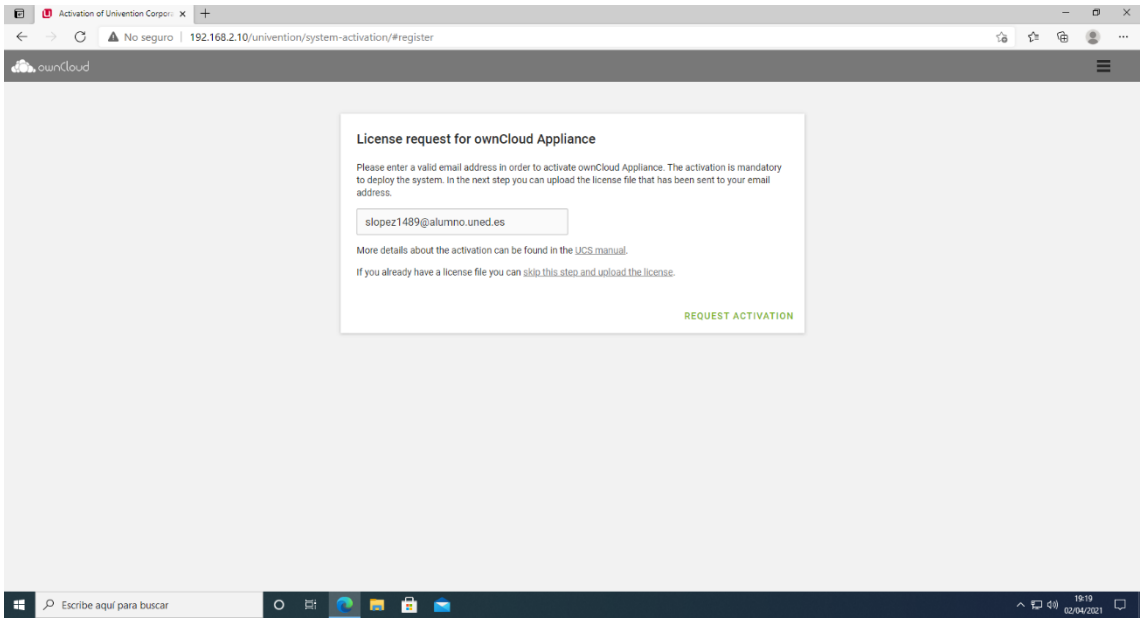

Figura 98. Ventana que muestra al introducir la dirección del servidor.

Nos enviará un correo con un archivo adjunto que tendremos que cargar en la ventana de la Figura 99.

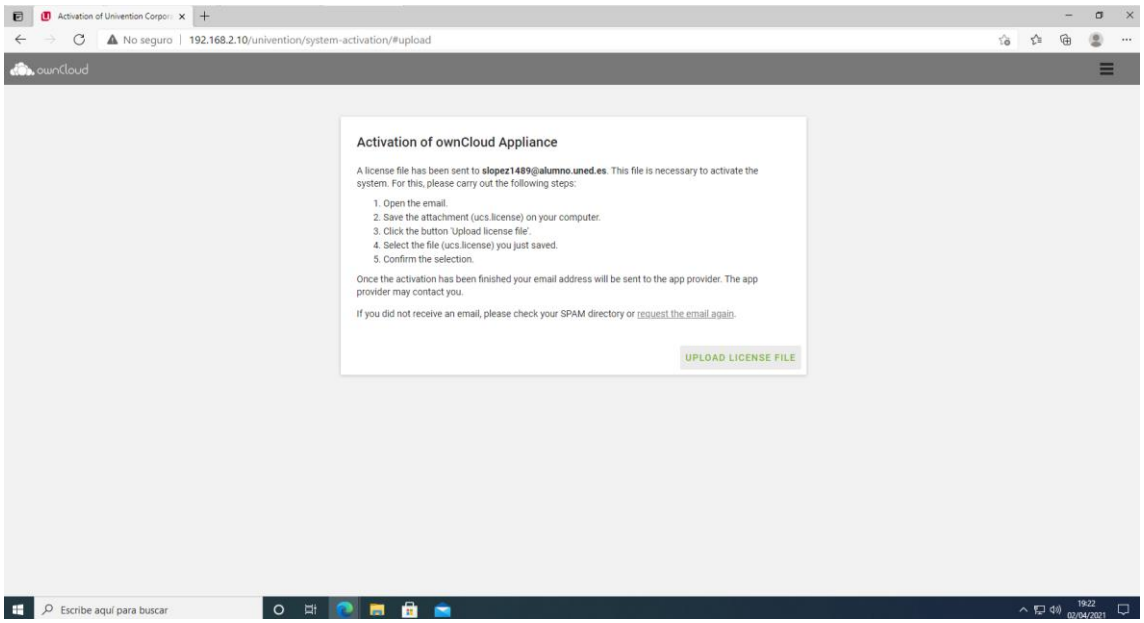

Figura 99. Ventana para poder cargar el archivo adjunto.

Una vez subido ya estará activado y podemos acceder a nuestro servidor OwnCloud creado, visualizando lo mostrado en la Figura 100.

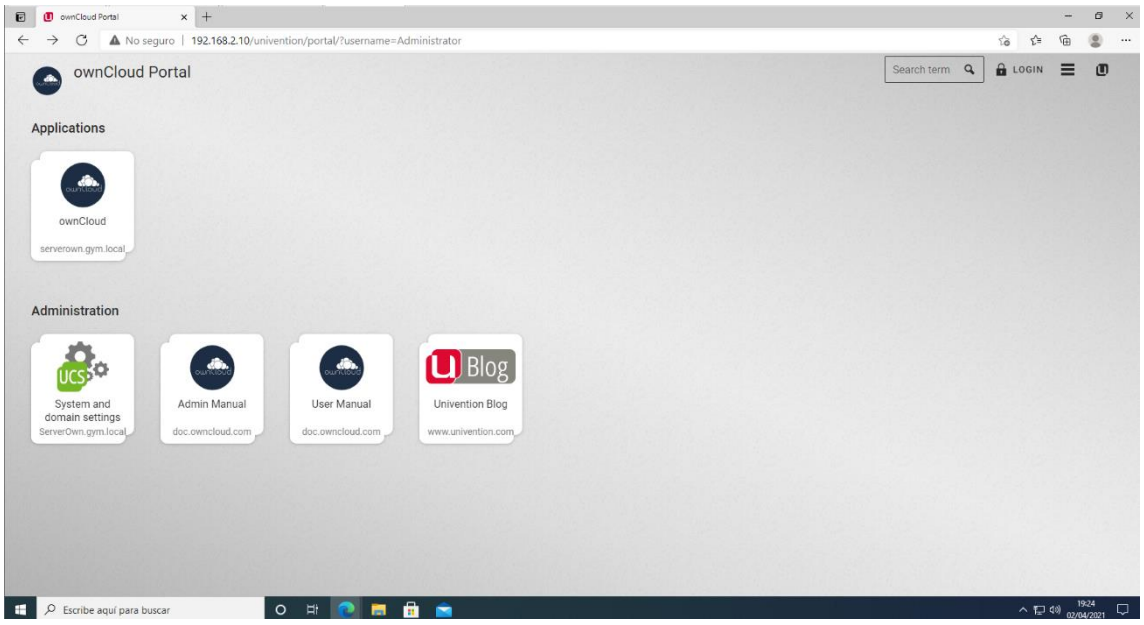

Figura 100. Ventana principal al acceder a http://192.168.2.10/

Para que el acceso sea más intuitivo para el cliente, al igual que el servidor web, haremos cambios en nuestro DNS.

En nuestro servidor controlador de dominio iremos a Administrador del Servidor->Herramientas->DNS.

En la barra de la izquierda desplegaremos el servidor y las zonas de búsqueda directa.

Haremos clic en el botón derecho del ratón en gym.local y seleccionaremos Alias Nuevo (CNAME).

Lo configuraremos como indica la Figura 101.

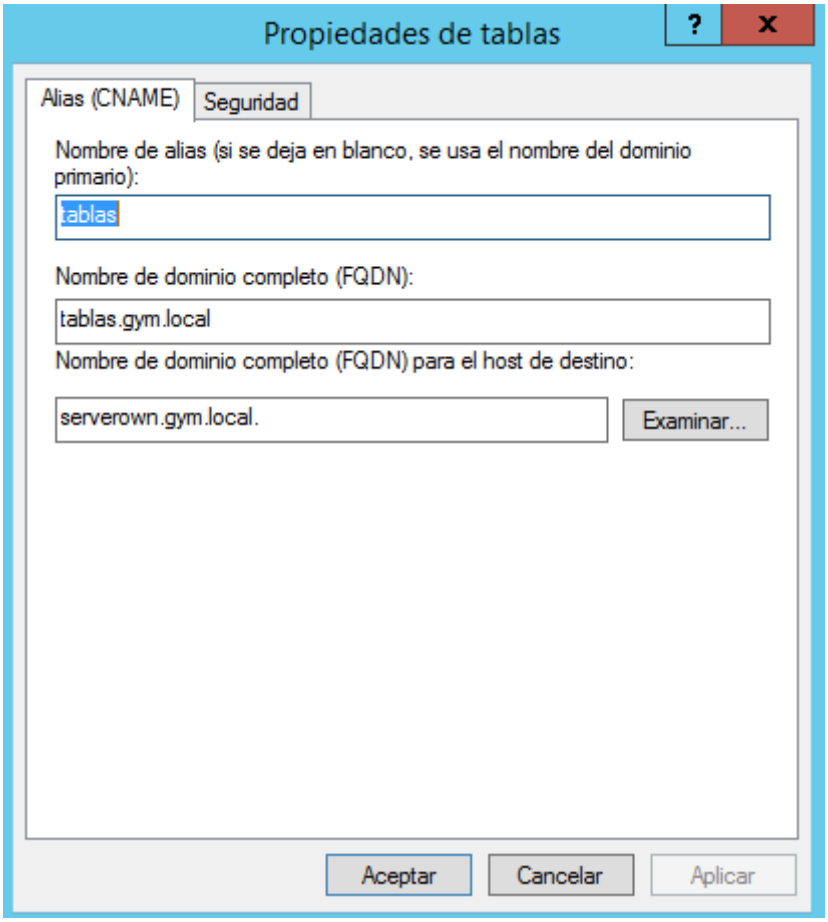

Figura 101. Creación de CNAME para Owncloud.

Una vez realizado el cambio podemos acceder de dos formas a nuestro OwnCloud, a través de una aplicación cliente instalada en el equipo que va a usarlo o vía navegador.

Se decide esta última ya que no requiere ninguna instalación.

Para ello sólo nos queda acceder a nuestro OwnCloud introduciendo la dirección http://tablas/owncloud

6.5.2. Configuración de administrador y clientes de OwnCloud.

Igual que en la Figura 102, al acceder a OwnCloud, lo primero que nos solicita es un usuario y una contraseña.

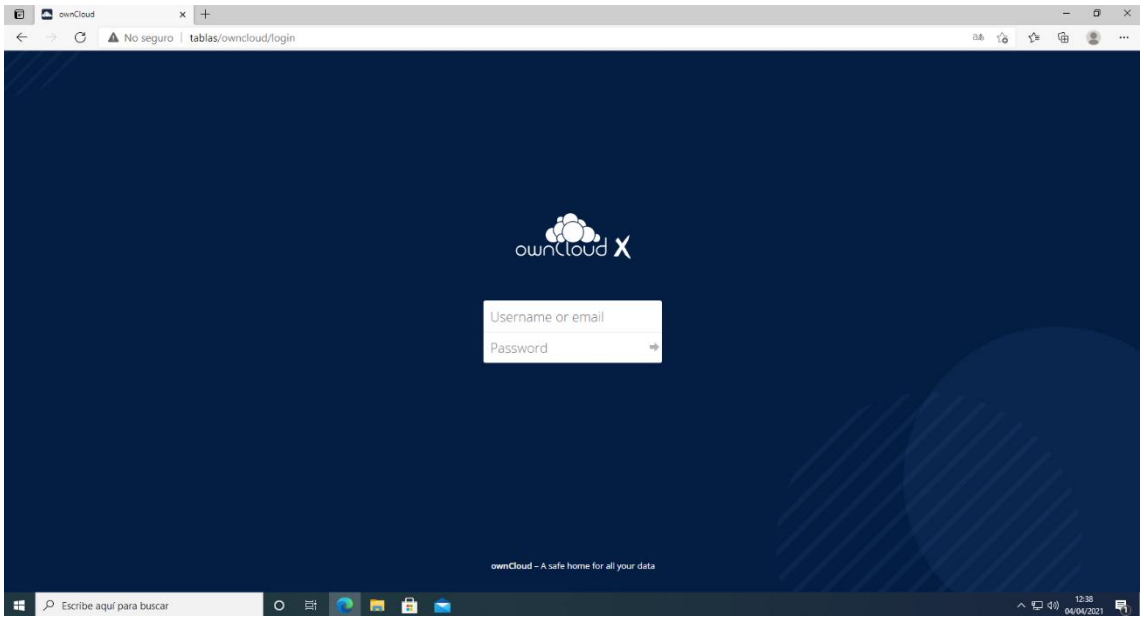

Figura 102. Acceso a OwnCloud.

Tal y como indica el desarrollador, por defecto el usuario y la clave será OwnCloud. Pertenecerá al grupo de administradores.

Al introducirla nos mostrará la pantalla principal que vemos en la Figura 103.

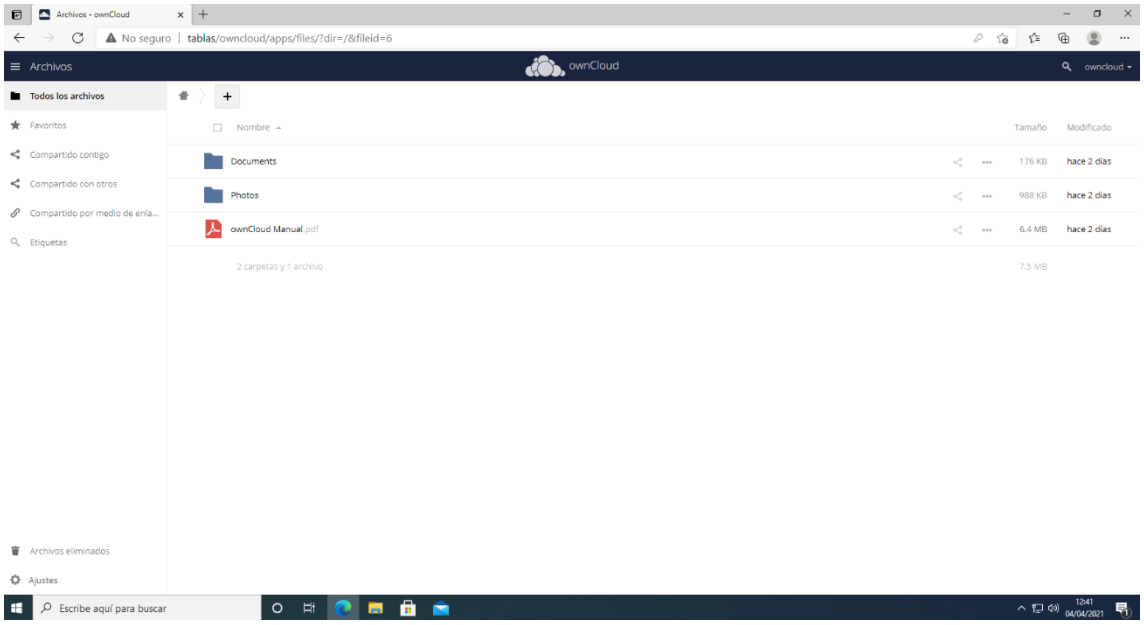

Figura 103. Pantalla principal de OwnCloud.

En el menú derecho, haciendo clic en ajustes, podemos introducir los datos del administrador, visualizando la Figura 104.

Este administrador será el encargado de introducir nuevos usuarios. También será el encargado de asignar espacio y delimitar los archivos que puede visualización de cada usuario.

También se pueden configurar varias opciones como envío de correos, que este proyecto no tratará.

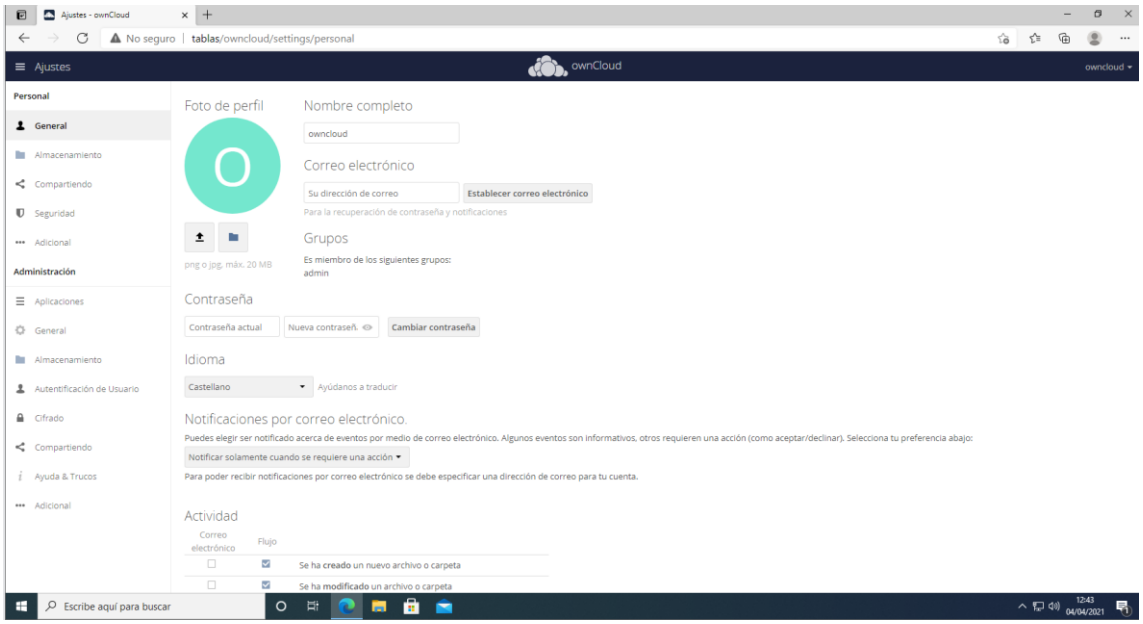

Figura 104. Pantalla de ajustes del administrador.

Igualmente, en el menú derecho podemos acceder a los usuarios.

Una vez dentro, como muestra la Figura 105, podemos ver los usuarios que pueden utilizar nuestro servidor.

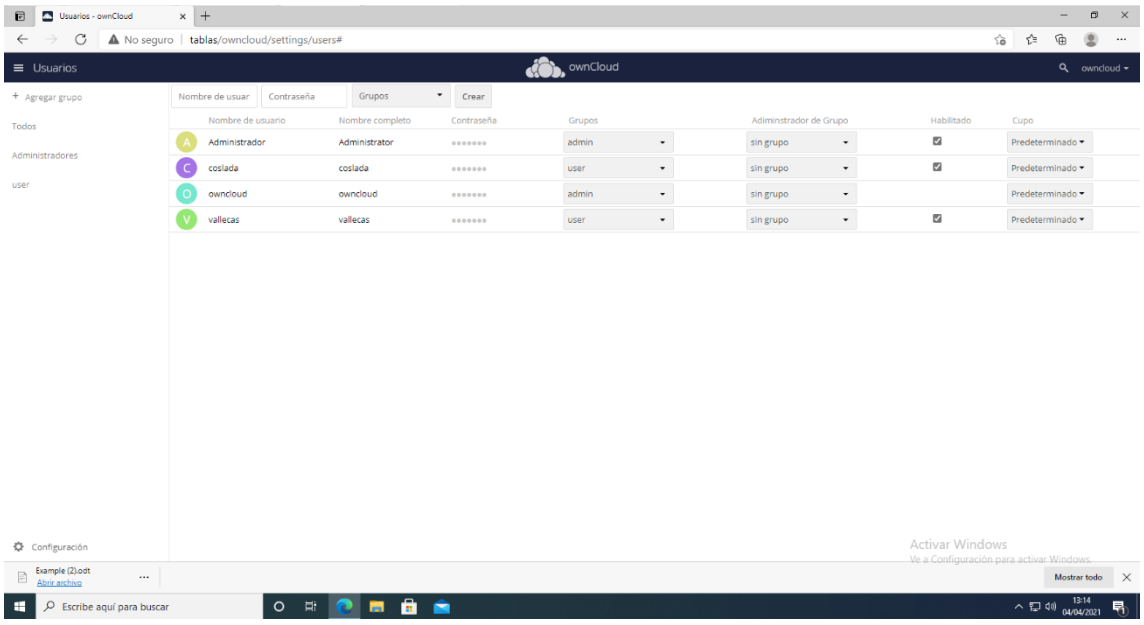

Figura 105. Pantalla de usuarios.

Se establece una jerarquía mediante grupos, a través de la cual otorgamos permisos según sea la necesidad.

Si nos fijamos en la parte superior, tenemos unas casillas para introducir nuevos usuarios. Podremos su nombre, su contraseña y el grupo al que pertenecen. Si no estuviera creado podemos crear el nuevo grupo. Además, si queremos se puede hacer que sea el administrador de su grupo.

En nuestro caso únicamente hemos creado dos clientes, uno por gimnasio, pero pueden ser tantos como usuarios queramos por gimnasio.

Una vez creado los clientes, nos vamos al menú de la derecha y hacemos clic en Archivos.

En esta ventana podemos ver los archivos que tenemos.

Por defecto vienen ya creadas algunas carpetas y archivos. En nuestro caso vamos a crear dos carpetas, una para cada gimnasio como podemos ver en la Figura 106.

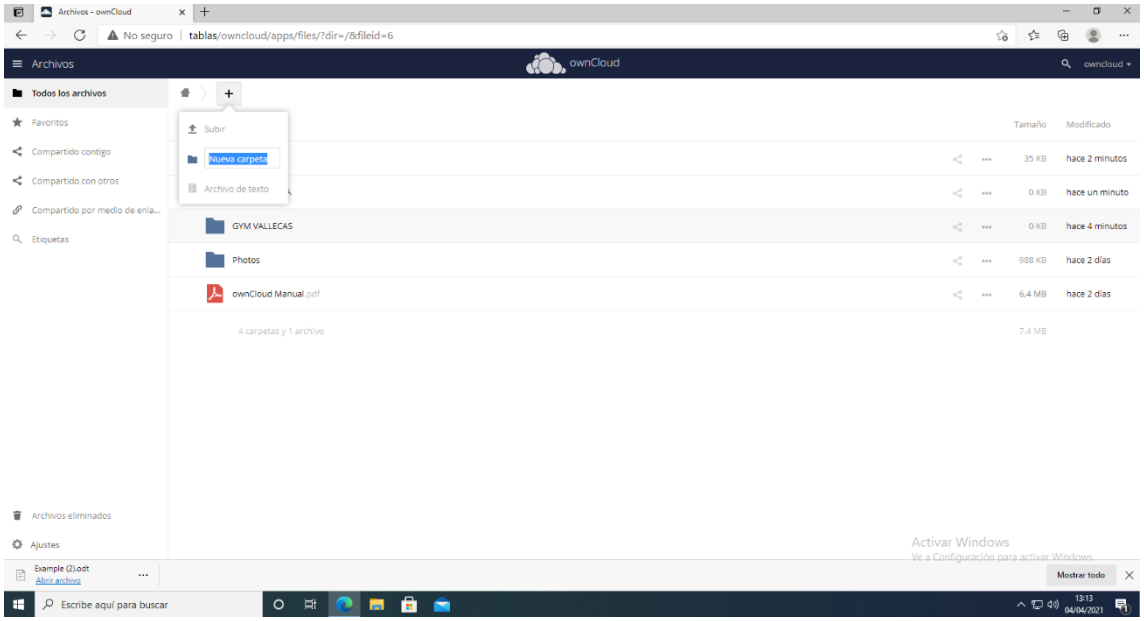

Figura 106. Creación de carpetas.

Como en la Figura 107, en cada carpeta subiremos los archivos que queremos que visualice cada gimnasio.

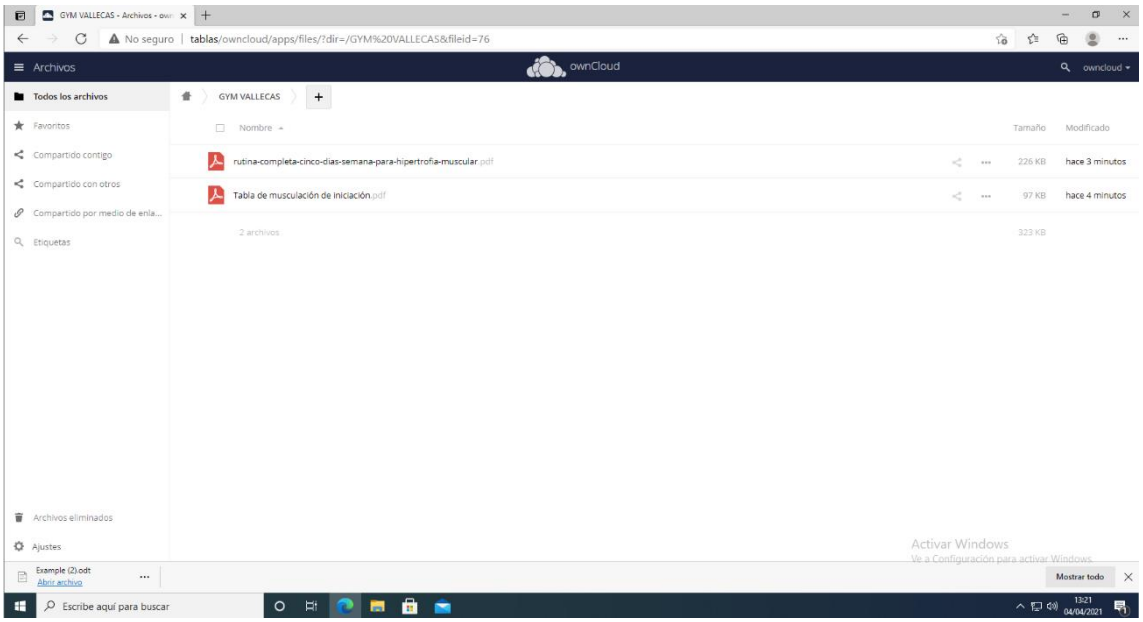

Figura 107. Archivos subidos en la carpeta creada

Una vez subidos los archivos, como podemos ver en la Figura 108, compartiremos la carpeta con el usuario correspondiente.

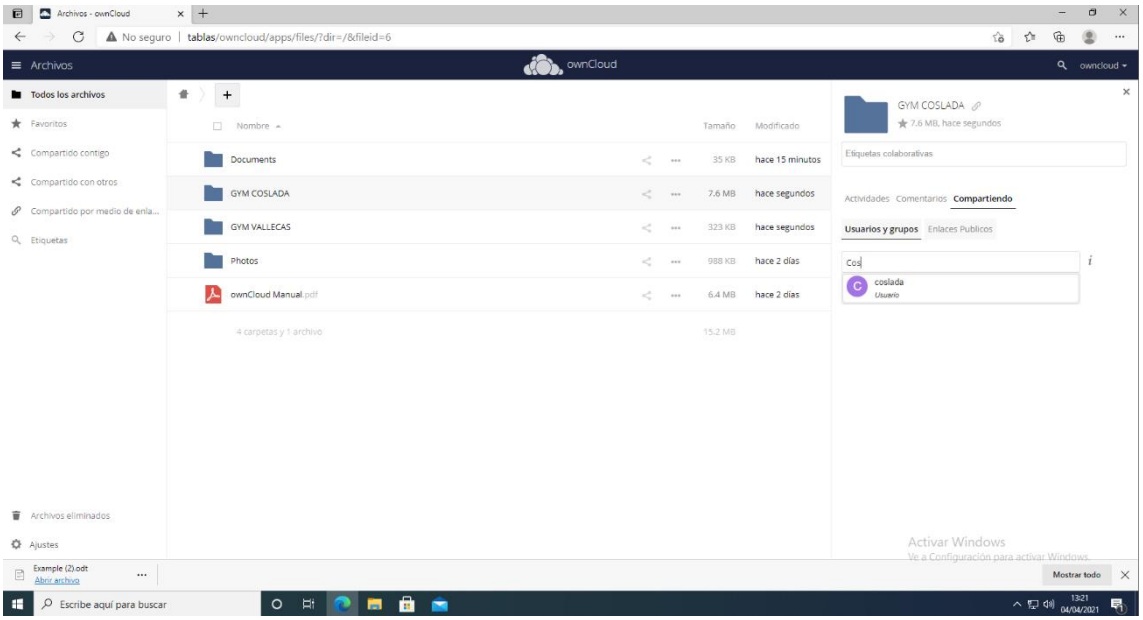

Figura 108. Selección del usuario para compartir la carpeta.

Por último, solo nos queda ingresar en http://tablas/owncloud con el usuario correspondiente y su contraseña, igual que en la Figura 109.

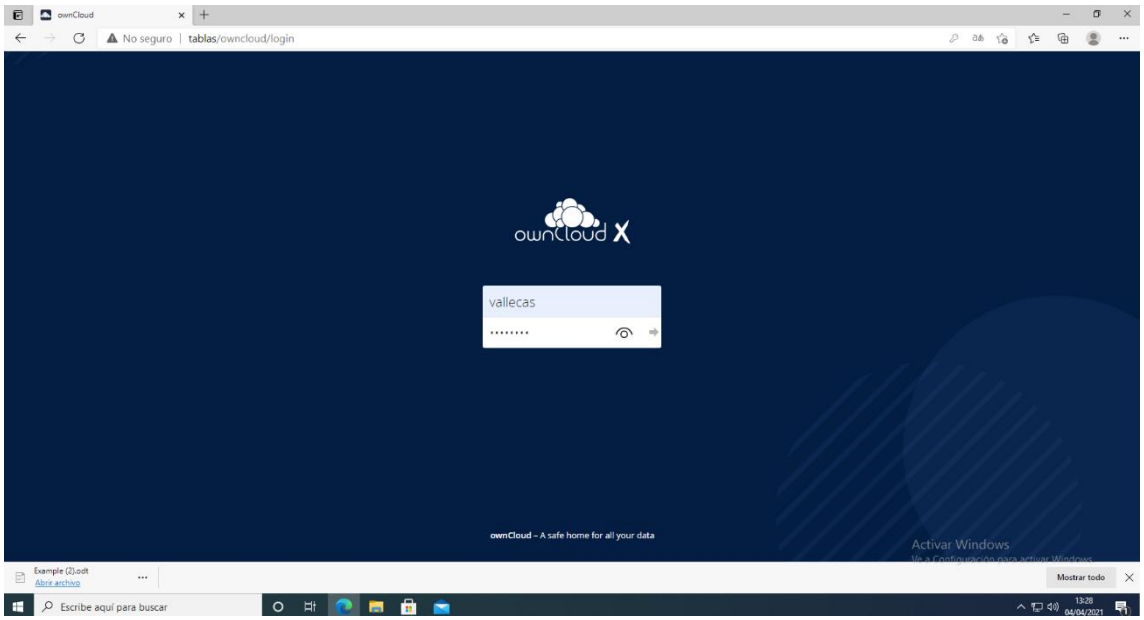

Figura 109. Introducción de las credenciales del usuario creado.

Ahí podemos ver los archivos que hemos compartido como muestra la Figura 110. Los podemos visualizar, descargar, compartir e incluso eliminar dependiendo de los privilegios que haya otorgado el administrador.

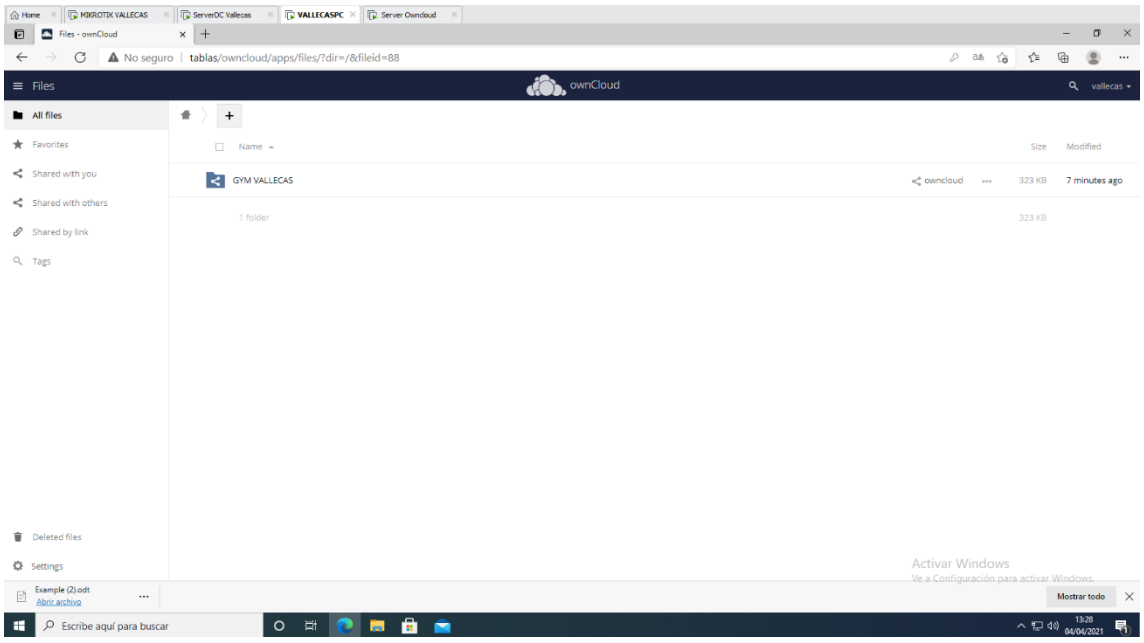

Figura 110. Página principal del usuario creado con su carpeta compartida.

7. Conclusiones y líneas futuras.

La mayor dificultad de acometer este tipo de instalación es la de identificar las necesidades del cliente, no sólo a corto plazo, sino para que en las futuras pueda llevarse a cabo sin tener que cambiar todo lo ya desarrollado.

Teniendo en cuenta que al ser una franquicia puede expandirse tanto en sedes como en número de usuarios que disfruten del negocio, hemos de ser capaces de expandirnos informáticamente hablando sin hacer grandes desajustes en el resto de los intervinientes del negocio.

Este proyecto, debido a la propuesta para su implantación, sería apropiado para su crecimiento porque con pocos ajustes (principalmente en los routers) dispondríamos de los recursos del resto de las sedes que ya están implementadas.

En este proyecto se ha aprendido a trabajar con componentes tanto software y como hardware que nunca había tenido contacto con ellos, aunque si tenía conocimiento de su existencia, como es el caso de los routers Mikrotik.

Estos routers, a través de su firewall, permiten afrontar los problemas de seguridad que se puedan presentar, haciendo que su elección para este proyecto sea el acertado en todo momento.

Me han parecido un material potente para su bajo coste y fácil manejo. Es muy intuitivo, y aunque en algún caso se complica como en el caso de la configuración del VPN, se dispone de mucho material donde apoyarse para su correcto funcionamiento.

También me sorprendido el potencial el que tiene WordPress. Investigando un poco se puede apreciar el amplio campo que maneja, pudiendo utilizar infinitos plugins para diversas funcionalidades. Sólo es necesario adaptar el blog o página web a tus necesidades y ponerlo en funcionamiento en un hosting web si quieres que sea visible a varios usuarios.

Hay que tener en cuenta que, al ser un sistema fácil de manejar, es ideal para personas que no tengan mucho conocimiento informático. Esta facilidad hará que cualquier usuario con unas nociones básicas pueda desarrollar infinidad de contenidos para publicarlos o cambiar el aspecto de la web a su antojo haciéndola más atractiva, sin necesidad de recurrir a un soporte informático. Toda una ventaja para pymes con bajo presupuesto y pocos recursos técnicos.

En cuanto a OwnCloud, he de decir que resulta una filosofía similar a OneDrive, que está más extendido actualmente, pero también como muchos recursos de los que poder beneficiarse al ser gratuito.

Siempre es bueno disponer de un servicio de almacenamiento sincronizado en todos los dispositivos, además de poder elegir a los usuarios con los que compartes archivos e información.

Es justo comentar que he disfrutado de la realización de este proyecto. He podido sufrir y a la par aprender con los errores que han ido surgiendo. La resolución de éstos, a través del ensayo-error o bien a través del apoyo en la comunidad de informáticos que existen en la red, conlleva la satisfacción del trabajo realizado correctamente.

Para terminar, este proyecto tiene capacidad para crecer en varias direcciones y servicios complementarios. Podría ser beneficioso ampliar campos como:

- Dotar al sistema de tantos usuarios personalizados como necesitemos. Este proyecto que ha tenido en cuenta únicamente 2, uno por sede, sería ampliable a varios usuarios para ser un sistema más personalizado.
- Implementar unidades organizativas dentro del Directorio Activo, para mejorar administrativamente la empresa, diferenciando secciones o departamentos y sus recursos.
- Servicios de Impresión. Es posible dotar a la empresa de un servidor de impresión donde poder compartir impresoras y escáneres de la red entre varios usuarios.
- Dotación de red Wifi. Sería beneficioso disponer de una red wifi donde los usuarios y/o máquinas puedan conectarse desde cualquier punto sin necesidad de cableado.
- Ampliación de la web, dotándola de una mayor información y utilidades. Se pueden añadir nuevos plugins que den mayores recursos al usuario que la visualiza.
- Visibilidad al exterior de la web. De esta forma se daría mayor publicidad al negocio y mejoraría la comodidad de los clientes en cuanto a la realización de reservas de salas desde sus domicilios.
- Servidor Asterisk. Añadiríamos un sistema de centralitas que mejoraría la comunicación entre diversos departamentos y sedes basado en tecnología IP.

8. Referencias Bibliográficas

[1] “Mikrotik” accesible desde https://mikrotik.com/. Fecha del último acceso: 29 de marzo de 2021.

[2] “XAMPP” accesible desde https://www.apachefriends.org/es/index.html. Fecha del último acceso 30 de marzo de 2021.

[3] “WordPress” accesible desde https://es.wordpress.org/. Fecha del último acceso 2 de abril de 2021.

[4] “OwnCloud” accesible desde https://owncloud.org/. Fecha del último acceso: 5 de abril de 2021.

[5] “Mikrotiklabs” accesible desde https://www.mikrotiklabs.com/2020/03/01/configuracion-de-openvpn-con-mikrotik/. Fecha del último acceso: 5 de abril de 2021.

[6] “Citelia” accesible desde https://citelia.es/blog/mikrotik-futuro-networking/ . Fecha del último acceso: 29 de marzo de 2021.

9. Anexos

Para acceder a los hosts y tener una mayor comodidad en el manejo, se utilizará la Tabla 4.

USUARIO	CONTRASEÑA
Administrador	@ministradorVA
USERVALLECAS	P@ssword1
USERCOSLADA	P@ssword2

Tabla 4. Tabla de usuarios y contraseñas en host (Fuente: propia).

Para acceder al servicio de OwnCloud utilizaremos los usuarios que se muestran en la Tabla 5.

NOMBRE DE USUARIO	CONTRASEÑA	TIPO DE USUARIO
owncloud	owncloud	Administrador
coslada	coslada	Usuario de Coslada
vallecas	vallecas	Usuario de Vallecas

Tabla 5. Tabla de usuarios y contraseñas para OwnCloud (Fuente: propia).

Para acceder como administrador de WordPress se utilizará el usuario y contraseña de la Tabla 6.

USUARIO	CONTRASEÑA
miusuariowp	contraseñamiusuariowp

Tabla 6. Tabla de administrador de WordPress (Fuente: propia).

Para la realización de este proyecto se ha trabajado para IPv4, deshabilitando IPv6 en las máquinas, teniendo las características que se muestra en la Tabla 7.

Máquina	Memoria	Procesador	Disco Duro
Server DC Vallecas	2 Gb	4	60 Gb
Server DC Coslada	2 Gb	4	60 Gb
Server WEB	2 Gb	4	60 Gb
Server Owncloud	2 Gb	4	50 Gb
VALLECAS PC	2 Gb	4	60 Gb
COSLADA PC	2 Gb	4	60 Gb
MIKROTIK VALLECAS	512 Mb	1	64 Mb
MIKROTIK COSLADA	512 Mb	1	64 Mb

Tabla 7. Características de las máquinas (Fuente: propia)

Se ha utilizado VMware® Workstation 15 Pro versión 15.5.5 build-16285975 para ejecutar las máquinas virtuales descritas en este proyecto, que podrán descargarse en el siguiente enlace:

https://unedo365-my.sharepoint.com/:f:/g/personal/slopez1489_alumno_uned_es/Eq2WQOc7l3FAtQbHNgt6rz4BrHgryRDEM9BZUlZnOR_e_g?e=X7rdrc