Proyecto Seguridad y Alta Disponibilidad - Trimestre 1

Versión 1.1.4c133

Pablo González Troyano - 2º ASIR - IES Villablanca

13 de noviembre de 2021

Presentación

1. Presentación **3**
1.1. Introducción . . . 3

2. Análisis y Diseño **5**
2.1. Empresa ficticia propuesta . . . 5
2.2. Plano del CPD de Bruselas . . . 7

3. Seguridad **9**
3.1. Control de Acceso físico . . . 9
3.2. Sistemas de protección contra incendios . . . 12
3.3. Sistemas anti-catástrofes . . . 14

4. Integridad **17**
4.1. Integridad de la información de la empresa . . . 17

5. Criptografía **19**
5.1. Criptografía . . . 19
5.2. Firma digital FNMT . . . 23

6. Fallos de electricidad **31**
6.1. Cálculo potencia del SAI . . . 31
6.2. Elección de dispositivos SAI . . . 33

7. IP y direccionamiento **37**
7.1. Direccionamiento IP de la empresa (general) . . . 37
7.2. Direccionamiento IP de la sede . . . 40
7.3. Configuración de dominios de la empresa . . . 42

8. Servicios y certificados **43**
8.1. Servidor SSH . . . 43
8.2. Servidor web . . . 45
8.3. Servidor FTP . . . 48
8.4. Servidor NFS . . . 51
8.5. Servidor SAMBA . . . 52
8.6. Servidor Rsync . . . 56
8.7. Convertirnos en Autoridad de Certificación . . . 58
8.8. Conseguir certificado Let's Encrypt . . . 63

8.9. Importar certificado Let's Encrypt en OMV . . . 66

9. Seguridad de la información **69**
9.1. RAID en Windows Server 2019 . . . 69
9.2. RAID en Linux Ubuntu Server 18.04 . . . 71
9.3. Recuperación de la información de RAID . . . 79

10. Servidor NAS **83**
10.1. Descargar y comprobar OpenMediaVault . . . 83
10.2. Instalar y configurar OpenMediaVault . . . 85
10.3. Configuración de RAID inicial . . . 87
10.4. Servicio SMB/CIFS . . . 88
10.5. Servicio NFS . . . 91
10.6. Servicio FTP . . . 92
10.7. Servicio SSH . . . 96
10.8. Servicio SSH autenticado con clave pública-privada . . . 98
10.9. Servicio Rsync . . . 103
10.10. Servicio Rsync automatizado . . . 105

11. NextCloud («Nube») **109**
11.1. Instalación de Sistema Operativo . . . 109
11.2. Instalación NextCloud . . . 117
11.3. Securizar Nextcloud con SSL/TLS . . . 122
11.4. Eliminar *index.php* de las URL . . . 124
11.5. Creación de usuarios en NextCloud . . . 124
11.6. Sincronización de datos cliente con NextCloud . . . 126
11.7. Instalar OnlyOffice en NextCloud . . . 136
11.8. Editar archivos con OnlyOffice . . . 139

12. *Sync & Backup* **141**
12.1. Sincronización entre la *home* y NextCloud . . . 141
12.2. Copias de seguridad incrementales con tar . . . 145
12.3. Copias de seguridad difereciales con tar . . . 146
12.4. Sincronizar carpetas de *backup* y NextCloud . . . 148

En esta página web se irán añadiendo los resúmenes de las tareas realizadas para el proyecto integrador de Seguridad y Alta Disponibilidad, en el curso de 2º ASIR.

Puedes acceder a la **web de la empresa** desde este enlace.

Nota: Este repositorio está todavía en desarrollo

CAPÍTULO 1

Presentación

1.1 Introducción

Este proyecto consistirá en el análisis, diseño, implementación de un plan de seguridad de una empresa y el desarrollo de servicios que ofrece a trabajadores y clientes. Esta empresa ficticia tendrá como mínimo:

a) Varias sedes en diferentes países estando la matriz en España.

b) Tendrá mínimo dos sedes en España (una matríz y una secundaria) y una sede en el extranjero.

c) En total tendrá más de 1000 empleados.

d) Hardware:

- Tendrá dos CPD uno en la matriz española y otro en una sede en el extranjero.
- Computadoras host y servidores.
- Dispositivos de interconexión gateway, routers, bridges, repetidores.
- Redes

e) **Software:**

- Sistemas operativos linux y windows.
- De red.
- Aplicaciones de empresas

f) **Servicios:**

- Almacenamiento de datos en local (Nas).
- Almacenamiento de datos en nube .
- Base de datos de la empresa.
- Servidores Web.
- Servidor FTP

    - Servidor DNS.
    - Copias de seguridad de los datos de empresa y de clientes.
- La empresa tendrá un dominio.
- La sede secundaría es la que vamos a implementar los servicios en este proyecto y tendrá como mínimo la siguiente arquitectura de red y de servicios:

1. *Introducción*

CAPÍTULO 2

Análisis y Diseño

2.1 Empresa ficticia propuesta

Para esta práctica se propone la empresa de venta y limpieza de alfombras de lujo «Carpet4You». Esta empresa, con sede en un pequeño pueblo de Badajoz, empezó su actividad a mediados de los años 80 y ha ido ampliando su mercado nacional e internacional, llegando a vender las alfombras del Burj Khalifa, embajadas rusas de todo el mundo. Además, las alfombras de Carpet4You se encuentran el el 20 % de las casas de Noruega, con un claro aumento en las ventas que los analistas prevén durante los próximos 12 años a tenor del 12 % interanual.

2.1.1 Sedes de la empresa

- La **sede central/operativa** de la empresa está en el pueblo de El Carrascalejo, en Badajoz. Para este sede trabajan en torno a 700 personas, siendo aproximadamente 100 de ellas trabajadores *full-remote*.
- La **sede técnica** de la empresa está situada en Bilbao. Desde esta oficina se coordinan todas las operaciones IT a nivel internacional y dispone de uno de los Centros de Proceso de Datos de la empresa. Esta sede emplea a unas 200 personas.
- La sede de **Bruselas** (Bélgica) se dedica a las ventas por todo el centro y Este de Europa. Trabajan unas 150 personas en esta sede.
- La sede de **Bergen** (Noruega) se encarga de coordinar las ventas de todo el norte de Europa. La temperatura de los paises nórdicos hace necesaria la compra de alfombras a gran escala.
- En tanto a los trabajadores *remotos*, aunque están distribuidos por el mundo, su área de acción se reduce a:
  - 15 empleados por toda Rusia.
  - 10 empleados en Reino Unido e Irlanda.
  - 5 empleados en Minsk, Bielorrusia.

2.1.2 Ubicaciones de Proceso de Datos

Centros de Proceso de Datos (CPD)

La empresa dispone de 2 grandes centros de datos en Europa, aunque tiene salas de proceso en todas las sedes de la empresa.

El CPD más importante se encuentra situado en una ubicación secreta en la ciudad de Bilbao. La Directiva de la empresa eligió esta ciudad pues es centro de interconexión global con cables submarinos como MAREA. Además, esta cuidad moderna provee de ingenieros recién graduados con ganas de aprender y ayudar a una gran empresa como Carpet4You a crecer.

Puntos de Presencia (POPs)

Debido a la característica distribuida de la empresa necesitamos tener puntos de presencia más allá de estos dos CPDs. La empresa dispondrá de salas de procesamiento de datos locales en cada una de sus sedes. En estas salas de proceso de datos se dispondrá de todo el *hardware* necesario para la conectividad de la sede, así como herramientas locales de compartición de archivos.

Para la página web se utilizan los servicios del proveedor Cloudflare, con presencia en más de 200 ciudades, lo que asegura a la empresa una velocidad excelente en la carga de la página web pública.

Nube pública

Se utiliza la zona de Londres de Google Cloud Platform para alojar los sistemas de acceso remoto para los trabajadores en Reino Unido. Se ha elegido contratar servicios de nube pública debido a que el proceso de datos de mayor intensidad se produce en los centros propios y las necesidades técnicas son demasiado elevadas como para desplegar un equipo propio.

Control de acceso a la red

Si bien la empresa dispone de conexiones y usuarios VPN, se están migrando ciertas aplicaciones a Cloudflare Access, que permite gestión centralizada de los servicios de gestión de identidad. De esta forma, se evita tráfico local de VPN (que no suele ser eficiente). También se cachean los recursos estáticos en *border*.

2.1.3 Rangos de IP asignados

Rangos públicos

La empresa dispone de una serie de rangos IP asignados por el RIR RIPE. Esto permite la conectividad indenpendiente y segura. La gestión propia asegura la optimización máxima de las rutas. Carpet4You dispone del AS número 88757. Este *Autonomous Number* tiene una serie de rangos IP asignados:

- Rangos IPv6:
  - Rango /48 1 –> 2001:db8:3c4d::/48 usado para el CPD de Bilbao
  - Rango /48 2 –> 2001:db8:3c4e::/48 usado para el CPD de Bélgica
  - Rango /48 3 –> 2001:db8:3c4f::/48 en reserva, se planea utilizar subsegmentos para la conectividad hacia Internet de las sedes y experimentación del equipo de I+D+i
- Rango en IPv4: 100.65.65.0. Subdividido

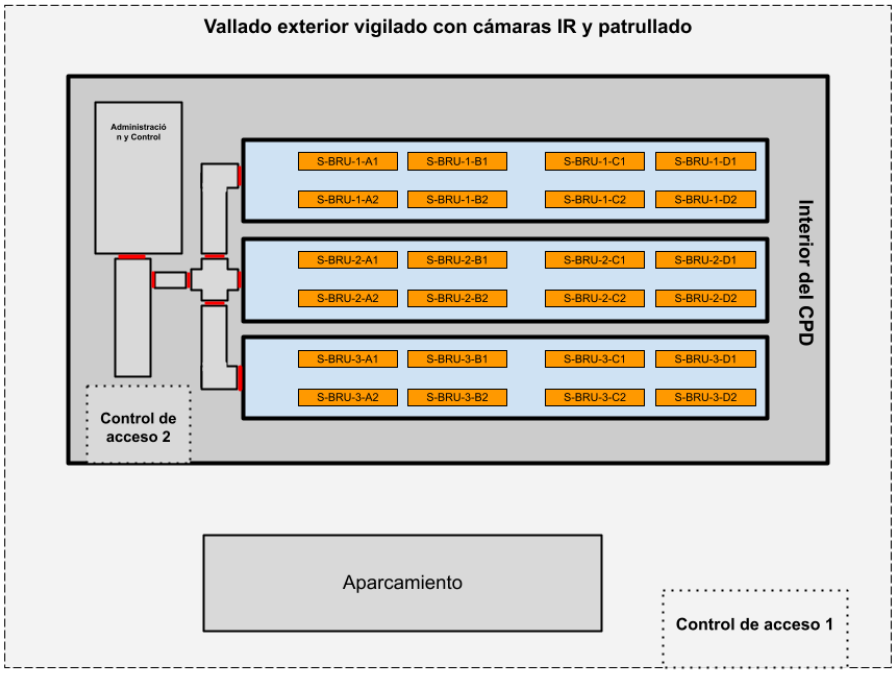
Dirección de red	Usado en	Rango de IPs utilizable	IP de Broadcast
100.65.65.0	CPD Bilbao	100.65.65.1 - 100.65.65.62	100.65.65.63
100.65.65.64	CPD Bélgica	100.65.65.65 - 100.65.65.126	100.65.65.127
100.65.65.128	Reserva	100.65.65.129 - 100.65.65.190	100.65.65.191
100.65.65.192	Reserva	100.65.65.193 - 100.65.65.254	100.65.65.255

Atención: Nótese que el rango de IPv4 no es enrutable en Internet y corresponde al rango de las IPs asigadas a los Internet Service Providers (IPS) para el uso de CG-NAT.

2.1.4 Dominio de la empresa

La empresa utiliza el dominio *carpet4you.site*

2.2 Plano del CPD de Bruselas



Nota: La versión en SVG está disponible desde este enlace

2.1. *Empresa ficticia propuesta*
2.2. *Plano del CPD de Bruselas*

CAPÍTULO 3

Seguridad

3.1 Control de Acceso físico

3.1.1 Sistema de grabación

Para el sistema de grabación de las oficinas se utilizará el sistema de **Unifi Protect Cameras**. Se puede obtener más información sobre este sistema en esta página.

Una de las características más importantes de este sistema radica en la funcionalidad de autoalojar el controlador y las grabaciones. Esto permite tener control total sobre la infraestructura. Además, de esta forma no tenemos tráfico externo en este sentido.

El departamento legal, por la alta inversión que realiza el departamento de I+D+i de la empresa nos aconsejó que las imágenes de los laboratorios de alfombras no salieran al exterior.

Cámaras de vídeo

Para la oficina de Bélgica se instalarán 40 cámaras de vídeo. Se utilizarán diferentes modelos:

- 15 Cámaras del modelo *AI 360*. La información se encuentra disponible en este enlace y el dataset aquí. Este modelo será utilizando para la grabación de vestíbulos y zonas de paso, gracias a su vista panorámica. También se instalarán en las salas de proceso de datos, 2 por sala.
- 2 Cámaras del modelo *G4 Pro*, para la grabación de pasillos entre las salas de proceso de datos. La información se encuentra disponible en este enlace y el dataset aquí.
- 5 Cámaras del modelo *G4 PTZ*. La información se encuentra disponible en este enlace y el dataset aquí. Se eligen estas cámaras para la grabación exterior gracias a su capacidad de zoom x22, movimiento de lente, etc. Se situará una cámara en cada esquina del edificio, así como una adicional en el control de acceso 1.

Gestión de grabaciones

La gestión de grabaciones se guardará en dos ubicaciones distintas como provisión de redunancia. Las grabacones serán guardadas durante 30 días en el centro y las grabaciones de los últimos 14 serán enviadas a través de conexión privada que la compañía tiene contratada (al menos) a otra sede de la empresa.

En todas las oficinas se dispone de un armario especial, marca *Rittal*, modelo *Micro Data Center Level E*. Más información en este enlace. En este se guardarán los equipos más importantes de la red. Por un lado, el sistema de gestión de grabaciones. Y los border routers que conectan los diferentes switches primarios de las salas. Estos border routers estarán conectados con dos 2 ISPs Tier 1, al menos. Y si la construcción lo permite, mediante canales exteriores distintos.

El hardware que alojará las grabaciones de las cámaras es el propio de la marca *Unifi*, el nombre del producto es *Unifi Protect Network Video Recorder Pro*. Hay disponible más información sobre dicho artículo en este enlace.

Con los discos de 8TB ya tenidos en cuenta el sistema de gestión y alojamiento de grabaciones tiene un coste aproximado de 1.500€.

Coste del sistema de grabaciones

Producto	Cantidad	Precio/Unidad	Precio total
Cámaras AI 360	15	249,00 €	3 735,00 €
G4 Pro	2	379,00 €	758,00 €
G4 PTZ	5	1 509,00 €	7 545,00 €
NVR Pro + HDD	1	1 500,00 €	1 500,00 €

3.1.2 Sistema de control de personas interior

El sistema de control de acceso es producido por la misma empresa que las cámaras. El nombre comercial es *Unifi Access*.

Debemos distinguir los siguientes dispositivos/partes de control: * Las tarjetas inteligentes. De estas dispondrán los empleados y las usarán para moverse por el centro. * Los lectores de tarjetas. Distinguimos dos modelos distintos:

- El AC Reader Pro, con pantalla y cámara integrada. Se instalará en las puertas de entrada a la sala de Control, así como en la de acceso al distribuidor de salas de proceso. Dispone de lector de tarjetas, Bluetooth para integración con la aplicación móvil de acceso, posibilidad de introducir PIN de acceso, y cámara para actuar de timbre y ser permitida la entrada por otra persona.
- El AC Reader Lite, que se instalará en las puertas de entrada a las salas de proceso de datos. Uno en cada lado de la puerta de paso. Así, como en el sentido de vuelta de las salas de proceso de datos. Permite la identificación con tarjeta inteligente, así como con la aplicación móvil.
- El Access Hub, que actúa de interfaz entre el controlador de los equipos, las cerraduras y los lectores. Se conecta mediante PoE al cotrolador y el resto de equipos de una pueta a este. Desde el Access Hub son alimentados mediante PoE los lectores.
- Todo el sistema es coordinado por el equipo *Dream Machine Pro*, que dispone de una interfaz web para la gestión y mantenimiento. En este equipo también se instalará el controlador para el sistema Wi-Fi. Tiene un coste aproximado de 500€

En el siguiente vídeo podemos ver cómo funciona el sistema:

Coste del sistema de control de paso

Producto	Cantidad	Precio/Unidad	Precio total
Tarjetas de control	200	3,00 $	600,00 $
Access Hub	7	199,00 $	1 393,00 $
Access Reader Pro	2	299,00 $	598,00 $
Access Reader Lite	7	99,00 $	693,00 $
Unifi Dream Machine	1	500,00 $	500,00 $

3.1.3 Sistema de arcos de seguridad y detectores de metales

La instalación y el mantenimiento de estas soluciones correrá a cargo de la empresa barcelonesa «OrcromSeguridad». Se instalará en el control de acceso 2 un conjunto de control del fabricante *Garret Metal Detectors*. En este enlace se encuentra disponible un folleto publicitario con los productos que incluye el conjunto. Son los siguientes:

- *Spectrum 6040*, que permite la inspección de mochilas y bolsos de empleados y visitantes. Se instará a los empleados a no pasar al interior con mochilas y bolsos, permitiéndolo dejar en taquillas vigiladas en el control. De esta manera se evita la sobre exposición de la empleada/o del Control, trabajadoras, trabajadores y visitantes a los rayos X, así como de sus pertenencias. En este enlace se puede obtener más información sobre este producto.
- *Garrett PD 6500i*, este arco de seguridad permite evitar el paso con objetos metálicos al interior del recinto. Desde este enlace se puede obtener más información sobre dicho producto.

El equipo será operado por un vigilante de seguridad propio (en Carpet4You no subcontratamos/externalizamos, pues creemos en el empleo de calidad y la confianza).

Se desconoce el precio de dicho sistema, al no ser público.

3.1.4 Sistema de prevención de intrusión exterior

Para prevenir el acceso desde el exterior se combinan diferentes medidas de seguridad.

- Por un lado, todo el recinto se encuntra vallado perimetramente con dos líneas de 2 metros de altura.
- En estas vallas instaladas alrededor del centro se han instalado carteles que indican que está prohibido el paso a la propiedad.
- Se han instalado detectores de movimiento que son activadas cuando cae la noche de forma automática.
- Para la entrada de vehículos se han instalado bolardos automáticos homologados para evitar la intrusión de camión a 90 km/h de forma directa. Estos se accionan desde el puesto de control 1.

3.1.5 Vigilancia perimetral y control interior

- El personal de control del acceso 1 está encargado de la vigilancia exterior, día y de noche.
- Se realizan periódicamente revisiones alrededor de las zonas exteriores del centro para controlar que no se han provocado daños al vallado ni producido incidencias que puedan afectar a la continuidad del centro y la operativa de la empresa.
- En el puesto de control 1 se localiza, como mínimo un agente de seguridad. Si bien, como se ha comentado anteriormente, son contratados directamente por la empresa, este personal NO tiene acceso a las salas de proceso de datos.
- Por seguridad, tampoco tienen acceso a la sala de Administración y Control directamente. Sí puede ser permitida la entrada por la empleada o el empleado de mayor rango del centro en un momento dado.

- En caso de necesidad máxima otra empleada o empleado de una sede distinta, con rango elevado, puede habilitar remotamente el acceso.

3.2 Sistemas de protección contra incendios

Mantener unas instalaciones seguras es vital. No solo para la seguridad de los datos, que es la materia que trataremos en profundidadidad, sino también para la seguridad de las personas: empleadas y empleados de nuestras sedes por el mundo. Por tanto, la empresa Carpet4You cuenta con los sistemas de protección contra incendios más avanzados del mercado.

Como empresa internacional, Carpet4You cumple con todas las regulaciones en materia de seguridad. Además se acoge a las recomendaciones de la norma NFPA 75, de protección contra incendios en Centros de Datos[1].

3.2.1 Prevención de incendios (PI)

Aunque siempre debemos estar preparados para enfrentarnos a un incendio de grandes dimensiones (como el que enfrentó OVH hace unos meses)[2] , los grandes incendios al principio son pequeños, por lo que es importante prevenirlos y en caso de que surjan, extinguirlos lo antes posible. Para hacerlo, se toman en consideración una serie de medidas (protección contra incendios pasiva):

- Las diferentes salas del edificio de procesamiento de datos estarán separadas por puertas ignífugas. Se ha evitado en la construcción del edificio los pasillos largos que puedas propagar incendios.
- En la construcción del edificio también se ha exigido que las paredes no contengan materiales inflamables (aislamientos plásticos, poliuretano, etc).
- Las empleadas y empleados del centro de datos han asistido a cursos de PRL[3] y PI. Con cada mejora o actualización del sistema se repiten rondas de formación.
- Se planifican simulacros de acción y evacuación, coordinados con el equipo de bomberos de la ciudad.

3.2.2 Detección y alerta de incendios

La detección de incendios en la instalación de Bélgica no se limitará solo a la(s) sala(s) de tratamiento de datos dentro del Centro, sino todo el recinto. Los centros de datos son altamente vulnerables a los incendios por características intrínsecas como la alta concentración de consumo energético, materiales plásticos en cables, falsos techos y suelos, etc.

Para la detección de incendios se utilizará la Gama *Notifier by Honeywell*. La lista de productos actualizada a Julio de 2021 se encuentra disponible en este enlace y el detalle de coste de los productos es accesible desde este otro enlace. Esta lista de productos y precios se ha obtenido de la web del proveedor JMSystems.

[1] Más información sobre dicho estándar se puede obtener aquí y aquí.
[2] En este artículo se puede obtener más información sobre el incendio que sufrió OVH.
[3] PRL: Prevención de Riesgos Laborales.

Productos de detección y alerta de incendios elegidos

- 1 Central analógicas AM-8200, que se situará en la sala de Administración y Control.
- 1 HON-CGW-MBB, El CLSS Gateway es la interfaz de Honeywell Fire que se conecta a una central o a una red de centrales de incendios de Honeywell, sirviendo de portal entre la central, la Nube y los dispositivos periféricos. La Pasarela CLSS permite leer el inventario del sistema de dispositivos conectados desde una central o una red de centrales y transmitir estos datos a la Nube de Honeywell. Conexión Wi-fi y/o Ethernet
- 2 LCD-8200, Panel repetidor para las centrales analógicas AM-8200. Se situarán en los controles de acceso.
- 45 detector óptico IR analógico de alta sensibilidad (NFXI-VIEW). Estarán situados 15 en cada sala de proceso de datos.
- 30 pulsadores de alarma M5A-RP02FF-N026-41.
- 10 Sirena EN54/3 y EN54/23 con cobertura "Wide" (DSE3-23 HW). Situadas en puntos estratégicos para la alerta del personal del centro.

Producto	Cantidad	Precio/Unidad	Precio total
AM-8200-EU	1	3 030,00 €	3 030,00 €
HON-CGW-MBB	1	500,00 €	500,00 €
LCD-8200	2	1 192,00 €	2 384,00 €
NFXI-VIEW	45	310,00 €	13 950,00 €
M5A-RP02FF-N026-41	30	75,69 €	2 270,00 €
DSE3-23 HW	10	89,11 €	891,10 €

3.2.3 Extinción de incendios

Extinción de incendios (off-room)

Para la extinción de incendios en los pasillos, vestíbulos y alrededores del edificio de CPD se implementan las siguientes medidas:

- Se instalan bombas de extinción de incendios en el exterior de la sede. De esta forma se podrían sofocar incendios provocados por, por ejemplo, coches. Un incendio exterior no sofocado puede propagarse al interior y ser mucho más problemático. Estas BIE (Bocas de Incendio Equipadas) estarán señalizadas acorde a la legalización y se encontrará una cada 100 metros en la pared exterior del edificio.
- Junto con las BIE, se instalarán hidrantes para facilitar la acción del equipo de bomberos en caso de ser necesario.
- Las mangueras de las BIE por norma general se encuentran entre los 20 y 50 metros. Se adquiere una manguera racorada (con los *«enganches»*) y un portamangueras, que serán depositados en el control de acceso 2 listos para ser desplegados en caso de ser necearios.
- No se instalarán aspersores no ningún método de extinción por agua en el interior del edificio. Esto podría provocar problemas con los componentes eléctricos.
- Se instalarán extintores de 5kg cada 100 metros por lateral, alternándolos. Lo que en la práctica significará que cada 50 metros habrá disponible un extintor. Así como uno de 10kg en cada control de acceso y en la sala de Administración y Control.

Extinción de incendios (on-room)

El sistema principal de extinción de incendios de la sala de proceso de datos estará basado en *FM-200*. Es un gas incoloro y no conductor, lo que permite ser usado en nuestro caso, con servidores. El compuesto es heptafluoropropano. Este gas se envasa en estado líquido en cilindros metálicos de alta presión. En caso de detectar un incendio, es liberado inmediatamente en la sala mediante tuberías, ocupando el mayor espacio posible (al ser un gas) en pocos segundos. Opera interrumpiendo la reacción en cadena. Es un gas no tóxico, por lo que agentes de bomberos y el propio personal de Carpet4You puede estar en la sala para colaborar en la extinción o retornar equipos sin necesidad de expulsar el gas. En el CPD de Bilbao previamente se utilizada CO_2, pero se ha actualizado recientemente a FM-200 por esta diferencia.

En este vídeo se puede ver como actúa el FM-200:

En la esta sala de proceso de datos también se situarán la señalización de emergencia y evacuacion (siempre clase A para facilitar la identificación aún en momentos de poca visibiliad o fallo de suministro eléctrico).

Aunque no se prevé su uso gracias a la instalación del sistema FM-200 serán instalados extintores de CO_2. En cada extremo del pasillo se situará un extintor de 5 Kg de CO_2(peso total 14Kg)[4]. De forma adicional, en los pasillos intermedios entre los primarios, perpendiculares a estos, se instalarán extintores de C02 de 2Kg. Estos extitores tiene un peso total de unos 8 Kg, aproximadamente. Se eligen estos para permitir que cualquier persona pueda utilizarlos y el peso de la solución no sea problema para aplicarlo.

Productos de extinción de incendios elegidos

Producto	Cantidad	Precio/Unidad	Precio total
BIE exterior	6	166,00 €	996,00 €
Manguera plana racorada exterior	1	200,00 €	200,00 €
Extintor 5 Kg (off-room)	6	47,80 €	1 242,80 €
Extintor 10 Kg (off-room)	2	149,00 €	298,00 €
Extintor 5 Kg (on-room)	6	47,80 €	1 242,80 €
Extintor 2 Kg (on-room)	6	47,80 €	1 242,80 €
Señalización (aprox.)	30	5, 00 €	150,00 €

Nota: no se incluye el sistema FM-200 al desconocer su precio.

Notas al pie de página

3.3 Sistemas anti-catástrofes

3.3.1 Terremotos

Los centros de datos de Carpet4You se encuentran en zonas con posibilidad limitada de terremotos, tal y como se puede ver en este mapa interactivo del servicio sismológico suizo.

[4] La información sobre precio y pesos de los extintores de CO_2se ha obtenido de esta página.

3.3.2 Inundaciomes

Todas las instalaciones de proceso de datos se encuentran situadas en zonas con probabilidad baja de inundación por lluvias.

Por las salas de proceso de datos, tanto de oficianas como de CPD, no discurren tuberías. Además, las salas de proceso de los CPD y los pasillos de acceso a estas son estancas, previniendo la filtración de agua hacia estas.

3.1. *Control de Acceso físico*
3.2. *Sistemas de protección contra incendios*
3.2. *Sistemas anti-catástrofes*

CAPÍTULO 4

Integridad

4.1 Integridad de la información de la empresa

A la web de la empresa (Carpet4You.site) se ha subido un documento (plano_CPD.pdf).

Lo primero que hacemos es obtener el archivo, esto normalmente se hace antes de crear subirlo a la web, pero al estar en un máquina virtual es así más sencillo

```
pablo@carpet:~$ curl https://carpet4you.site/images/plano_CPD.pdf -o plano_CPD.pdf
```

Una vez lo tenemos debemos generar las sumas de comprobación, utilizando los diferentes sistemas que tenemos para ello.

4.1.1 Realización de sumas de comprobación

Suma de comprobación MD5

```
pablo@carpet:~$ md5sum plano_CPD.pdf
a68fed06b2892d8d3de98f6a11f61414  plano_CPD.pdf
```

Suma de comprobación SHA256

```
pablo@carpet:~$ sha256sum plano_CPD.pdf
2e4dd97fb037c115938022556020da86080656c85df963c24f1260489cf2e261  plano_CPD.pdf
```

Suma de comprobación SHA512

```
pablo@carpet:~$ sha512sum plano_CPD.pdf
1ec7ac99fa424a958e8f046f31aff6b524aa80cb860111ac2d0480f0282ec2bad8af35cee85cdde57708a5f2049b02e82628ec2b
↪ plano_CPD.pdf
```

Una vez generados los *checksums*, también llamados *sumas de comprobación*, *huellas digitales* o *sumas de verificación* debemos subirlo a la web.

A continuación se recogen las sumas en esta página web:

Método de generación	Suma generada
MD5	a68fed06b2892d8d3de98f6a11f61414
SHA256	2e4dd97fb037c115938022556020da86080656c85df963c24f1260489cf2e261
SHA512	1ec7ac99fa424a958e8f046f31aff6b524aa80cb860111ac2d0480f0282ec2bad8af35cee85cdde57708a5f2049b02e826

4.1. *Integridad de la información de la empresa*

CAPÍTULO 5

Criptografía

5.1 Criptografía

5.1.1 Ejercicio 4.1

Genera un par de claves asimétricas de un empleado que tendrá tu nombre, apellidos y tu correo electrónico de gmail. Captura la pantalla el comando utilizado y el resultado obtenido.

Nota: Se utilizará el correo pablo@carpet4you.site en vez de mi dirección personal de Gmail.

Para generar un par de claves asimétricas debemos seguir las siguientes instrucciones:

```
pablo@carpet:~$ gpg --gen-key
gpg (GnuPG) 2.2.12; Copyright (C) 2018 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: keybox '/home/pablo/.gnupg/pubring.kbx' created
Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: Pablo González
Email address: pablo@carpet4you.site
You are using the 'utf-8' character set.
You selected this USER-ID:
    "Pablo González <pablo@carpet4you.site>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
```

(continué en la próxima página)

(proviene de la página anterior)

```
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /home/pablo/.gnupg/trustdb.gpg: trustdb created
gpg: key 48CF9B50966CC9B7 marked as ultimately trusted
gpg: directory '/home/pablo/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/pablo/.gnupg/openpgp-revocs.d/
↪D5AA1DFFB6A4557305CECF4148CF9B50966CC9B7.rev'
public and secret key created and signed.

pub   rsa3072 2021-10-23 [SC] [expires: 2023-10-23]
    D5AA1DFFB6A4557305CECF4148CF9B50966CC9B7
uid                      Pablo González <pablo@carpet4you.site>
sub   rsa3072 2021-10-23 [E] [expires: 2023-10-23]
```

Para ver las clave generada podemos utilzar el siguiente comando:

```
pablo@carpet:~$ gpg -k
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2023-10-23
/home/pablogontroya/.gnupg/pubring.kbx
---------------------------------------
pub   rsa3072 2021-10-23 [SC] [expires: 2023-10-23]
    D5AA1DFFB6A4557305CECF4148CF9B50966CC9B7
uid           [ultimate] Pablo González <pablo@carpet4you.site>
sub   rsa3072 2021-10-23 [E] [expires: 2023-10-23]
```

5.1.2 Ejercicio 4.2

Genera un par de claves asimétricas que servirán para tu empresa que tendrá como datos el nombre de tu empresa y el correo electrónico del administrador de tu empresa. Captura la pantalla el comando utilizado y el resultado obtenido.

Para generar un par de claves asimétricas ejecutar el comando siguiente. El comando nos pedirá el nombre y el correo electrónico que queremos utilizar para la generación. También la clave simétrica que protegerá la clave privada.

```
gpg gen-key
[...]
public and secret key created and signed.

pub   rsa3072 2021-10-23 [SC] [expires: 2022-01-21]
    0171E7FC0657E4CCFAEC3C23164857A2CDB61EEC
uid                      Carpet4You Management (Las mejores alfombras del universo)
↪<info@carpet4you.site>
sub   rsa3072 2021-10-23 [E] [expires: 2022-01-21]
```

5.1.3 Ejercicio 4.3

Muestra las claves privadas de tu empleado y de tu empresa. Captura la pantalla el comando utilizado y el resultado obtenido.

Para ver las claves privadas que tenemos en nuestro *keyring* debemos ejecutar el siguiente comando:

```
pablo@carpet:~$ gpg -k
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   2  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: next trustdb check due at 2022-01-21
/home/pablogontroya/.gnupg/pubring.kbx
-------------------------------------
pub   rsa3072 2021-10-23 [SC] [expires: 2023-10-23]
    D5AA1DFFB6A4557305CECF4148CF9B50966CC9B7
uid           [ultimate] Pablo González <pablo@carpet4you.site>
sub   rsa3072 2021-10-23 [E] [expires: 2023-10-23]

pub   rsa3072 2021-10-23 [SC] [expires: 2022-01-21]
    0171E7FC0657E4CCFAEC3C23164857A2CDB61EEC
uid           [ultimate] Carpet4You Management (Las mejores alfombras del universo)
↪<info@carpet4you.site>
sub   rsa3072 2021-10-23 [E] [expires: 2022-01-21]
```

5.1.4 Ejercicios 4.4 y 4.5

Exporta las claves privadas/públicas de tu empleado y de tu empresa a archivos que se entregaran con el proyecto. Por cada uno de ellos se tendrán los archivos ClavePublicaNombreApellidos.key que contendrá la clave pública y ClavePrivadaNombreApellidos.key que contendrá la clave privada del usuario y ClavePublicaNombreEmpresa.key y ClavePrivadaNombreEmpresa.key de las empresas.

Para exportar las claves públicas:

```
pablo@carpet:~$ gpg --armor --output ClavePublicaPabloGonzalez.key --export␣
↪D5AA1DFFB6A4557305CECF4148CF9B50966CC9B7

pablo@carpet:~$ gpg --armor --output ClavePublicaCarpet4You.key --export␣
↪0171E7FC0657E4CCFAEC3C23164857A2CDB61EEC
```

Para exportar las claves privadas (nos pedirá la clave simétrica):

```
pablo@carpet:~$ gpg --armor --output ClavePrivadaPabloGonzalez.key --export-secret-keys␣
↪D5AA1DFFB6A4557305CECF4148CF9B50966CC9B7

pablo@carpet:~$ gpg --armor --output ClavePrivadaCarpet4You.key --export-secret-keys␣
↪0171E7FC0657E4CCFAEC3C23164857A2CDB61EEC
```

5.1.5 Ejercicio 4.6

En el moodle del instituto en el apartado del proyecto estarán las claves públicas y privadas de un tercer empleado genérico que tienes que importar al anillo de tu servidor de usuarios. Captura la pantalla el comando utilizado y el resultado obtenido.

Una vez descargadas desde el Aula Virtual las claves, debemos extraer los .key del archivo comprimido tar.gz:

```
pablo@carpet:~$ tar -xf 'ClavesPublicayPrivada Empleado genérico .tar.gz'
```

Advertencia: Se ha producido un error al importar la clave pública. Parece que ocupa 0 bytes:

```
pablo@carpet:~$ ls -lah
-rwxr-xr-x 1 pablo pablo 5241 Nov 11  2019 PrivateKeyEmpleadoGenerico.key
-rwxr-xr-x 1 pablo pablo    0 Nov 11  2019 PublicKeyEmpleadoGenerico.key
```

Importaremos la clave privada:

```
gpg --import PrivateKeyEmpleadoGenerico.key
```

Aunque no sepamos la contraseña simétrica, la clave pública será importada.

Para ver la clave pública importada:

```
user@server-carpet:~$ gpg --list-keys
/home/user/.gnupg/pubring.kbx
-----------------------------
pub   rsa3072 2019-11-07 [SC] [expires: 2021-11-06]
    2F537C9D14C7E613DE5C0EEDA540561B0E2FED4D
uid           [ unknown] Empleado Generico Empresa <EmpleadoGenerico@empresa.com>
sub   rsa3072 2019-11-07 [E] [expires: 2021-11-06]
```

5.1.6 Ejercicio 4.7

Cifra un fichero con el texto "Hola Mundo" y encriptarlo con el empleado genérico. Captura la pantalla el comando utilizado y el resultado obtenido. Entrega el fichero encriptado.

```
pablo@carpet:~$ echo "Hola Mundo" > Empleado-PabloGonzález.txt
pablo@carpet:~$ gpg -a -r pablo@carpet4you.site --encrypt Empleado-PabloGonzález.txt

pablo@carpet:~$ ll E*
    -rw-r--r-- 1 pablogontroya pablogontroya  11 Oct 23 23:03 Empleado-PabloGonzález.txt
    -rw-r--r-- 1 pablogontroya pablogontroya 736 Oct 23 23:04 Empleado-PabloGonzález.txt.
↪asc
```

5.1.7 Ejercicio 4.8

Desencripta el fichero. Captura la pantalla el comando utilizado y el resultado obtenido.

Para desencriptar el fichero debemos utilizar el comando que podemos ver a continuación. Nos pedirá la clave simétrica de la clave privada.

```
pablo@carpet:~$ gpg --decrypt Empleado-PabloGonzález.txt.asc
gpg: encrypted with 3072-bit RSA key, ID 8D27C3D26858C7E2, created 2021-10-23
    "Pablo González <pablo@carpet4you.site>"
Hola Mundo
```

5.1.8 Ejercicio 4.9

Firma digitalmente con la clave asimétrica de tu empresa el fichero que has subido a la web en el anterior ejercicio creando una firma separada del archivo. Sube la firma y la clave pública a tu web junto a los hash para que un usuario pueda comprobar la autoría del fichero. Captura la pantalla el comando utilizado y el resultado obtenido.

```
pablo@carpet:~$ gpg --output plano_CPD.pdf.sign --sign plano_CPD.pdf
```

Para verificar la firma del archivo podemos ejecutar:

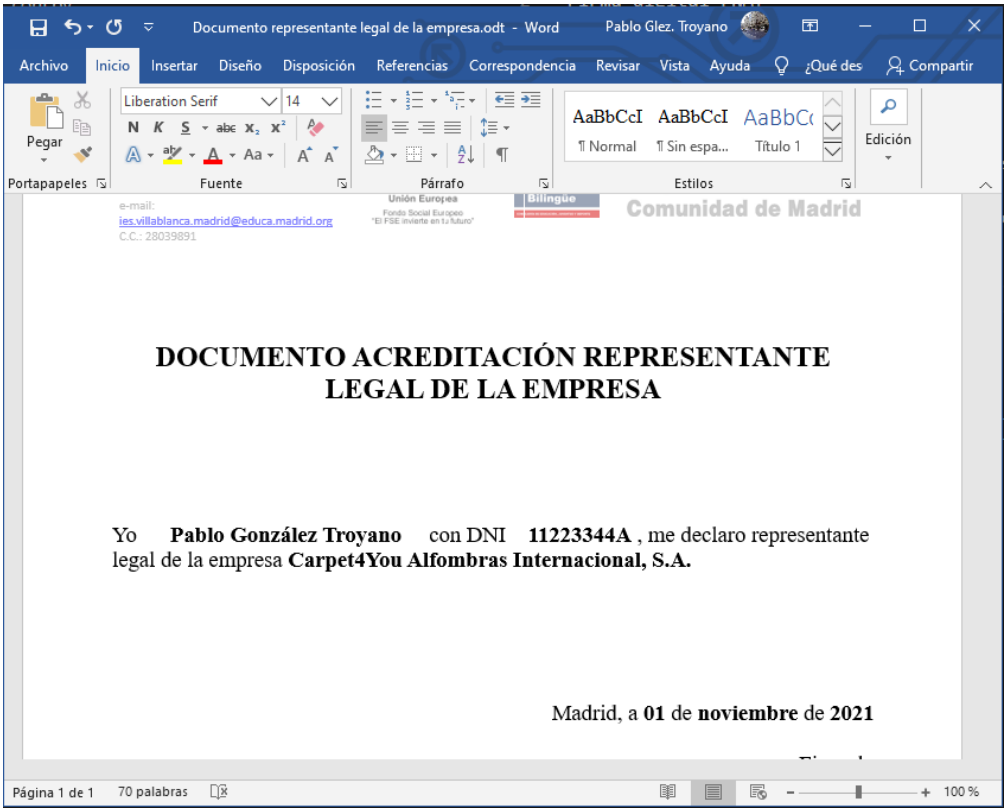
```
pablo@carpet:~$ gpg --verify plano_CPD.pdf.sign
gpg: Signature made Sat 23 Oct 2021 11:19:36 PM CEST
gpg:                using RSA key D5AA1DFFB6A4557305CECF4148CF9B50966CC9B7
gpg: Good signature from "Pablo González <pablo@carpet4you.site>" [ultimate]
gpg: WARNING: not a detached signature; file 'plano_CPD.pdf' was NOT verified!
```

5.2 Firma digital FNMT

5.2.1 Rellenar documento y generar PDF

Descargamos el documento plantilla desde el Aula Virtual.

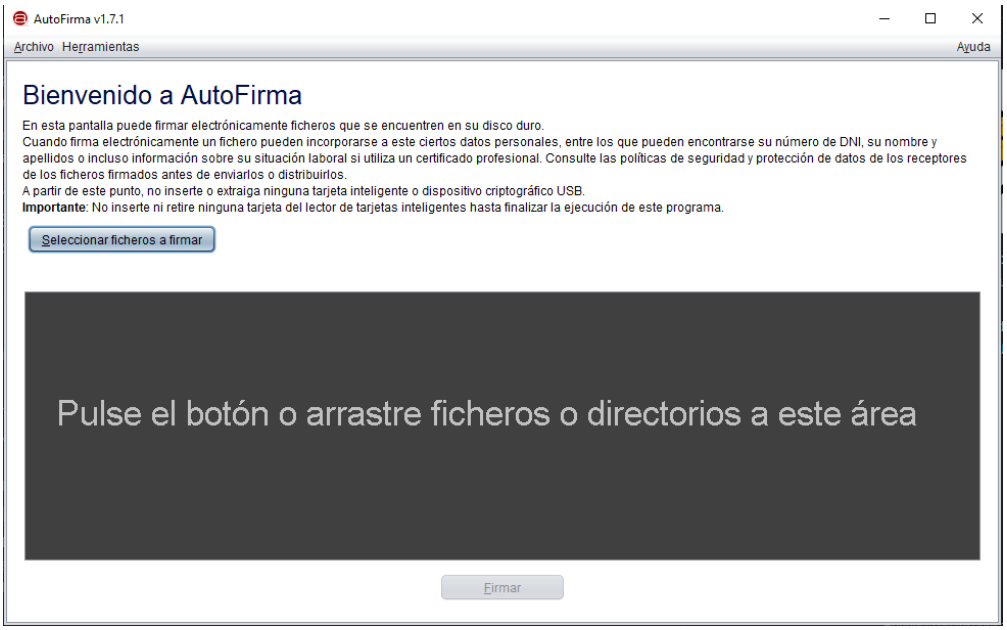
Procederemos a cumplimentarlo utilizando cualquier programa de edición de documentos. Una vez hecho, lo exportaremos como PDF.



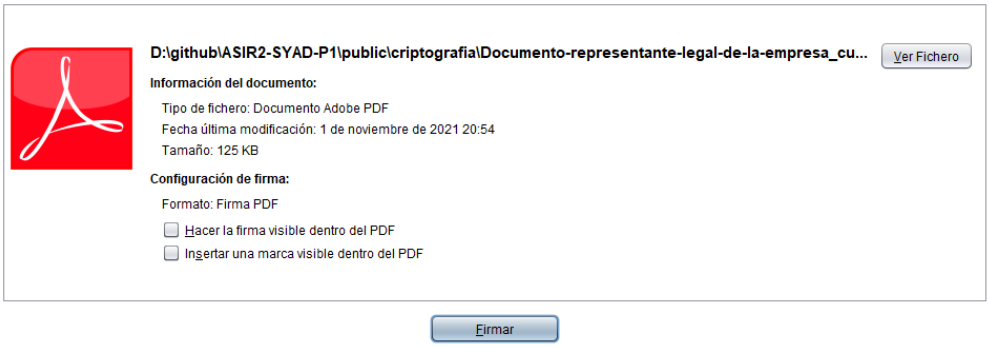
5.2.2 Firmar el documento con AutoFirma

Si no lo hemos hecho, descargaremos el programa AutoFirma desde la página web oficial. Importaremos, si no lo hecho ya, nuestro certificado electrónico en nuestro sistema.

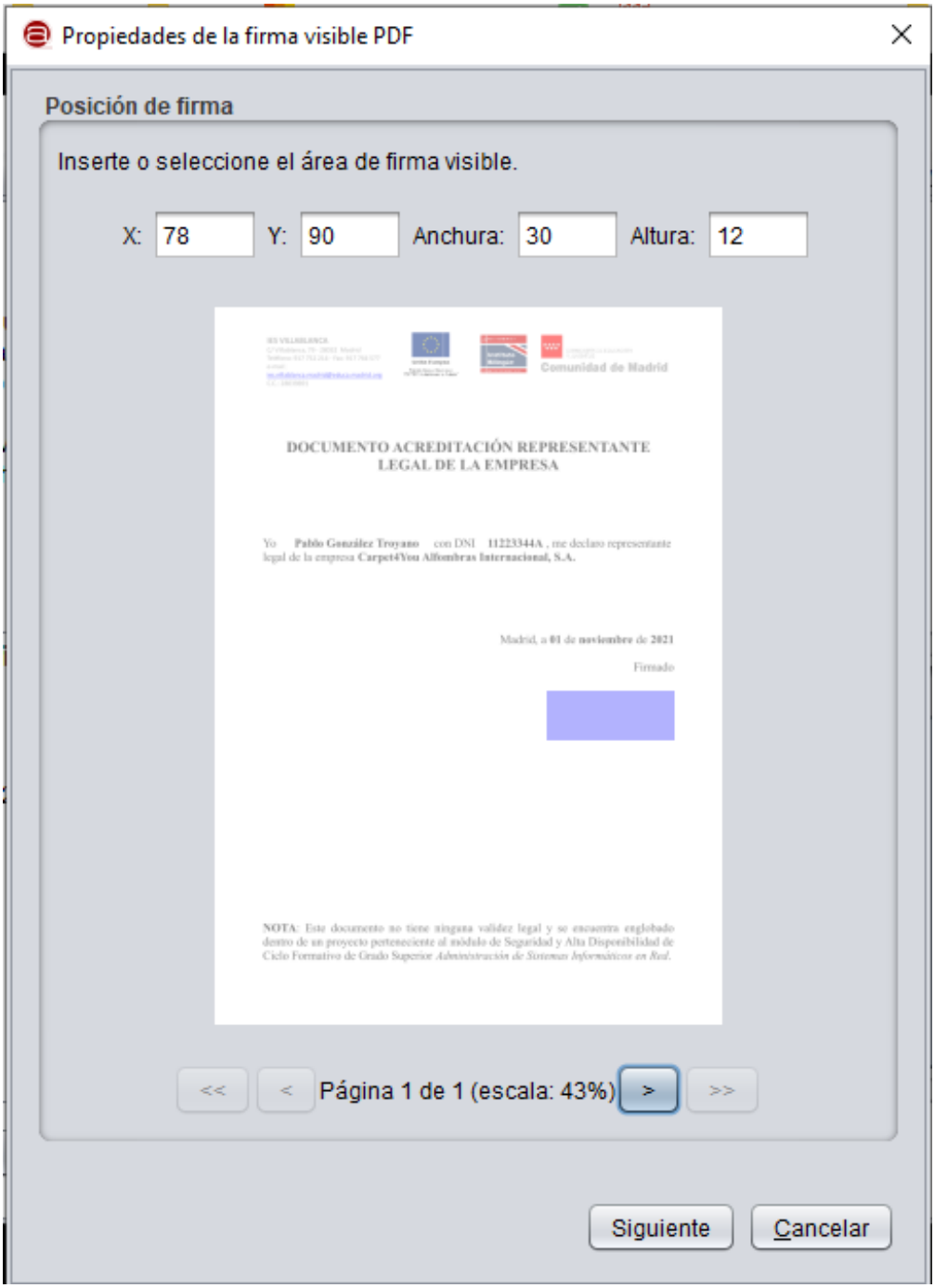
Al iniciar la aplicación, veremos la siguiente ventana. Hacemos clic en *Seleccionar ficheros a firmar*.



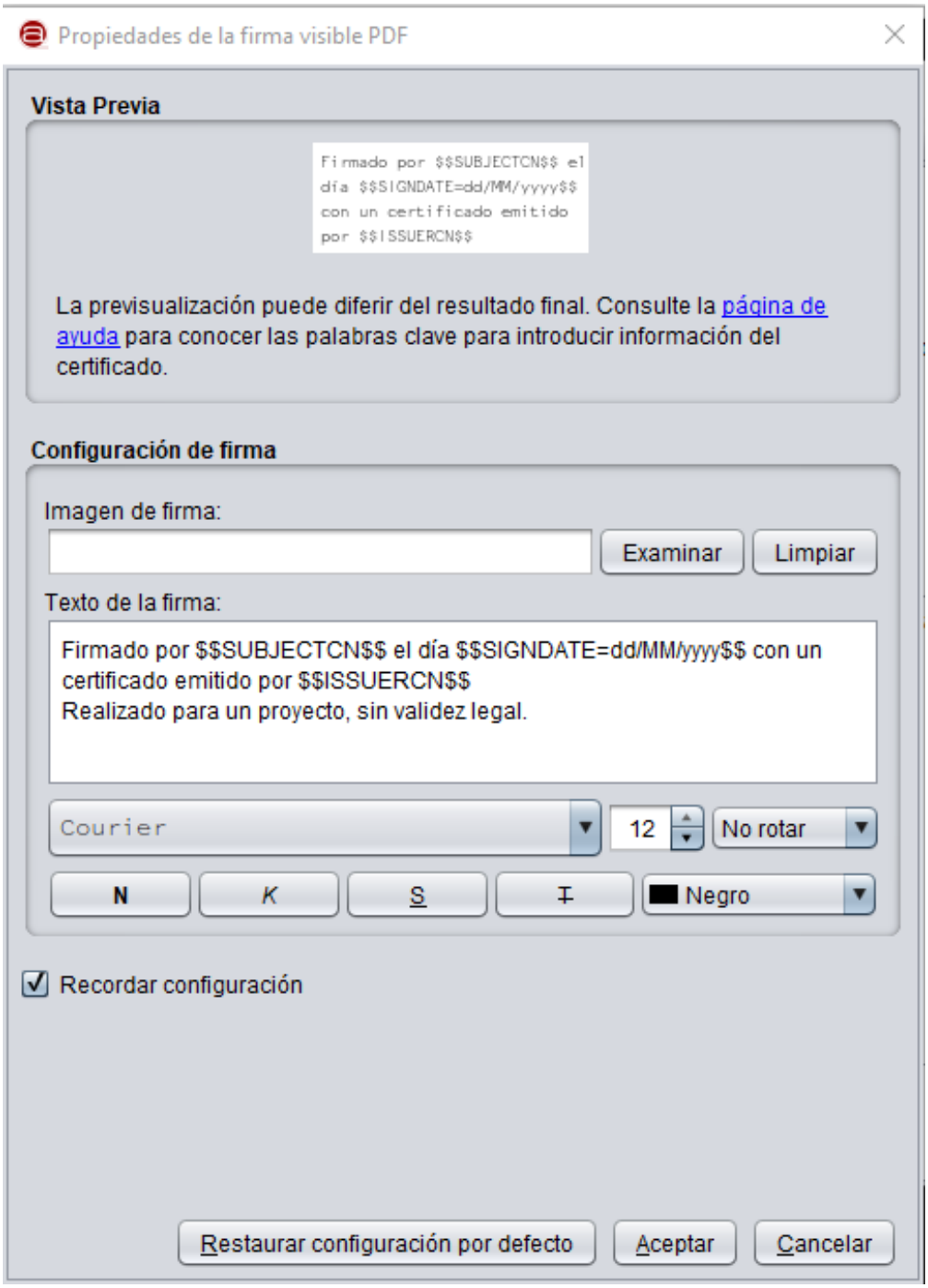
Al seleccionar el fichero, se cargarán los datos en la ventana inferior:



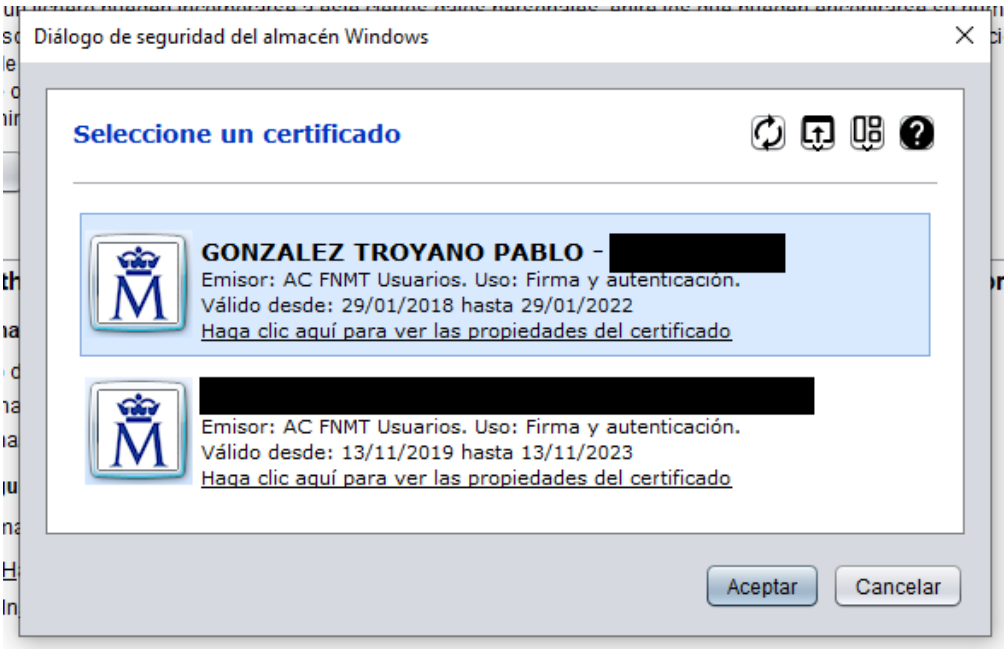
Seleccionamos la opción de *Hacer la firma visible dentro del PDF* y hacemos clic en *Firmar*. A continuación debemos seleccionar la ubicación donde queremos que sea visible la firma:



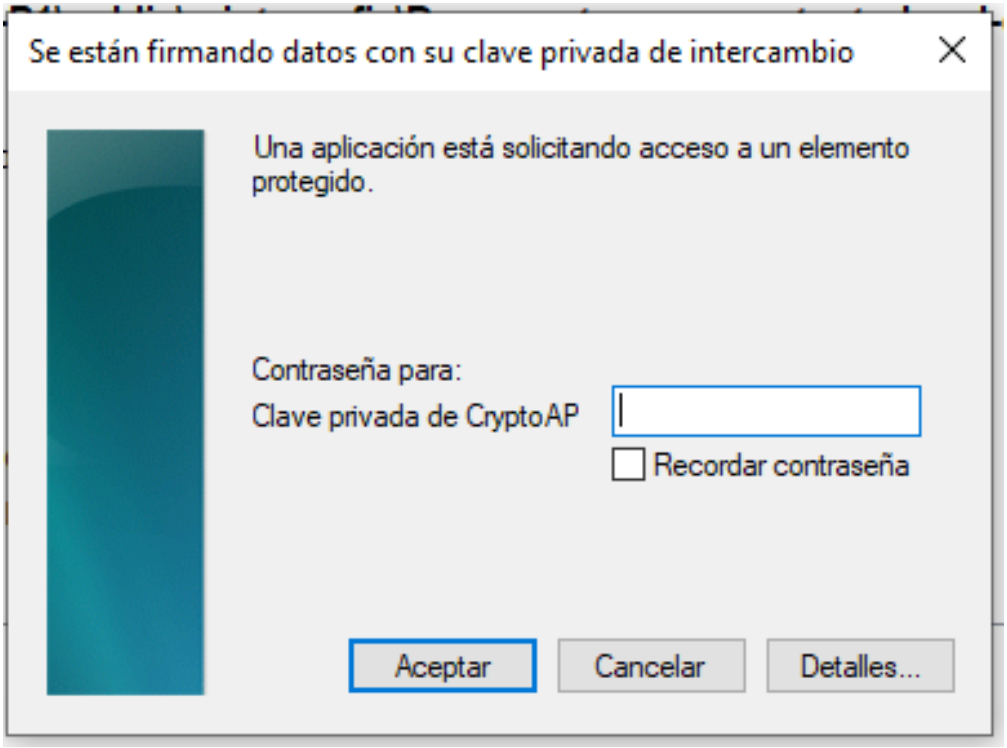
Hacemos clic en *Siguiente*. Veremos una ventana donde podremos cambiar el texto visible de la firma.



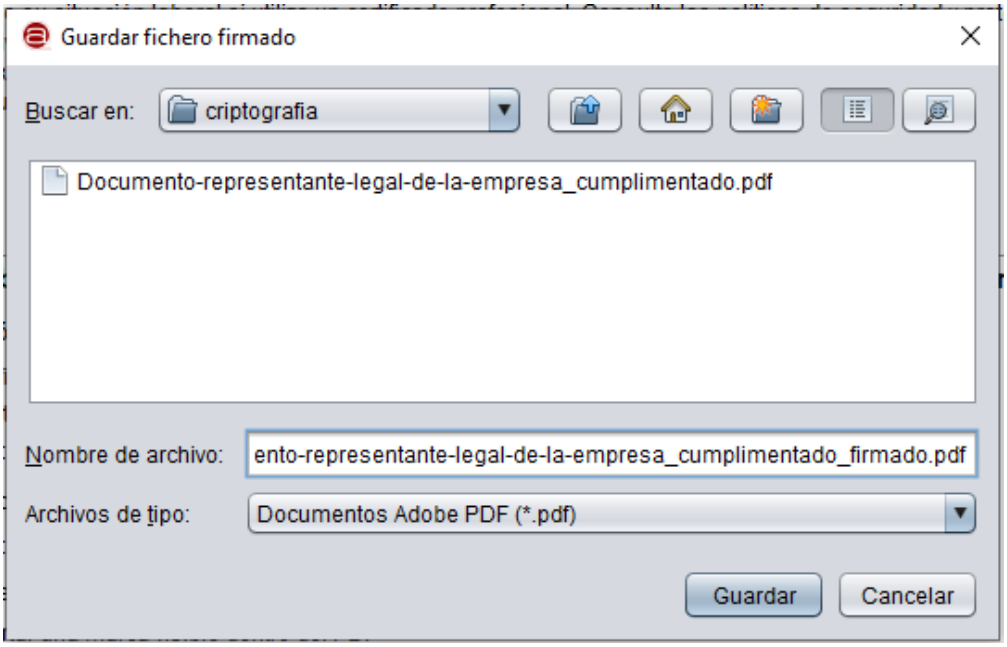
Seleccionamos el certificado con el que queremos firmar el documento:



Introducimos la contraseña que protege el uso del certificado:

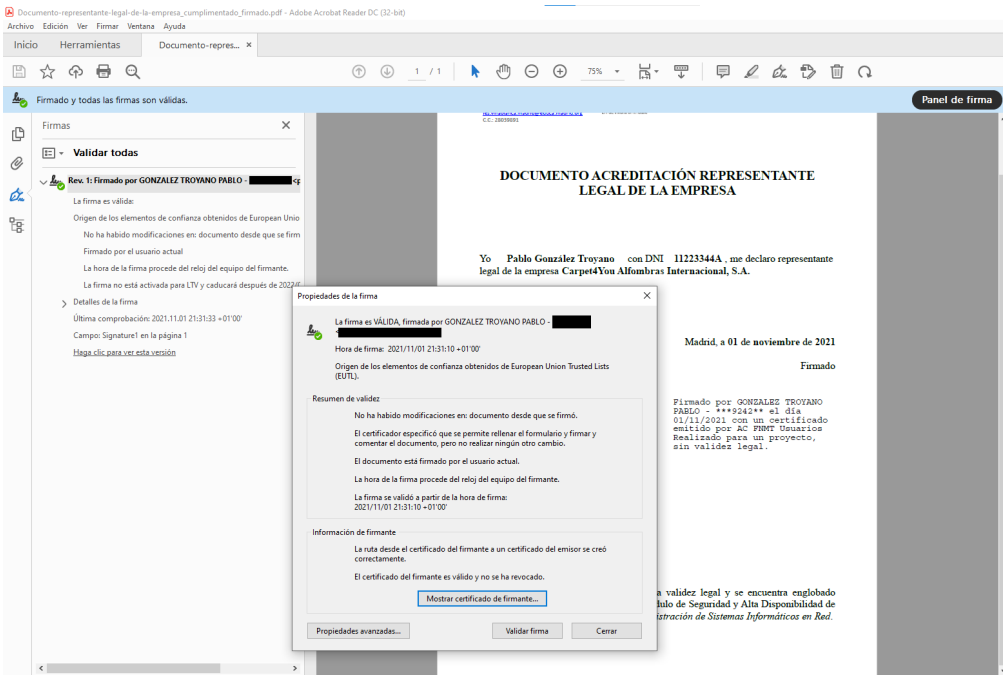


Elegimos la ubicación donde se guardará el archivo.



Veremos el mensaje de confirmación:

Si abrimos el fichero con un lector de PDF veremos los detalles de la firma:



Nota: En esta página se encuentran todos los documentos, a excepción del documento firmado con el certificado electrónico. También se encuentran disponibles el el Repositorio de Github.

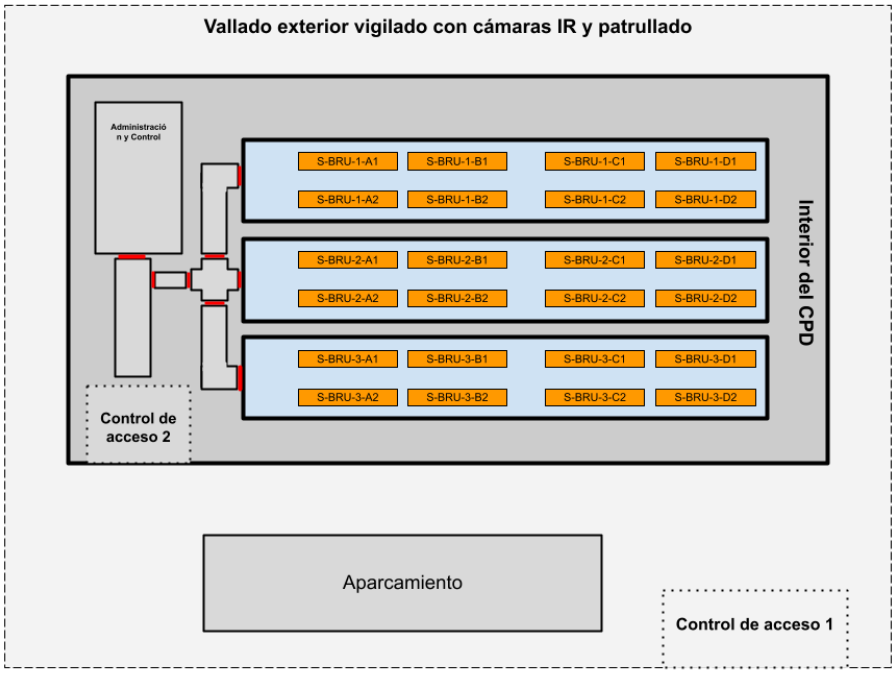
5.1. *Criptografía*
5.2. *Firma digital FNMT*

CAPÍTULO 6

Fallos de electricidad

6.1 Cálculo potencia del SAI

Viendo el plano del CPD Bruselas nos percatamos de la gran cantidad de equipos que puede alojar:



6.1.1 Cálculo del número de equipos

Cada zona en naranja tiene espacio para 3 racks estandar. Serán racks de 42U x 19 pulgadas, aproximadamente 2 metros de alto por 50cm de ancho.

Con un sencillo cálculo podemos obtener la cifra de hasta 72 racks que podemos tener funcionando en el CPD. La sección *D* de los racks[1] contará con los equipos de conectividad y balanceo de carga entre los servidores. La comunicación con el exterior se realiza en los *border routers*, situados en la planta sótano del edificio.

En este momento se estima que únicamente se está utilizando aproximadamente la mitad del espacio. Por tanto tenemos unos 35 racks que asegurar.

Aunque estos racks tienen hasta 42U para el despliegue de equipos,se están utilizando 30, evitando situar los equipos en las posiciones inferiores para evitar que las trabajadoras y trabajadores tengan que agacharse y mantener posiciones poco ergonómicas.

Importante: Por tanto tenemos 35 racks y 30 Us = 1050 U disponibles

No todos los equipos ocupan 1U, unos 300 aproximadamente ocupan 2U, los dedicados al almacenamiento en Hadoop. Los resultados son: 600U ocupadas por 300 equipos dedicados al almacenamiento, 350U con 350 equipos dedicados al procesamiento y 100U ocupadas por 100 equipos dedicados a la interconexión.

6.1.2 Cálculo de la potencia de los equipos

En la elección de los dispositivos se ha tenido en cuenta la eficiencia y el consumo energético.

Se toma una media de 200W por equipo. Los switches y equipos de conectividad consumen menos que los equipos de almacenamiento, y estos a su vez menos que los equipos de procesamiento.

Importante: Tenemos por tanto 200W * 750 equipos = 150 000 W

6.1.3 Cálculo de la capacidad necesaria de respaldo

El objetivo de est CPD es estar siempre operativo. En cualquier caso, la empresa puede permitirse durante un espacio limitado del tiempo la pérdida de un CPD sin que esto afecte a las operaciones visibles de la empresa. El SLO[2] es del 100 %, pero el SLA[3] acordado con la ejecutiva de la empresa es menor, del 99,5 %. Tener un SLA del 99,5 % significa no estar más de 1,8 días fuera de servicio en un periodo de 1 año natural.

Sin embargo, gracias a la característica distribuida de la empresa y a nuestro sistema de control DNS podríamos redirigir algunos servicios a otro CPD mientras dure la incidencia en un CPD dado.

Los servicios internos podrían verse afectados, sobre todo los menos cruciales. El objetivo crucial es que la parte visible de la empresa (web, portales de relaciones con clientes) no se vea afectado y la diferencia de rendimiento sea mínima.

Por tanto, la capacidad energética de respaldo se ha calculado para alimentar los sistemas durante aproximadamente 3h para los equipos de conectividad principal y *critical* (gestión interna, gestión de grabaciones y red interna).

Para el resto de equipos, con mantenimiento de 1h hora la empresa ha calculado que será suficiente.

[1] Cada conjunto de 3 racks está identificado por un código único, que no solo lo identifica a nivel de CPD, sino de toda la empresa. De esta forma *S-BRU-2-C1* significa *Servidor, en CPD BRUselas, sala 2, sección C, conjunto 1*. En Bilbao la nomenclatura es similar, cambiando *BRU* por *BIO*, que es el distintivo del aeropuerto de la ciudad.

[2] *Service Level Objective*, Objetivo de nivel de servicio. Lo que se espera que el servicio esté disponible.

[3] *Service Level Agreement*, Acuerdo de nivel de servicio. Aunque se utiliza en acuerdos comerciales, en Carpet4You la utilizamos para definir el mínimo de tiempo que debe estar completamente operativo el CPD.

En primera instancia se ha pensado en las soluciones UPS de AEG, de la gama PROTECT 4. Esta gama está especialmente pensado para Data Centers e infraestructuras crítcas. Como curiosidad, son los que utilizan en el provedor de servicios de hosting alemán Strato[4] .

Si se utilizara esta gama sería necesario instalarlos en una sala especialmente dedicada en el sotáno, debido a su peso (más de 3 toneladas) y sus dimensiones (2100x1915x960 mm, Ancho, Alto, Fondo).

Importante: Por tanto, calculamos que: * 1h de actividad para un armario no crítico. Resistencia calculada de 200W * 30U = 6000W. * 3h de actividad para un armario crítico. Resistencia calculada de 200W * 20U = 4000W.

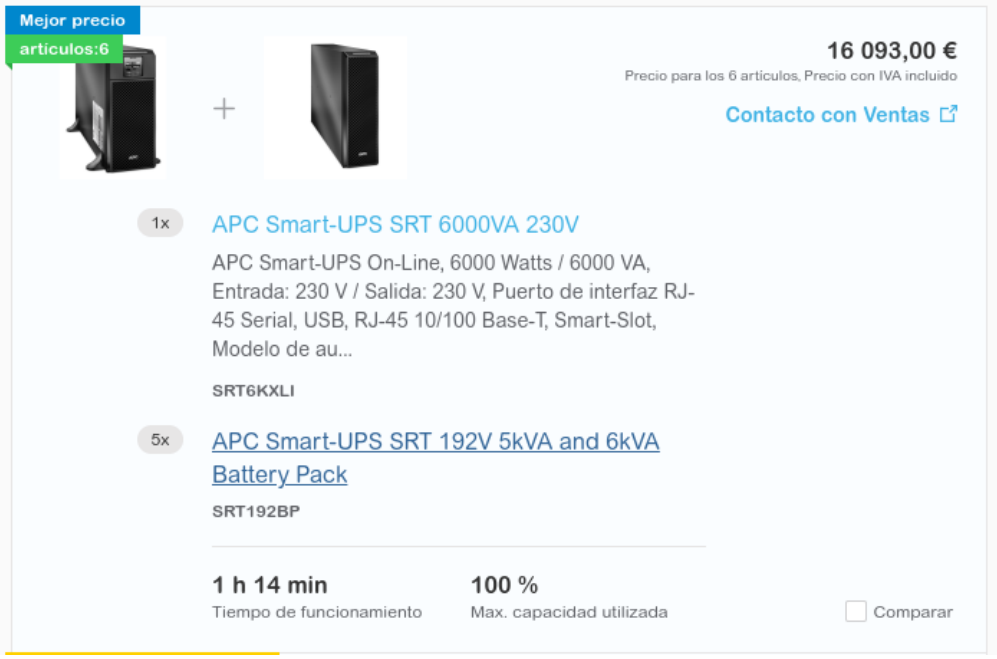
Notas al pie de página

6.2 Elección de dispositivos SAI

Carpet4You se decanta por los productos SAI de la marca APC, filial de la empresa Schneider Electric.

6.2.1 Armario no crítico

Para los dispositivios SAI de los armarios no críticos tenemos la configuración aquí mostrada:



El conjunto lo dividimos en 2:

- Por un lado, tenemos la unidad central, a la que se conectan los dispositivos en sí. Es el modelo Smart-UPS SRT de APC 6000 VA 230 V, número de serie SRT6KXLI. Accede a los detalles del producto en este enlace.

[4] En esta página se puede obtener la referencia del cliente.

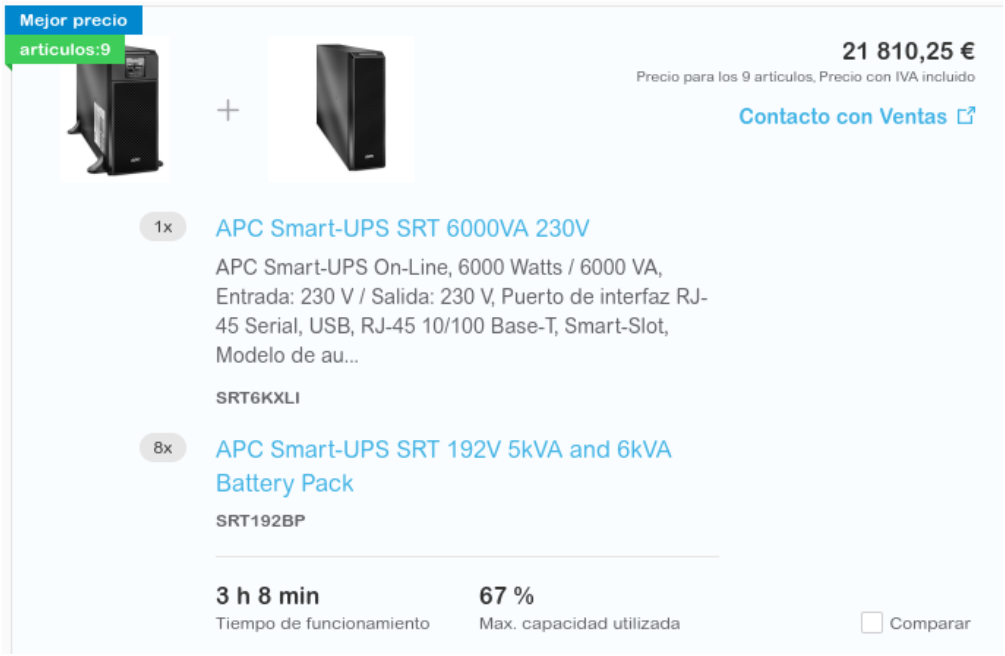
- Por otro lado, tenemos las baterias que vamos añadiendo. Podemos añadir hasta 10 conjuntos más. En nuestro caso añadimos 5 conjuntos adicionales más. Accede a los detalles del producto en este enlace.

En la siguiente tabla tenemos los detalles:

Producto	Cantidad	Precio/Unidad	Precio total
SRT6KXLI	1	6 564,25 €	6 564,25 €
SRT192BP	5	1 905,75 €	9 528,75 €
Coste total: 16 093,00 €			

6.2.2 Armario crítico

Para los dispositivios SAI de los armarios no críticos tenemos la configuración aquí mostrada:



El conjunto lo dividimos en 2:

- Por un lado, tenemos la unidad central, a la que se conectan los dispositivos en sí. Es el modelo Smart-UPS SRT de APC 6000 VA 230 V, número de serie SRT6KXLI. Accede a los detalles del producto en este enlace.
- Por otro lado, tenemos las baterias que vamos añadiendo. Podemos añadir hasta 10 conjuntos más. En nuestro caso añadimos 8 conjuntos adicionales más. Accede a los detalles del producto en este enlace.

En la siguiente tabla tenemos los detalles:

Producto	Cantidad	Precio/Unidad	Precio total
SRT6KXLI	1	6 564,25 €	6 564,25 €
SRT192BP	8	1 905,75 €	15 246,00 €
Coste total: 21 810,25 €			

6.1. *Cálculo potencia del SAI*

6.2. *Elección de dispositivos SAI*

CAPÍTULO 7

IP y direccionamiento

7.1 Direccionamiento IP de la empresa (general)

7.1.1 Rangos de IP asignados

Rangos públicos

La empresa dispone de una serie de rangos IP asignados por el RIR RIPE. Esto permite la conectividad indenpendiente y segura. La gestión propia asegura la optimización máxima de las rutas. Carpet4You dispone del AS número 88757. Este *Autonomous Number* tiene una serie de rangos IP asignados:

- Rangos IPv6:
  - Rango /48 1 –> 2001:db8:3c4d::/48 usado para el CPD de Bilbao
  - Rango /48 2 –> 2001:db8:3c4e::/48 usado para el CPD de Bélgica
  - Rango /48 3 –> 2001:db8:3c4f::/48 en reserva, se planea utilizar subsegmentos para la conectividad hacia Internet de las sedes y experimentación del equipo de I+D+i

Atención: Nótese que los rangos IPv6 no son enrutables en Internet y corresponde y son subrangos del rango dedicado por IANA para la confección de documentación.

- Rango en IPv4: 100.65.65.0. Subdividido

Dirección de red	Usado en	Rango de IPs utilizable	IP de Broadcast
100.65.65.0	CPD Bilbao	100.65.65.1 - 100.65.65.62	100.65.65.63
100.65.65.64	CPD Bélgica	100.65.65.65 - 100.65.65.126	100.65.65.127
100.65.65.128	Reserva	100.65.65.129 - 100.65.65.190	100.65.65.191
100.65.65.192	Reserva	100.65.65.193 - 100.65.65.254	100.65.65.255

Atención: Nótese que el rango de IPv4 no es enrutable en Internet y corresponde al rango de las IPs asigadas a los Internet Service Providers (IPS) para el uso de CG-NAT.

Rangos privados

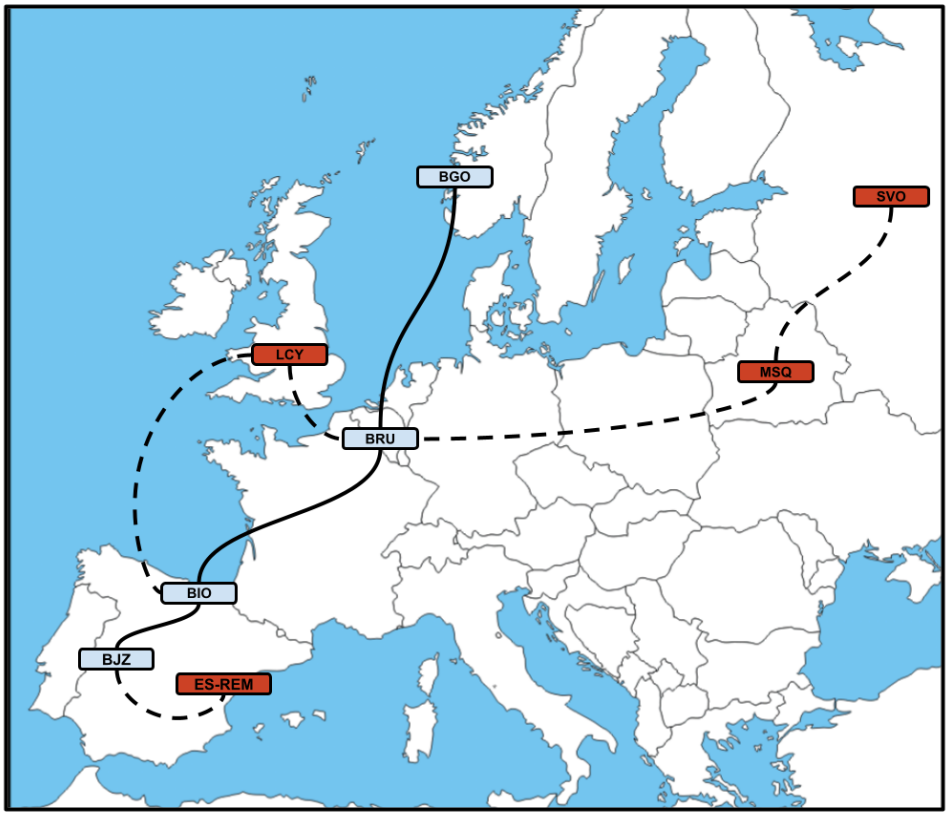
Los rangos privados están recogidos en el RFC1918 de la Internet Engineering Task Force.

En el caso de Carpet4You, se ha decicido utilizar el rango privado 10.0.0.0/8 para direccionamiento IP interno. La amplitud de este rango permite a la empresa crecer, mantener subredes dedicadas por sede y no tener problemas a futuro.

Dirección de red y VLANs	Usado en
10.201.0.0/16 ▪ 10.201.0XX.0/24 ▪ 10.201.1XX.0/24 ▪ 10.201.2XX.0/24	**Sede Badajoz (B1)** ▪ Rangos utilizados para Management ▪ Rangos utilizados para los diferentes dptos. ▪ Direcciones internas para servidores
10.202.0.0/16 ▪ 10.202.0XX.0/24 ▪ 10.202.1XX.0/24 ▪ 10.202.2XX.0/24	**Sede Bilbao (B2)** ▪ Rangos utilizados para Management ▪ Rangos utilizados para los diferentes dptos. ▪ Direcciones internas para servidores
10.203.0.0/16 ▪ 10.203.0XX.0/24 ▪ 10.203.1XX.0/24 ▪ 10.203.2XX.0/24	**Sede Bruselas (B3)** ▪ Rangos utilizados para Management ▪ Rangos utilizados para los diferentes dptos. ▪ Direcciones internas para servidores
10.204.0.0/16 ▪ 10.204.0XX.0/24 ▪ 10.204.1XX.0/24 ▪ 10.204.2XX.0/24	**Sede Bergen (B4)** ▪ Rangos utilizados para Management ▪ Rangos utilizados para los diferentes dptos. ▪ Direcciones internas para servidores
10.205.0.0/16 ▪ 10.205.1.0/24 ▪ 10.205.2.0/24 ▪ 10.205.4.0/24 ▪ 10.205.201.0/24 ▪ 10.205.202.0/24 ▪ 10.205.203.0/24 ▪ 10.205.204.0/24	**Trabajadores Remotos** ▪ Trabajadores Remotos en Rusia ▪ Trabajadores Remotos en Minsk ▪ Trabajadores Remotos en Reino Unido ▪ Trabajadores Remotos asignados a sede B1 ▪ Trabajadores Remotos asignados a sede B2 ▪ Trabajadores Remotos asignados a sede B3 ▪ Trabajadores Remotos asignados a sede B4

7.1.2 Conectividad física para las sedes

Conexión entre sedes



Nota: La imagen en formato SVG es accesible desde este enlace

Nota: El color rojo simboliza trabajadoras y trabajadores remotos. Las líneas discontínuas simbolizan conexiones utilizando infraestructura de Internet pública. Las líneas contínuas son líneas dedicadas.

Para las conexiones entre sedes se contratan fibras oscuras con diferentes proveedores:

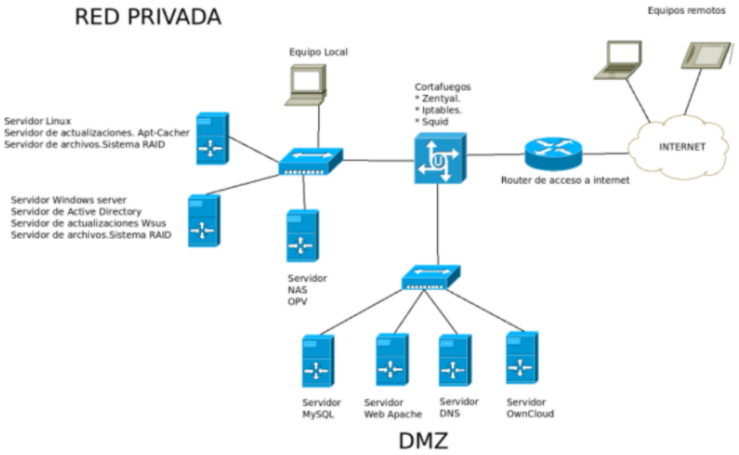
- Para la conexión entre Bajadoz (BJZ) y Bilbao (BIO) el proveedor es Correos Telecom.
- Para la conexión entre Bilbao (BIO) y Bruselas (BRU); así como entre Bruselas (BRU) y Bergen (BGO) está contratada con el proveedor Colt.

7.2 Direccionamiento IP de la sede

Tal y como podemos ver en el cuadro de IPs de la página de direccionamiento IP de toda la empresa, a la sede de bruselas le corresponde el siguiente rango:

Dirección de red y VLANs	Usado en
10.203.0.0/16 ▪ 10.203.0XX.0/24 ▪ 10.203.1XX.0/24 ▪ 10.203.2YY.XXX/32	**Sede Bruselas (B3)** ▪ Rangos utilizados para Management ▪ Rangos utilizados para los diferentes dptos. ▪ Direcciones internas para servidores

En tanto a los requisitos mínimos, tenemos el siguiente mapa de red proporcionado en las instrucciones de la práctica:



7.2.1 Hardware de red

Toda la infraestructura de la red de la sede estará compuesta por equipos de la gama *Unifi*, del fabricante Ubiquiti Networks.

Al igual que las cámaras y el control de acceso, toda la infraestructura es gestionable desde un único panel web.

Las funcionalidades de los equipos Unifi son equiparables a los archiconocidos *Cisco*. Una de las mayores diferencias radica en el menor precio de adquisición y mayor facilidad de mantenimiento. Los switches de Unifi trabajan a nivel 3, por lo que pueden enrutar tráfico de varias redes sin necesidad de switch.

Otra de las opciones a bajarar era *Sophos*, pero las licencias anuales son prohibitibas.

Nota: Es posible que Unifi no sea suficientemente potente en comparación con otras soluciones. Por ejemplo, en el análisis de tráfico encriptado.

Si la decisión final fuera mía, tuviera presupuesto y tiempo para conocer la solución me decantaría por la solución de Cisco Meraki. Combina la sencillez de Unifi con la potencia tradicional de Cisco.

7.2.2 VLANs - Management

Tal y como podemos ver en el cuadro anterior, tenemos disponibles IPs entre 10.203.001.0/16 hasta 10.203.099.0/16 para management.

Por comodidad, trabajaremos con redes /24. Entendemos como *Management* las direcciones necesarias para servicios internos: el propio equipamiento de red, teléfonos VoIP, cámaras y resto de equipamiento.

Las VLAN definidas para management son:

- **VLAN10**, rango IP 10.203.010.0/24. En esta red se incluirán los dispositivos de red.
- **VLAN11-20**, rangos IP 10.203.011.0/24 - 10.203.020.0/24. Se incluirán en estos rangos los teléfonos VoIP. Se reservará un subrango para cada departamento.
- **VLAN25**, rango IP 10.203.025.0/24. Se incluirán en esta red el hardware de control de acceso.
- **VLAN30**, rango IP 10.203.030.0/24. Se inclurán en este rango de IP las cámaras de seguridad.
- **VLAN50**, rango IP 10.203.050.0/24. A este rango pertenecerán los dispositivos de casting hacia TV y proyectores con capacidad inalámbrica.
- **VLAN99**, rango IP 203.099.0/24. Este rango estará dedicado a los invitados.

7.2.3 VLANs - Empleadas y empleados

Tal y como podemos ver en el cuadro anterior, tenemos disponibles IPs entre 10.203.100.0/16 hasta 10.203.199.0/16 para los equipos de empleadas y empleados.

A tener en cuenta: todos los departamentos tienen menos de 250 empleados/equipos. En caso de tener más empleados que IPs disponibles en un red tipo C, se utilizarán dos o más redes.

Todas las empleadas y empleados tendrán a su disposición una red inalámbrica para la conxión d sus dispositivos móviles y portátiles si lo tuvieran.

Siendo `Y` un número de departamento se crean las siguientes VLANs

- **VLAN1YY**, 10.203.1YY.0/24. A estas VLANs se conectarán los equipos propiedad de la empresa.
- **VLAN1(YY+50)**, 10.203.1(YY+50).0/24. A estas VLANs se conectarán los equipos propiedad de la empleada o empleado (BYOD).

7.2.4 VLANs - Servicios internos

Tal y como podemos ver en el cuadro anterior, tenemos disponibles IPs entre 10.203.200.0/16 hasta 10.203.250.0/16 para sericios internos. Se define 250 en tercer byte para que sea más secillo.

Se define la **VLAN222**, con rango de IP 10.203.222.0/24 para la zona DMZ. En ella se localizan el servidor MySQL, el servidor Apache, el servidor DNS, el servidor OwnCloud y los futuros servidores o equipos que cumplan la característica de estar detrás de la DMZ.

En cualquier caso, que estén dentro de algo que llamemos *DMZ* no significa que tengan todos los pueros abiertos. De hecho, por seguridad, solo tendán abiertos los estrictamente necesarios.

Se define la **VLAN203**, con rango de IP 10.203.203.0/24 para los equipos servidor que no estén dentro de la DMZ. Entre estos equipos figuran el servidor Windows (para AD y actualizaciones entre otros), así como el servidor Linux (APT-Cacher entre otros). También se incluye en esta VLAN el servidor NAS.

Nota: Se entiende que no es necesario indicar cada IP para cada equipo de la red.

La puerta de enlace tendrá una IP primaria (la de *management*) dentro de la VLAN10. A su vez, tendrá la primera IP en cada VLAN.

7.3 Configuración de dominios de la empresa

Toda la empresa se organiza en torno al dominio *Carpet4You.site*.

La web pública se encuentra en https://carpet4you.site.

Para los equipos internos se crean los siguientes subdominios DNS:

- *.corp.carpet4you.site*, sobre este subdominio se organizarán los recursos de la empresa que se utilizan directamente por los empleados. Lo que podríamos identificar como una especie de *frontend*.
- *.people.carpet4you.site*, sobre este subdominio se alojan los equipos cliente de las trabajadoras u trabajadores, siguiendo una nomenclatura definida para identificarlos.
- *.int.carpet4you.site*, dentro de este subdominio se organizarán los recursos de la empresa que funcionan en una capa de abstracción inferior.
- Los equipos físicos de los CPD, en caso de poder ser comunicados directamente desde el exterior (entiéndase exterior como una conexión SSH, siempre asegurada, limitada y autenticada) tendrán un subdominio que coincidirá con el CPD al que pertenecen. Por ejemplo, *s25.a1.1.bru.int.carpet4you.site* pertenece al servidor número 25, del bastidor A1, en la sala 1, del CPD de Bruselas.

7.1. *Direccionamiento IP de la empresa (general)*
7.2. *Direccionamiento IP de la sede*
7.3. *Configuración de dominios de la empresa*

CAPÍTULO 8

Servicios y certificados

8.1 Servidor SSH

A continuación se detalla el proceso de instalación y configuración del servidor SSH para un equipo de la empresa.

8.1.1 Máquina Virtual de trabajo

Se utilizará una máquina virtual con Ubuntu Server 18.04 como sistema operativo. Se le asignan 4 GB de RAM y 4 vCPUs. En tanto a la red, se configuran 2 adaptadores virtuales: * Adaptador 1, configurado en modo NAT para la conexión a internet. * Adaptador 2, confiugrado en modo solo-anfitrión, para la conexión SSH y a los servicios.

En tanto al usuario administrador utiliza la (poco segura) combinación user:user.

8.1.2 Instalación del servidor SSH

Para instalar el servidor SSH, si no estuviera instalado, debemos ejecutar el siguiente comando:

```
user@server-carpet:~$ apt update
user@server-carpet:~$ apt install openssh-server
```

Si lo acabamos de instalar debemos iniciarlo y permitir su inicio en el arranque del equipo:

```
user@server-carpet:~$ systemctl enable ssh
user@server-carpet:~$ systemctl start ssh
```

8.1.3 Configuración personalizada

Cambiar puerto de conexión

Para cambiar el puerto de conexión debemos editar el archivo */etc/ssh/sshd_config* para modificar la siguiente política:

```
Port 3200
```

Conexión mediante clave publica

Primero debemos haber generado un par de claves, como es nuestro caso. La clave pública debemos copiarla al archivo *~/.ssh/authorized_keys*. En nuestro caso la hemos generado desde el equipo cliente y la hemos copiado al servidor.

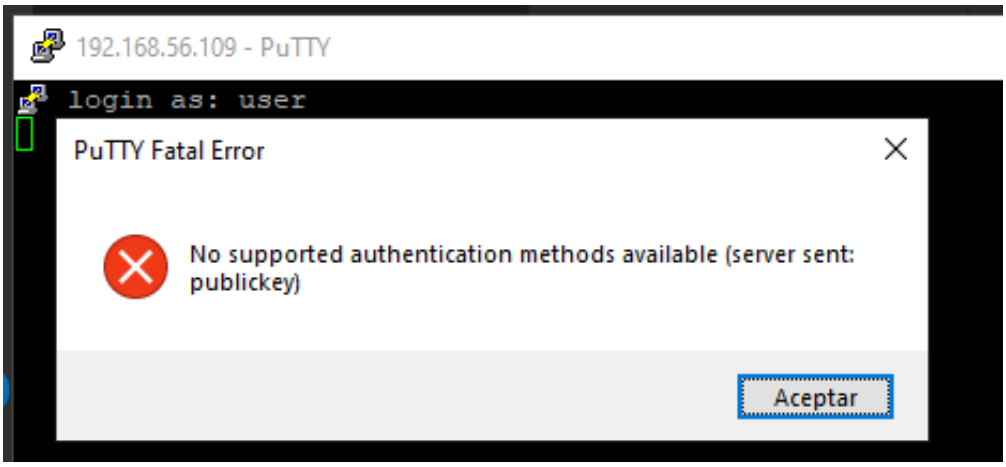
```
user@server-carpet:~/.ssh$ cat authorized_keys
ssh-rsa␣
↪AAAAB3NzaC1yc2EAAAADAQABAAACAQDMyXStDPWjrmR2WejGUFS6RN5TlWNOiXErOANYAwY2jeOA2i0EPgBNhIV+PEy+APUZzUJOE
USfPDIT5GcgeuHSMm3WwU+ax6IeJ8lYRJuVGP9cmiJFhVYSOF1FrjuC39vLuTmSPxr4kzU/
↪TronZmQ5jbwWuZfEtSAMEslaQST1t9HTZZWPXmyhyn
ya1f4tAxD34vOTDZ6Cc3N+xI3NuCBFZRd1fVDsOKyot3vhwpNi0VbVYF9uMFGQdgiTPVSRgrnbxTiUtfyvz4FnyWHRZl+x+k7n11zoj
zPAbss7Be8hK1Tmh68J5UfOPowWNWW1dG1RakyVuLd1t/eYTn8t+w7qnMp8mkosat6LW/ARD1BupCCmPe/
↪hTyysh5pMe66gb6R1yMBrHzokbd6EOv
C5f2Rlc+TYETujJronVIwznAeNuJB3F8U1v4PDcGpzDTAmHcTLyi7Mp32J2qbkjQ+lNO9vnr7eE+mWV86GB5KlxR7f0VTHPbso5gYbG
imV9/
↪K6AUqCb4HNDBcYs3D19OsWQFNTKCp80CZPl5XcUXCase3qbpnoInXkSUdNCYnkGskgzVZuiJmt7uxIGLaLoXXpBczN7Bj1LbVmZ48
w7Qq13Vwepzs8nEbcvLxD3Z0vN8t+e5kSxU3McyIqTQ== user@server-carpet
```

Lo siguiente que debemos hacer es modifcar el archivo */etc/ssh/sshd_config* para modificar las siguientes políticas:

```
PasswordAuthentication no
```

Debemos reiniciar el servicio tal y como hemos visto anteriormente.

Si intentamos conectarnos ahora (con el programa Putty en Windows) recibiremos un error.



Desconexión automática

Debemos modifcar el archivo */etc/ssh/sshd_config* para modificar las siguientes políticas:

```
ClientAliveInterval 60
```

Solo usuario "administrador"

Debemos modifcar el archivo */etc/ssh/sshd_config* para modificar las siguientes políticas:

```
AllowUsers administrador
```

No permitir acceso root

Debemos modifcar el archivo */etc/ssh/sshd_config* para modificar las siguientes políticas:

```
PermitRootLogin no
```

Prohibir acceso a usuario "invitado"

Debemos modifcar el archivo */etc/ssh/sshd_config* para modificar las siguientes políticas:

```
DenyUsers invitado
```

8.2 Servidor web

8.2.1 Instalar servidor web

Para instalar el servidor SSH, si no estuviera instalado, debemos ejecutar el siguiente comando:

```
user@server-carpet:~$ apt update
user@server-carpet:~$ apt install apache2
```

Si lo acabamos de instalar debemos iniciarlo y permitir su inicio en el arranque del equipo:

```
user@server-carpet:~$ systemctl enable apache2
user@server-carpet:~$ systemctl start apache2
```

8.2.2 Conectarse al servidor web

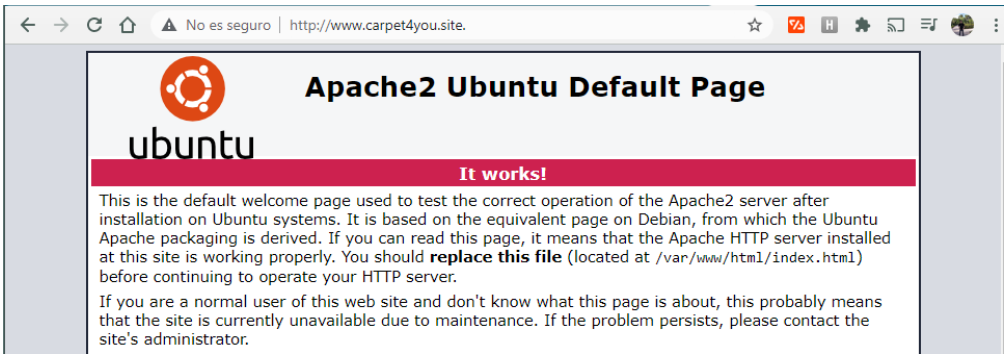
Modificar archivo hosts / añadir subdominio

En nuestro caso, al disponer de un dominio resoluble en Internet, hemos añadido el subdominio *www.carpet4you.site*.

Comprobaremos con el comando *dig* si ha sido añadido correctamente:

```
user@server-carpet:~$ dig www.carpet4you.site.

; <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> www.carpet4you.site.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30217
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.carpet4you.site.           IN      A

;; ANSWER SECTION:
www.carpet4you.site.    3600    IN      A       192.168.56.109

;; Query time: 111 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Oct 24 19:37:36 UTC 2021
;; MSG SIZE  rcvd: 64
```

Si ahora intentamos conectarnos a dicho dominio desde el navegador web veremos:



Nota: Si no tuviéramos un archivo disponible siempre podríamos editar el archivo hosts de nuestro equipo.

8.2.3 Generar certificado autofirmado

Para generar el certificado autofirmado podemos utilizar el siguiente comando:

```
user@server-carpet:~$ sudo openssl req -x509 -nodes -days 90 -newkey rsa:2048 -keyout /
↪etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt
```

Vamos a desgranar el comando:

- **openssl**, es el comando básico para la gestión de OpenSSL.
- **req**, indicamos que queremos usar el estándar X.509 de petición de firma de certificados (CSR).
- **-x509**, modificador de la opción anterior, con la que indicamos que queremos autofirmarlo en vez de generar una petición de firma a una entidad de certificación.

- **-nodes**, indica que no queremos proteger el certificado con una contraseña. Esto es importante puesto que Apache necesitará utilizar el certificado sin que un usuario/a tenga que introducir la contraseña simétrica con cada petición.
- **-days 90**, periodo de validez del certificado.
- **-newkey rsa:2048**, esto especifica que queremos generar un nuevo certificado y una nueva clave al mismo tiempo. No hemos creado la clave necesaria para firmar el certificado en un paso anterior, así que tenemos que crearla junto con el certificado. La parte rsa:2048 le indica que cree una clave RSA de 2048 bits.
- **-keyout**, este modificador indica a OpenSSL dónde guardar el archivo de clave privada generado que estamos creando.
- **-out**, indicamos dónde queremos guardar el certificado que estamos creando.

Nos pedirá una serie de datos que podremos ir completando con el teclado:

```
Generating a RSA private key
.......................+++++
.+++++
writing new private key to '/etc/ssl/private/apache-selfsigned.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Badajoz
Locality Name (eg, city) []:El Carrascalejo
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Carpet4You
Organizational Unit Name (eg, section) []:IT Management
Common Name (e.g. server FQDN or YOUR name) []:www.carpet4you.site
Email Address []:pablo@carpet4you.site
```

8.2.4 Configurar el sitio nuevo en Apache

Creamos el archivo:

```
user@server-carpet:~$ sudo nano /etc/apache2/sites-available/www.carpet4you.site.conf
```

En dicho archivo, añadimos el siguiente texto:

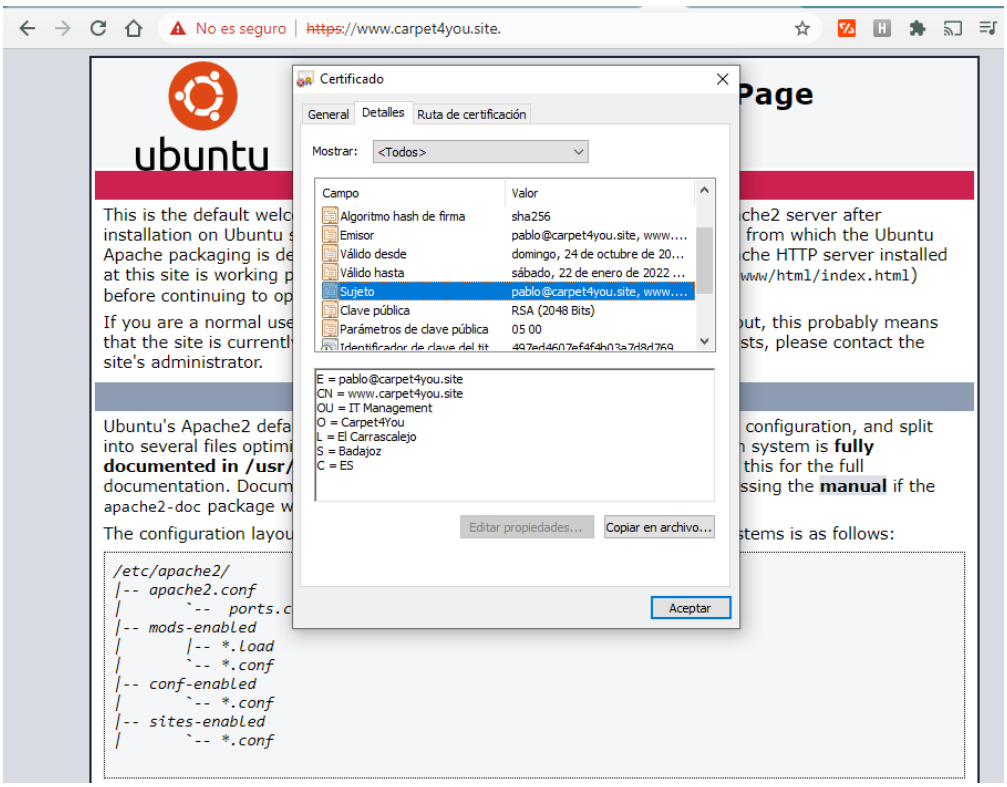
```
<VirtualHost *:443>
    ServerName www.carpet4you.site
    DocumentRoot /var/www/html
    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key
</VirtualHost>
```

También debemos activar una serie de módulos y configuraciones

```
user@server-carpet:~$ sudo a2enmod ssl
user@server-carpet:~$ sudo a2enmod headers
user@server-carpet:~$ sudo a2enconf ssl-params
```

Reiniciamos el servicio tal y como hemos visto de forma previa.

Ahora podremos visitar la web con el nuevo certificado y comprobar que funciona:



8.3 Servidor FTP

8.3.1 Instalación de proftpd

Actualizaremos los paquetes disponibles desde los repositorios:

```
user@server:~$ sudo apt update
```

Después instalaremos Samba:

```
user@server:~$ sudo apt install proftpd
```

8.3.2 Configuración del servicio

Editaremos el archivo de configuración

```
user@server:~$ sudo nano /etc/proftpd/proftpd.conf
```

Aquí modificamos/añadimos las siguientes entradas:

```
ServerName   "Carpet4You"

DefaultRoot /md0/home/usuario1 usuario1
DefaultRoot /md0/home/compartidoFTP usuario2
DefaultRoot /md0/home/compartidoFTP usuario4
```

Guardamos el archivo

> DefaultRoot /home/usuario1 usuario1 DefaultRoot /home/compartidoFTP usuario2 DefaultRoot /home/compartidoFTP usuario4

8.3.3 FTP Seguro

Generar certificado

Instalamos, si no lo estuviera ya, OpenSSL:

```
user@server:~$ sudo apt install openssl -y
```

Generamos la clave, introduciendo los datos que nos solicite el comando:

Importante: Fijaremos los bits de la misma en 2048, no en 1024 como se puede ver en el ejemplo del archivo de configuración.

```
user@server:~$ sudo openssl req -x509 -newkey rsa:2048 -keyout /etc/ssl/private/proftpd.
↪key -out /etc/ssl/certs/proftpd.crt -nodes -days 90
```

Configuramos los permisos correctos para la clave y el certificado:

```
user@server:~$ sudo chmod 600 /etc/ssl/private/proftpd.key
user@server:~$ sudo chmod 600 /etc/ssl/certs/proftpd.crt
```

Activar FTP Seguro

Volvemos a editar el archivo de configuración `/etc/proftpd/proftpd.conf`. En dicho archivo, descomentamos, si no lo estuviera ya, la siguiente línea:

```
Include /etc/proftpd/tls.conf
```

En este archivo, `/etc/proftpd/tls.conf`, añadimos o modificamos las sigueintes líneas:

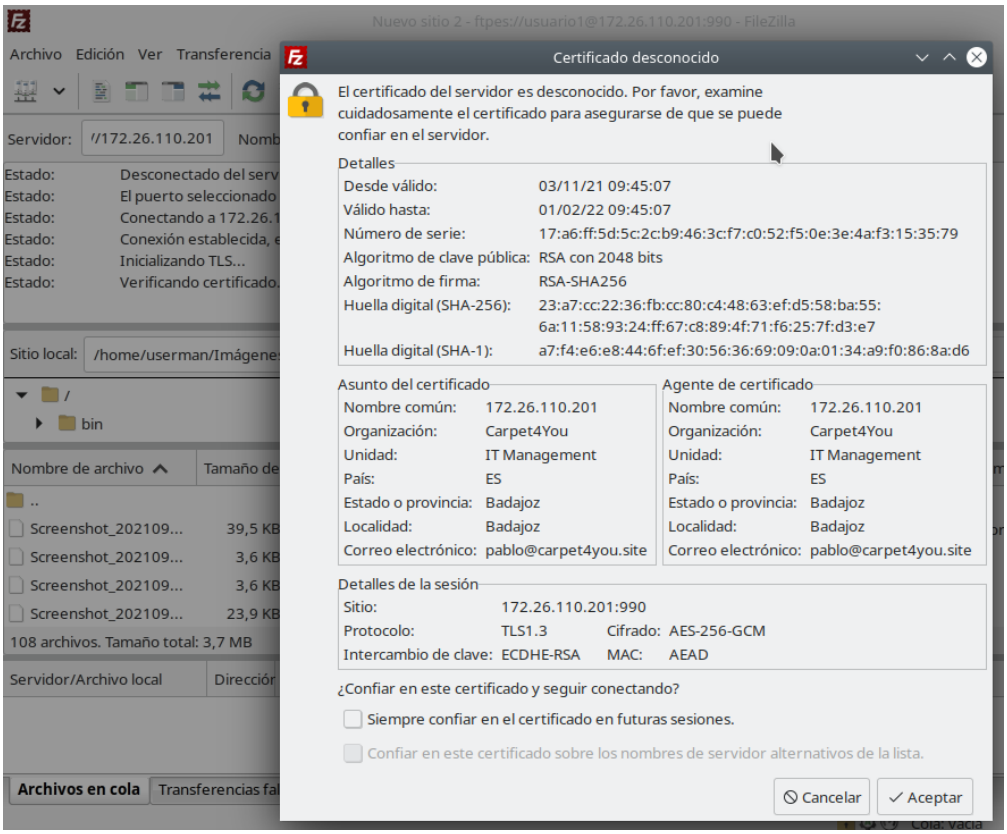
```
TLSRSACertificateFile /etc/ssl/certs/proftpd.crt
TLSRSACertificateKeyFile /etc/ssl/private/proftpd.key
TLSEngine on
TLSLog /var/log/proftpd/tls.log
TLSProtocolo SSLv23
TLSRequired off
TLSOptions NoCertRequest NoSessionReuseRequired
TLSVerifyClient off
```

Una vez hecho, debemos reiniciar el servicio:

```
user@server:~$ systemctl restart proftpd
```

8.3.4 Conexión al servidor

En el programa Filezilla introducimos los datos de conexión



8.4 Servidor NFS

8.4.1 Instalar servidor NFS

Actualizamos los paquetes disponibles en los repositorios e instalamos, si no lo estuviera ya, el paquete.

```
pablo@server:$/ sudo apt update
pablo@server:$/ sudo apt install nfs-common
```

8.4.2 Configuración NFS

Crear carpeta nueva

Crearemos una carpeta en el RAID1, que será la que compartiremos después:

```
pablo@server:$/ sudo mkdir /mnt/md0/compartidoNFS -p
```

Si ahora vemos los permisos, nos daremos cuenta de que el propietario de la carpeta es `root:root`. Por seguridad, NFS realiza las acciones con las credenciales `nobody:nogroup`. Para que los permisos de la carpeta coincidan con los que utilizará NFS, cambiaremos los mismos:

```
pablo@server:$/ sudo chown nobody:nogroup /mnt/md0/compartidoNFS
```

Añadir comparticiones

Editaremos el archivo `/etc/exports`, añadiendo:

```
/mnt/md0/compartidoNFS 192.168.56.102(rw,sync,no_root_squash,no_subtree_check)
/mnt/md0/compartidoNFS 192.168.56.0/24(r,sync,no_subtree_check)
```

Reiniciaremos el archivo

```
pablo@server:$/ sudo systemctl restart nfs-kernel-server
```

8.4.3 Configuración del cliente

Crear los puntos de montaje:

```
pablo@cliente:$/ sudo mkdir -p /nfs/compartidoNFS
```

8.5 Servidor SAMBA

8.5.1 Instalación de Samba

Actualizaremos los paquetes disponibles desde los repositorios:

```
user@server:~$ sudo apt update
```

Después instalaremos Samba:

```
user@server:~$ sudo apt install samba
```

Al instalar SAMBA, por defecto se iniciará el *daemon*. Para trabajar más cómodos y evitar problemas de seguridad hasta que esté completamente configurado, vamos a detener el servicio:

```
user@server:~$ sudo systemctl stop smbd.service
```

8.5.2 Configuración de Samba

Debemos conocer sobre qué adaptador vamos a trabajar, pues lo necesitaremos posteriormente para la configuración.

Para hacerlo, usaremos el siguiente comando:

```
user@server:~$ ip a

    1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default␣
↪qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
    2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group␣
↪default qlen 1000
        link/ether 08:00:27:d5:b1:16 brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 85970sec preferred_lft 85970sec
        inet6 fe80::a00:27ff:fed5:b116/64 scope link
        valid_lft forever preferred_lft forever
    3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group␣
↪default qlen 1000
        link/ether 08:00:27:62:5d:9d brd ff:ff:ff:ff:ff:ff
        inet 192.168.56.109/24 brd 192.168.56.255 scope global dynamic enp0s8
        valid_lft 470sec preferred_lft 470sec
        inet6 fe80::a00:27ff:fe62:5d9d/64 scope link
        valid_lft forever preferred_lft forever
```

En nuestro caso, la interfaz que usaremos será la *enp0s8*.

Copiaremos, para hacer *rollback* en caso de ser necesario, el archivo de configuración de Samba:

```
user@server:~$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.1.bak
```

Nota: Es muy interesante mantener las últimas versiones de los archivos de configuración. De esta manera, tenemos una especie de historial por si quisiéramos revertir los ajustes a una configuración anterior.

Edición del archivo de configuración

Truco: Puede ser interesante renombrar el archivo original y crear uno limpio para no tener comentarios «inútiles» en el archivo de configuración.

```
user@server:~$ sudo nano /etc/samba/smb.conf

   #Este archivo contendrá:
   [global]
       server string = Carpet4You_SambaServer
       workgroup = carpet4you.site
       interfaces = enp0s8
       bind interfaces only = yes
       log file = /var/log/samba/smb.log
       max log size = 10000
       ; Está en KiB, por defecto está en 1000. Logrotate recomendable.

       server role = standalone server

       ; Esta opción sincronizará la contraseña del comando smbpasswd con la contraseña␣
↪de UNIX en segundo plano
       unix password sync = yes
       passwd program = /usr/bin/passwd %u
       passwd chat = "*New Password:*" %n\n "*Reenter New Password:*" %n\n "*Password␣
↪changed.*"
       ;
       map to guest = bad user
```

Guardamos el archivo. Para comprobar si la configuración es corracta podemos usar el siguiente comando:

```
user@server:~$ sudo testparm
   Load smb config files from /etc/samba/smb.conf
   rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
   Loaded services file OK.
   Server role: ROLE_STANDALONE

   Press enter to see a dump of your service definitions
   [...]
```

8.5.3 Creación de usuarios

Vamos a crear dos usuarios Samba: *marta* y *juan*.

Usaremos los siguientes comandos:

```
user@server:~$ sudo adduser --shell /usr/sbin/nologin --home /md0/home/marta --ingroup␣
↪sambashare marta
user@server:~$ sudo adduser --shell /usr/sbin/nologin --home /md0/home/juan --ingroup␣
↪sambashare juan
```

Si como *root* o como usuarios con permisos para ejecutar *sudo* creáramos un archivo o directorio en las carpetas de los usuarios tendríamos un problema, pues el usuario final no podría editarlo.

Para remediarlo ejecutamos los siguientes comandos:

```
user@server:~$ sudo chown juan:sambashare /md0/home/juan
user@server:~$ sudo chown marta:sambashare /md0/home/marta
user@server:~$ sudo chmod -R 2770 /md0/home/juan/
user@server:~$ sudo chmod -R 2770 /md0/home/marta/
```

Ya tenemos creados los usuarios en el sistema operativo, pero no en Samba, para hacerlo:

```
# -a para añadir (add) el usuario
user@server:~$ sudo smbpasswd -a juan
# -e para activar (enable) el usuario
user@server:~$ sudo smbpasswd -e juan
user@server:~$ sudo smbpasswd -a marta
user@server:~$ sudo smbpasswd -e marta
```

8.5.4 Configurar las carpetas compartidas

Volveremos a modificar el archivo `/etc/samba/smb.conf`, añadiendo el siguiente contenido:

```
[marta]
    path = /md0/home/marta
    browseable = no
    read only = no
    force create mode = 0660
    force directory mode = 2770
    valid users = marta

[juan]
    path = /md0/home/juan
    browseable = no
    read only = no
    force create mode = 0660
    force directory mode = 2770
    valid users = juan
```

Truco: Con cada cambio en el archivo de configuración es recomendable ejecutar `testparm` Puede ser recomendable añadir un grupo o usuario administrador para la gestión Samba.

Crearemos una carpeta compartida global, la llamaremos `tolmundo`, también otra en `/home/compartidoNFS`:

```
user@server:~$ sudo mkdir -p /samba/tolmundo
user@server:~$ sudo mkdir -p /home/compartidoNFS
```

Añadiremos la siguiente sección al archivo `/etc/samba/smb.conf` para activar estas comparticiones:

```
[tolmundo]
    path = /samba/tolmundo
    browseable = yes
    read only = no
    force create mode = 0660
    force directory mode = 2770
    valid users = @sambashare user
[compartidoNFS]
    path = /home/compartidoNFS
    browseable = yes
    read only = no
    force create mode = 0660
    force directory mode = 2770
    valid users = @sambashare juan marta
```

8.5.5 Iniciar el servicio

Para iniciar el servicio ejecutamos:

```
user@server:~$ sudo systemctl start smbd.service
```

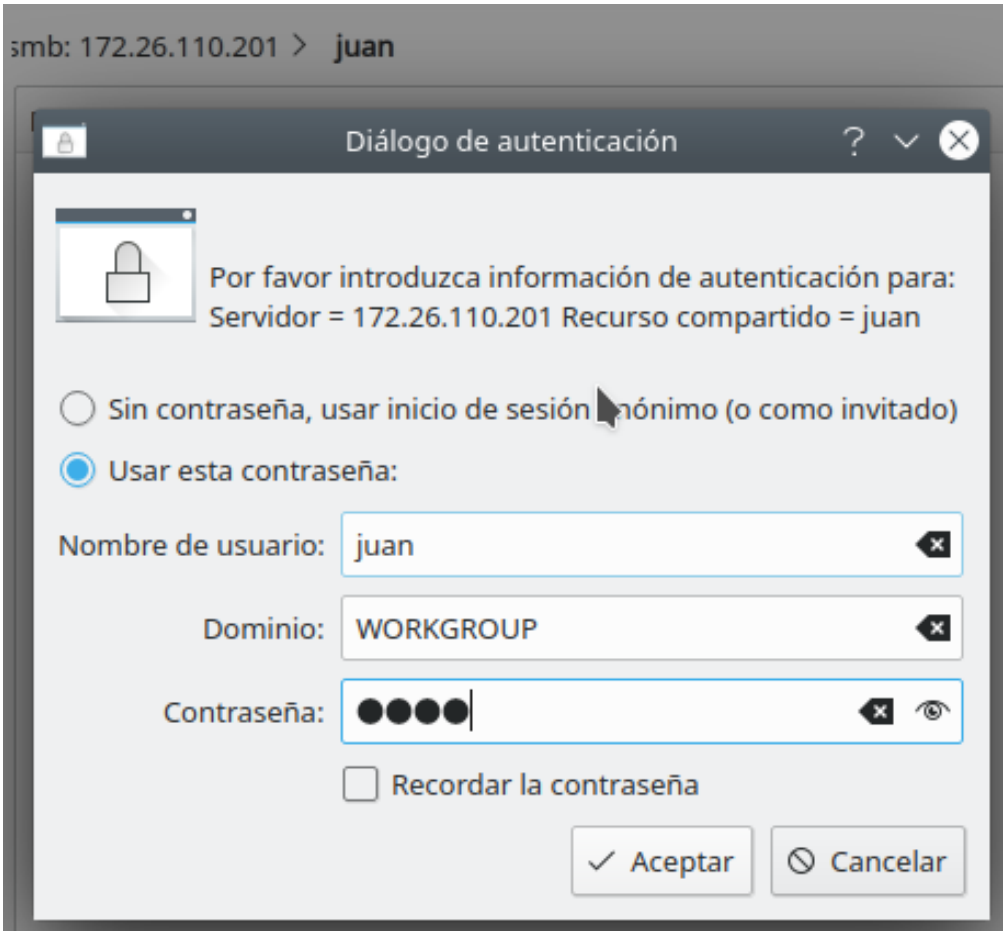
También debemos permitir el acceso a través del Firewall:

```
user@server:~$ sudo ufw allow samba
```

8.5.6 Conexión a carpeta

Para conectarnos a la carpeta usamos `smb://<IP-del-Servidor>/<Recurso>`, en Linux. En Windows abriremos el explorador de archivos y escriremos `\<IP-del-Servidor>/<Recurso>`.

Veamos un ejemplo en Linux:



8.6 Servidor Rsync

8.6.1 Configuración del servicio

Por defecto, en la mayoría de los sistemas Unix está instalado Rsync. Pero sólo es utilizable como cliente.

Si solicitamos el *status* del servicio veremos que nos indica como falta el archivo `/etc/rsyncd.conf`

```
root@server-carpet:/home/user# systemctl status rsync.service
     rsync.service - fast remote file copy program daemon
       Loaded: loaded (/lib/systemd/system/rsync.service; enabled; vendor preset:␣
↪enabled)
       Active: inactive (dead)
    Condition: start condition failed at Wed 2021-11-03 11:14:46 UTC; 2min 32s ago
               └─ ConditionPathExists=/etc/rsyncd.conf was not met
```

Crearemos dicho archivo, en el que añadiremos:

```
lock file = /var/run/rsync.lock
log file = /var/log/rsyncd.log
```

(continué en la próxima página)

(proviene de la página anterior)

```
pid file = /var/run/rsyncd.pid

[rsync]
    path = /home/programster/code
    comment = Archivos_Carpet4You
    uid = user
    gid = user
    read only = no
    list = yes
    auth users = user
    secrets file = /etc/rsyncd.secrets
    hosts allow = 172.26.0.0/255.255.0.0
```

La autenticación la realizaremos mediante clave SSH, siguiendo los pasos descritos en *Servicio Rsync automatizado*.

Reiniciaremos el servicio para aplicar los cambios:

```
root@server-carpet:/ systemctl restart rsync.service
```

8.6.2 Configuración de autenticación

Generar clave SSH

Por motivos de seguridad **no vamos a usar la misma clave SSH**. Por motivos intrínsecos a la ejecución del comando (debe ejecutarse de forma automática, sin interacción del usuario) la clave no debe tener contraseña simétrica.

Desde el cliente, vamos a generarla. uando nos pida introducir contraseña, haremos clic en Intro para no fijar ninguna:

```
user@cliente:~$ ssh-keygen -t rsa
```

La guardaremos en `~/.ssh/rsync`.

Copiar clave pública a servidor

Iniciando en el propio servidor (mediante SSH, por ejemplo), añadimos la clave publica al archivo `/home/user/.ssh/authorized_keys`. Después de copiarla tendremos, al menos, dos clave:

- La clave pública para el inicio SSH «típico».
- La clave pública que utilizaremos para la autenticación contra Rsync.

Probar conexión a carpeta

Para comprobar si funciona Rsync debemos generar algunos archivos y después comprobar si se copian.

```
user@cliente:~$ sudo rsync -avRh -e "ssh -i /home/user/.ssh/rsync" prueba/ user@172.26.
↪110.201:/rsync/
```

8.6.3 Tarea cron

Añadiremos la tarea crontab con el siguiente comando:

```
user@cliente:~$ sudo su #Necesitamos que la tarea la ejecute root
user@cliente:~$ crontab -e

# En el archivo que se nos abre añadimos el siguiente comando:
    */15 * * * * sudo rsync -avRh -e "ssh -i /home/user/.ssh/rsync" prueba/ user@172.26.
↪110.201:/rsync/
```

8.6.4 Limitar acceso desde IP cliente

Como medida de seguridad adicional, limitaremos el uso de la clave pública. Indicaremos que únicamente se pueda utilizar desde el equipo cliente. Para identificar al equipo usaremos su clave pública.

```
from="<IP-del-Cliente>" ssh-rsa <Clave-SSH> <Comentario-SSH>
```

8.7 Convertirnos en Autoridad de Certificación

8.7.1 Generar certificado AC y confianza

Generar la clave privada de la Autoridad de Certificación. Nos solicitará una contraseña para protegerla.

```
user@server-carpet:~$ openssl genrsa -des3 -out CA_Carpet4You.key 2048
```

Generamos el certificado raíz para nuestra AC:

```
user@server-carpet:~$ openssl req -x509 -new -nodes -key CA_Carpet4You.key -sha256 -days␣
↪365 -out CA_Carpet4You.pem
```

Nos solicitará la contraseña de nuestra clave privada de AC, así como una serie de datos para el certificado raíz:

```
Enter pass phrase for CA_Carpet4You.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Badajoz
Locality Name (eg, city) []:El Carrascalejo
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Carpet4You Trust
Organizational Unit Name (eg, section) []:Trust Service Management
Common Name (e.g. server FQDN or YOUR name) []:AC Carpet4You Trust
Email Address []:pablo@carpet4you.site
```

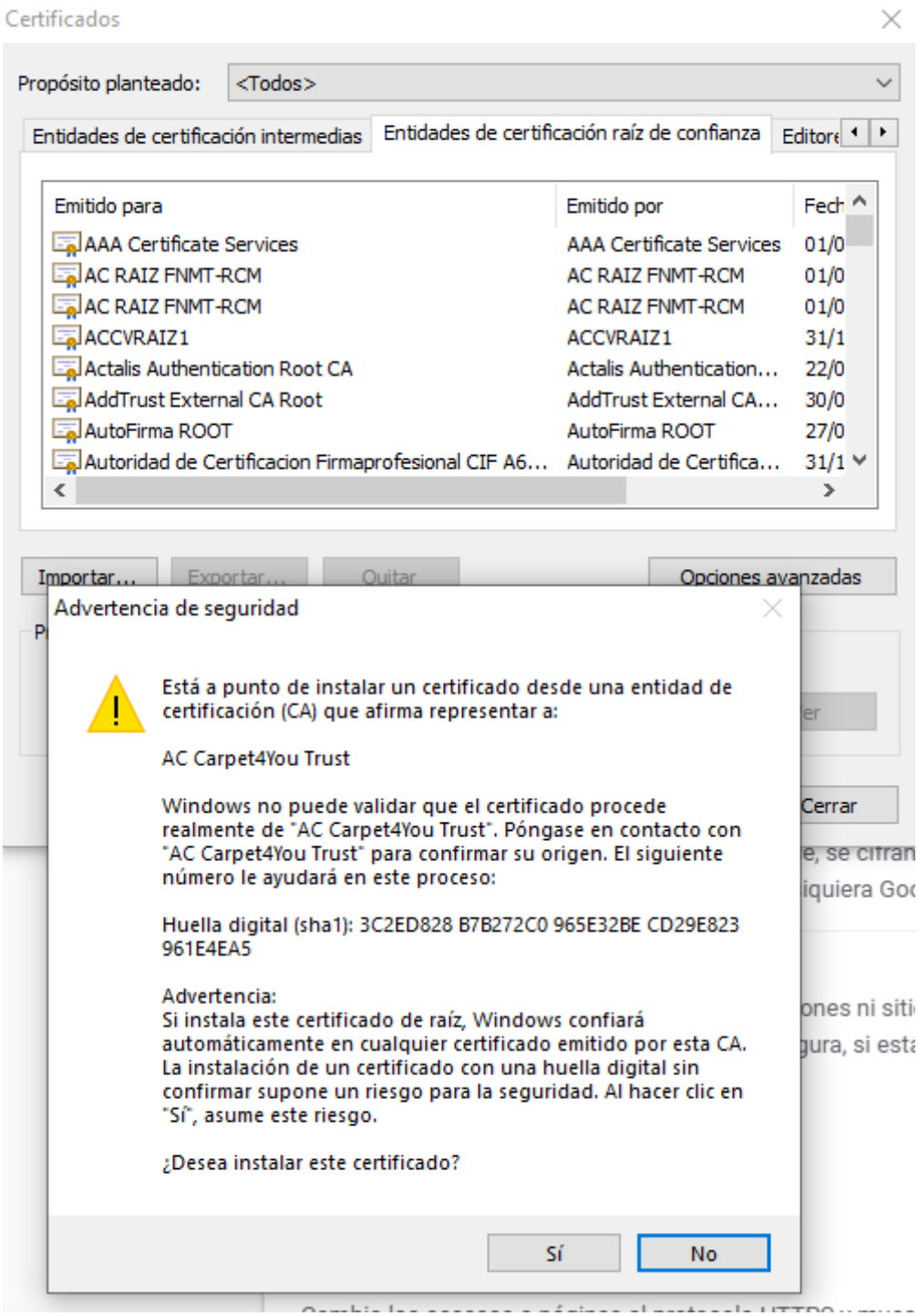
8.7.2 Importar certificado AC en dispositivo

Normalmente no debemos importar ningún certificado raíz puesto que en el Sistema Operativo ya vienen añadidos. En nuestro caso, debemos importarlo manualmente.

Para importar el certificado debemos navegar en los ajustes del navegador Chrome hasta chrome://settings/security. Una vez aquí hacemos clic en *Gestionar certificados*.

En la pantalla que nos aparece debemos desplazarnos hasta la sección *Entidades de certificación raíz de confianza* y hacer clic en Importar.

Seleccionamos el archivo *CA_Carpet4You.pem* generado de forma previa. Veremos un aviso al importarlo:


Certificados
Propósito planteado:
<Todos>
Entidades de certificación intermedias
Entidades de certificación raíz de confianza
Editore
Emitido para
Emitido por
Fech
AAA Certificate Services
AAA Certificate Services
01/0
AC RAIZ FNMT-RCM
AC RAIZ FNMT-RCM
01/0
AC RAIZ FNMT-RCM
AC RAIZ FNMT-RCM
01/0
ACCVRAIZ1
ACCVRAIZ1
31/1
Actalis Authentication Root CA
Actalis Authentication...
22/0
AddTrust External CA Root
AddTrust External CA...
30/0
AutoFirma ROOT
AutoFirma ROOT
27/0
Autoridad de Certificacion Firmaprofesional CIF A6...
Autoridad de Certifica...
31/1
Importar...
Exportar...
Quitar
Opciones avanzadas
Cerrar
Advertencia de seguridad
Está a punto de instalar un certificado desde una entidad de certificación (CA) que afirma representar a:
AC Carpet4You Trust
Windows no puede validar que el certificado procede realmente de "AC Carpet4You Trust". Póngase en contacto con "AC Carpet4You Trust" para confirmar su origen. El siguiente número le ayudará en este proceso:
Huella digital (sha1): 3C2ED828 B7B272C0 965E32BE CD29E823 961E4EA5
Advertencia:
Si instala este certificado de raíz, Windows confiará automáticamente en cualquier certificado emitido por esta CA. La instalación de un certificado con una huella digital sin confirmar supone un riesgo para la seguridad. Al hacer clic en "Sí", asume este riesgo.
¿Desea instalar este certificado?
Sí
No

8.7.3 Creción de certificado firmado por nuestra CA

Private key

Crearemos nuestra clave privada para el servidor:

```
user@server-carpet:~$ openssl genrsa -out www.carpet4you.site.key 2048
```

CSR

Iniciamos una *Certificate Signing Request* (CSR):

```
user@server-carpet:~$ openssl req -new -key www.carpet4you.site.key -out www.carpet4you.
↪site.csr
```

Archivo de configuración

Lo siguiente que haremos es crear el certificado utilizando la CSR, la clave privada de CA, el certificado de nuestra CA y un certificado de configuración que vamos a crear a continuación.

En este archivo, que llamaremos *www.carpet4you.site.ext* añadiremos el siguiente contenido:

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = www.carpet4you.site
```

Generar certificado final

```
openssl x509 -req -in www.carpet4you.site.csr -CA CA_Carpet4You.pem -CAkey CA_Carpet4You.
↪key -CAcreateserial \
-out www.carpet4you.site.crt -days 90 -sha256 -extfile www.carpet4you.site.ext
```

Ahora tendremos varios archivos:

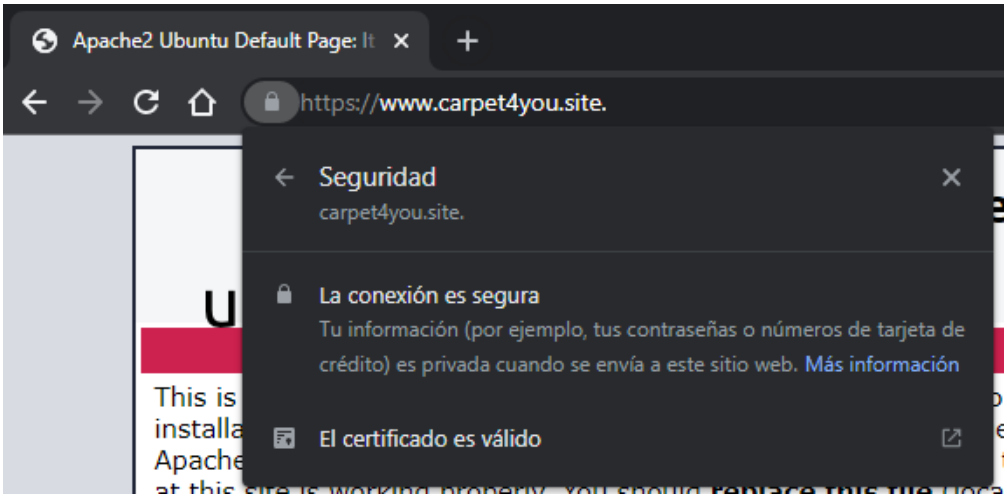
```
user@server-carpet:~$ ll ww*
-rw-rw-r-- 1 user user 1570 oct 24 21:30 www.carpet4you.site.crt
-rw-rw-r-- 1 user user 1147 oct 24 21:21 www.carpet4you.site.csr
-rw-rw-r-- 1 user user  210 oct 24 21:28 www.carpet4you.site.ext
-rw------- 1 user user 1679 oct 24 20:47 www.carpet4you.site.key
```

Utilizar certificado en Apache

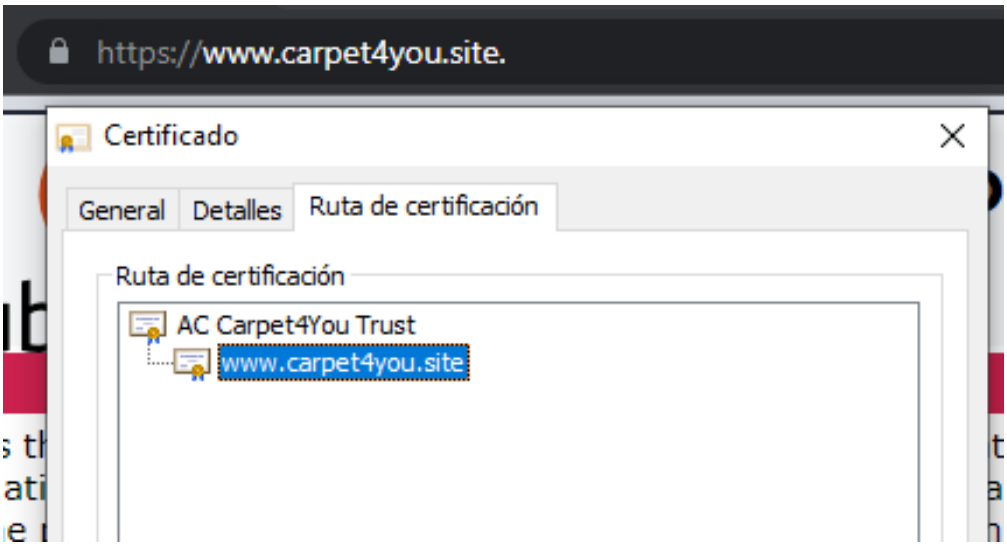
Modificamos el archivo */etc/apache2/sites-available/www.carpet4you.site.conf* para que pase a ser de la siguiente manera:

```
<VirtualHost *:443>
    ServerName www.carpet4you.site
    DocumentRoot /var/www/html
    SSLEngine on
    SSLCertificateFile /home/user/www.carpet4you.site.crt
    SSLCertificateKeyFile /home/user/www.carpet4you.site.key
</VirtualHost>
```

Ahora no aparecerá ningún error al cargar la página:



Si hacemos clic en los detalles del certificado para ver la ruta de certificación veremos:



8.8 Conseguir certificado Let's Encrypt

En esta página podremos ver información sobre cómo funciona el servicio ofrecido por Let's Encrypt. Sin duda, es una gran evolución en la seguridad de Internet.

8.8.1 Seleccionar dominios

Lo primero que debemos hacer es seleccionar para qué dominios vamos a generar el/los certificados. Debemos tener en cuenta que Let's Encrypt solo ofrece certificados *DV*, *Domain Validated*, en inglés.

En nuestro caso serán dos los dominios para los que solicitaremos el certificado: `nas.corp.carpet4you.site`, `cloud.carpet4you.site`, `ftp.corp.carpet4you.site` y `www.carpet4you.site`.

8.8.2 Instalar utilidad

Comprobaremos que el gestor snap está instalado y en la última versión disponible. También eliminaremos, si lo tuviéramos instalado con otro gestor de paquetes, la utilidad certbot

```
user@server-carpet:~$ sudo snap install core; sudo snap refresh core
user@server-carpet:~$ sudo apt-get remove certbot
```

Una vez hemos comprobado que podemos instalar *snaps*, instalamos el *snap* que nos permitirá generar el certificado. También generaremos un enlace para asegurarnos de que encontrará el binario a la hora de ejecutar el comando.

```
user@server-carpet:~$ sudo snap install --classic certbot
user@server-carpet:~$ sudo ln -s /snap/bin/certbot /usr/bin/certbot
```

8.8.3 Solicitar *challenge*

El método de comprobación que tiene Let's Encrypt consiste en generar *challenges*, retos, para que los usuarios los completen y una vez confirmado, otorgar el certificado.

Esto es importante, pues de no ser así, cualquier persona podría generar certificados para cualquier dominio (con el consiguiente problema que esto supondría).

```
user@server-carpet:~$ sudo certbot certonly --manual \
                        --preferred-challenges dns
```

Al ejecutar el comando comienza el proceso. Al inicio, nos solicita los dominios para los que queremos generar el certificado:

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator manual, Installer None
Please enter in your domain name(s) (comma and/or space separated)  (Enter 'c'
to cancel): www.carpet4you.site,nas.corp.carpet4you.site,ftp.corp.carpet4you.site,cloud.
↪carpet4you.site
```

Después de introducir los nombres de dominio nos aparecerá el siguiente mensaje:

```
Obtaining a new certificate
Performing the following challenges:
dns-01 challenge for cloud.carpet4you.site
dns-01 challenge for ftp.corp.carpet4you.site
dns-01 challenge for nas.corp.carpet4you.site
dns-01 challenge for www.carpet4you.site

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
NOTE: The IP of this machine will be publicly logged as having requested this
certificate. If you're running certbot in manual mode on a machine that is not
your server, please ensure you're okay with that.

Are you OK with your IP being logged?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: y
```

Nos proporcionará el *challenge*. Debemos añadir el registro tipo TXT para superar el reto.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please deploy a DNS TXT record under the name
_acme-challenge.cloud.carpet4you.site with the following value:

WTQAiXp_8WWagHsgWr0zbtUfM8JLzGU3YTyppeRe4ss

Before continuing, verify the record is deployed.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue
```

Pulsamos Enter y se nos mostrarán los siguientes retos, para los siguientes dominios:

```
Please deploy a DNS TXT record under the name
_acme-challenge.ftp.corp.carpet4you.site with the following value:

KZCH_bizmFToeL80CO9ZB8xNQrnkVKi124L8eVKS82I

Before continuing, verify the record is deployed.
(This must be set up in addition to the previous challenges; do not remove,
replace, or undo the previous challenge tasks yet. Note that you might be
asked to create multiple distinct TXT records with the same name. This is
permitted by DNS standards.)

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue

Please deploy a DNS TXT record under the name
_acme-challenge.nas.corp.carpet4you.site with the following value:

moHQsqoKoCtJWuRdlsE4ZVf27M_5sC8PGXjT3g6FYxI

Before continuing, verify the record is deployed.
(This must be set up in addition to the previous challenges; do not remove,
replace, or undo the previous challenge tasks yet. Note that you might be
asked to create multiple distinct TXT records with the same name. This is
```

(continué en la próxima página)

(proviene de la página anterior)

```
permitted by DNS standards.)

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue

Please deploy a DNS TXT record under the name
_acme-challenge.www.carpet4you.site with the following value:

JKLQaxpDRPVFB_oIMQgU5Thir78RJ49w2_BHmu7KUr8

Before continuing, verify the record is deployed.
(This must be set up in addition to the previous challenges; do not remove,
replace, or undo the previous challenge tasks yet. Note that you might be
asked to create multiple distinct TXT records with the same name. This is
permitted by DNS standards.)

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue
```

Pasados unos segundos, el sistema comprueba si los registros han sido añadidos:

```
Press Enter to Continue
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
/etc/letsencrypt/live/www.carpet4you.site/fullchain.pem
Your key file has been saved at:
/etc/letsencrypt/live/www.carpet4you.site/privkey.pem
Your cert will expire on 2022-01-25. To obtain a new or tweaked
version of this certificate in the future, simply run certbot
again. To non-interactively renew *all* of your certificates, run
"certbot renew"
- If you like Certbot, please consider supporting our work by:

Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
Donating to EFF:                    https://eff.org/donate-le
```

En la carpeta `/etc/letsencrypt/live/www.carpet4you.site/` tendremos los certificados y demás:

```
root@lets-encrypt-1:/etc/letsencrypt/live/www.carpet4you.site# ll
total 12
drwxr-xr-x 2 root root 4096 Oct 27 07:14 ./
drwx------ 5 root root 4096 Oct 27 07:14 ../
-rw-r--r-- 1 root root  692 Oct 27 07:14 README
lrwxrwxrwx 1 root root   43 Oct 27 07:14 cert.pem -> ../../archive/www.carpet4you.site/
↪cert1.pem
lrwxrwxrwx 1 root root   44 Oct 27 07:14 chain.pem -> ../../archive/www.carpet4you.site/
↪chain1.pem
lrwxrwxrwx 1 root root   48 Oct 27 07:14 fullchain.pem -> ../../archive/www.carpet4you.
↪site/fullchain1.pem
```

(continué en la próxima página)

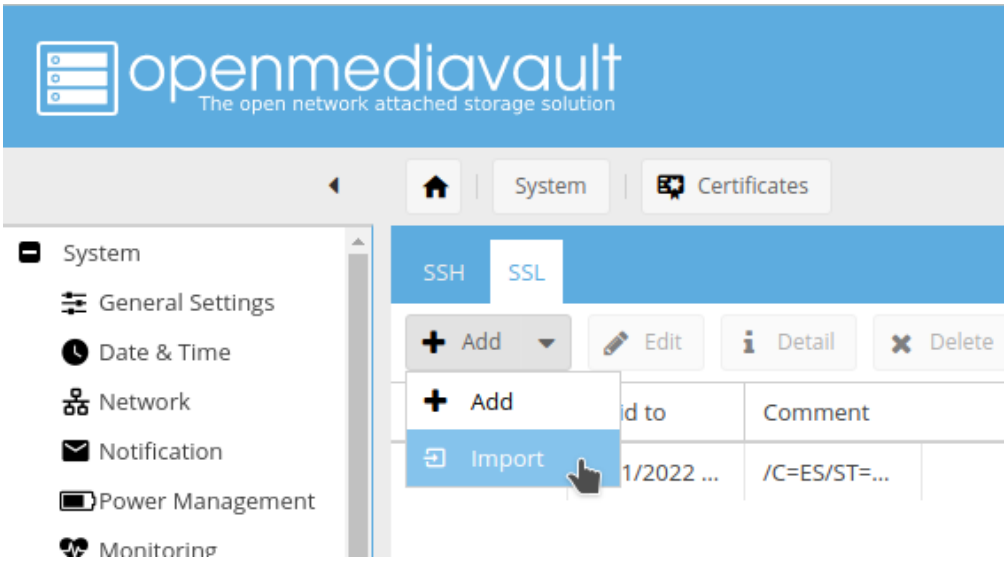
(proviene de la página anterior)

```
lrwxrwxrwx 1 root root   46 Oct 27 07:14 privkey.pem -> ../../archive/www.carpet4you.
↪site/privkey1.pem
```

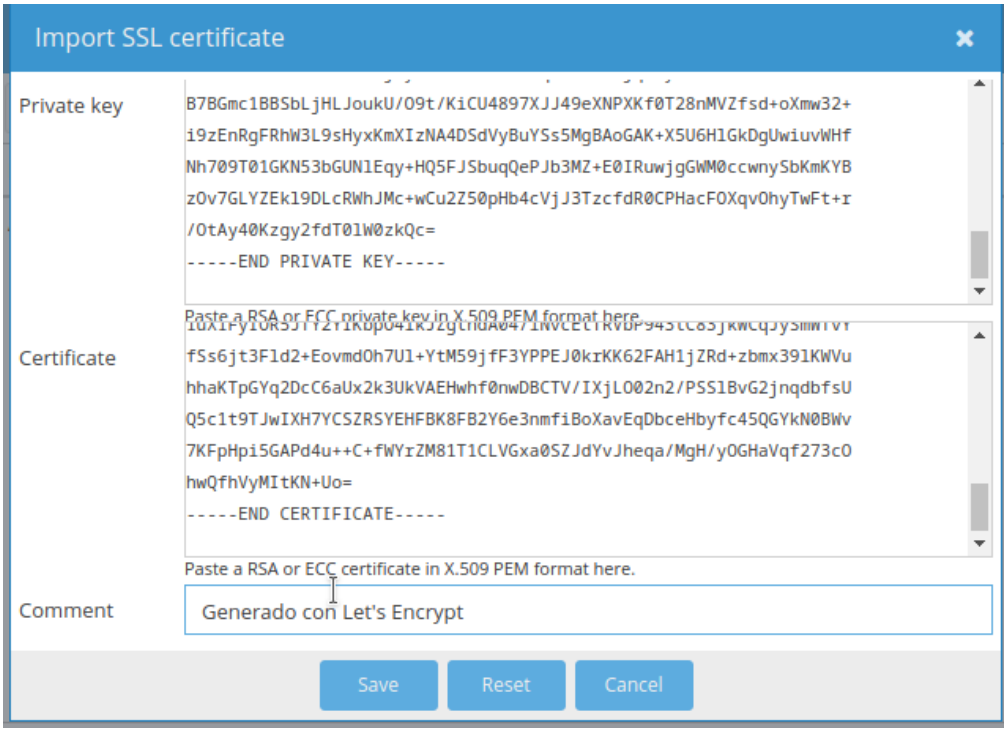
¡Estos son los certificados!

8.9 Importar certificado Let's Encrypt en OMV

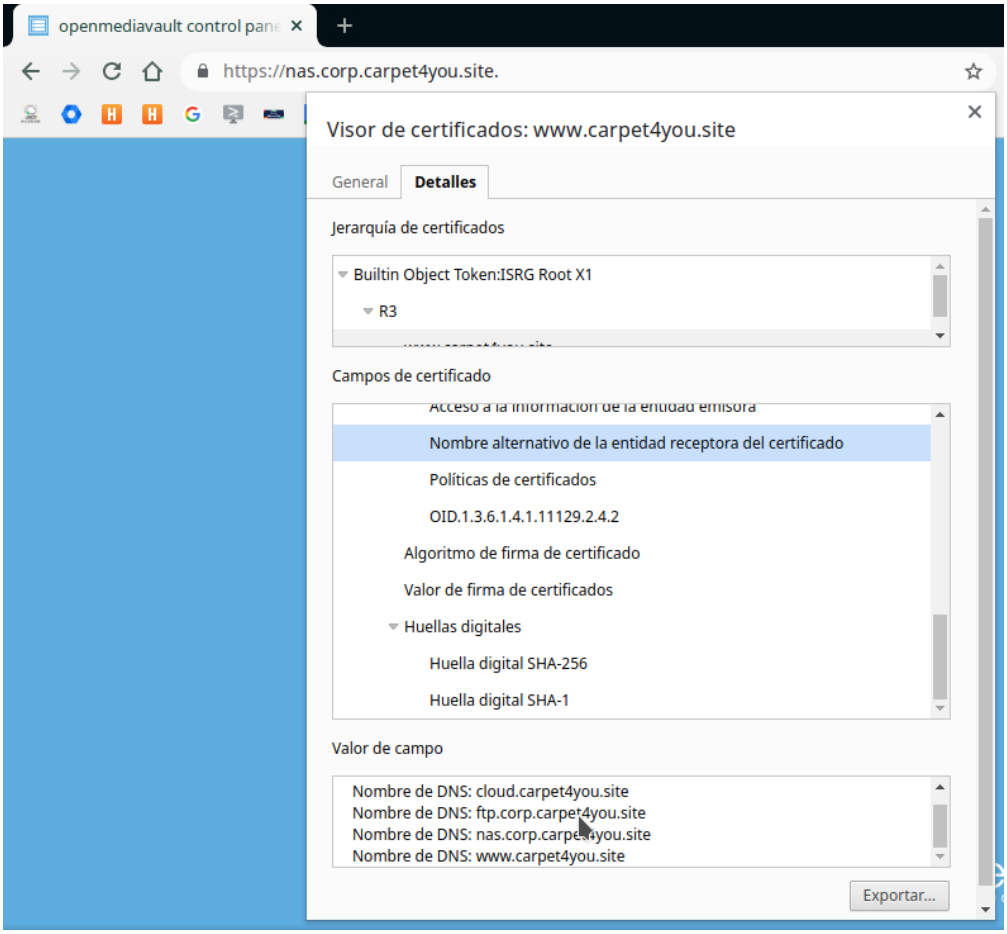
Para importar un certificado en OpenMediaVault debemos navegar hasta Certificados > SSL. Aquí, en el botón de Añadir, seleccionamos la opción de *Importar*



Copiamos y pegamos el contenido de la clave privada y el certificado en la interfaz web y guardamos los cambios. Desde el apartado *General Settings* seleccionamos el nuevo certificado importado:



Si ahora navegamos a la web, veremos el certificado correcto:



8.1. *Servidor SSH*
8.2. *Servidor web*
8.3. *Servidor FTP*
8.4. *Servidor NFS*
8.5. *Servidor SAMBA*
8.6. *Servidor SAMBA*
8.7. *Convertirnos en Autoridad de Certificación*
8.8. *Conseguir certificado Let's Encrypt*
8.9. *Importar certificado Let's Encrypt en OMV*

CAPÍTULO 9

Seguridad de la información

9.1 RAID en Windows Server 2019

9.1.1 Configuración de la MV

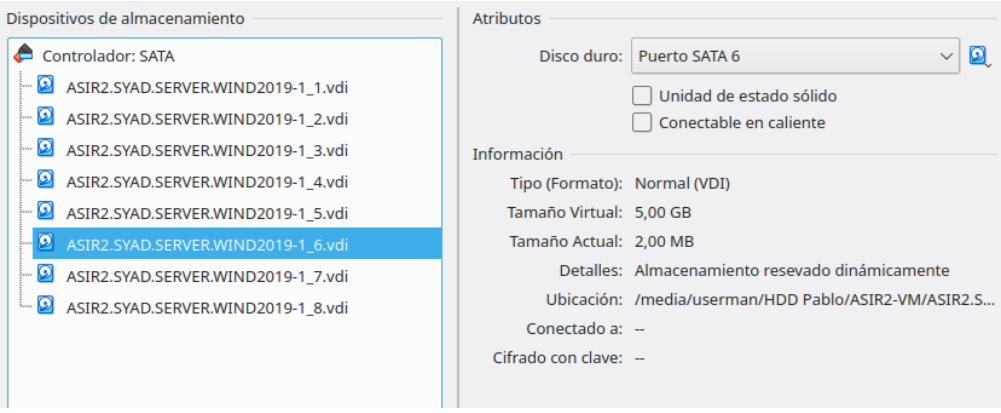
Se utilizará una máquina virtual con Windows Server 2019 como sistema operativo. Se le asignan 4 GB de RAM y 4 vCPUs. En tanto a la red, se configuran 1 adaptador virtual:

- Adaptador 1, configurado en modo NAT para la conexión a internet.

En tanto al usuario administrador utiliza la (poco segura) combinación administrador:Clave_00.

Se añaden 8 discos virtuales a la máquina:

- El disco principal de 50GB, donde almacenaremos el sistema operativo.
- 7 discos de 5GB que utilizaremos para configurar los sistemas RAID.

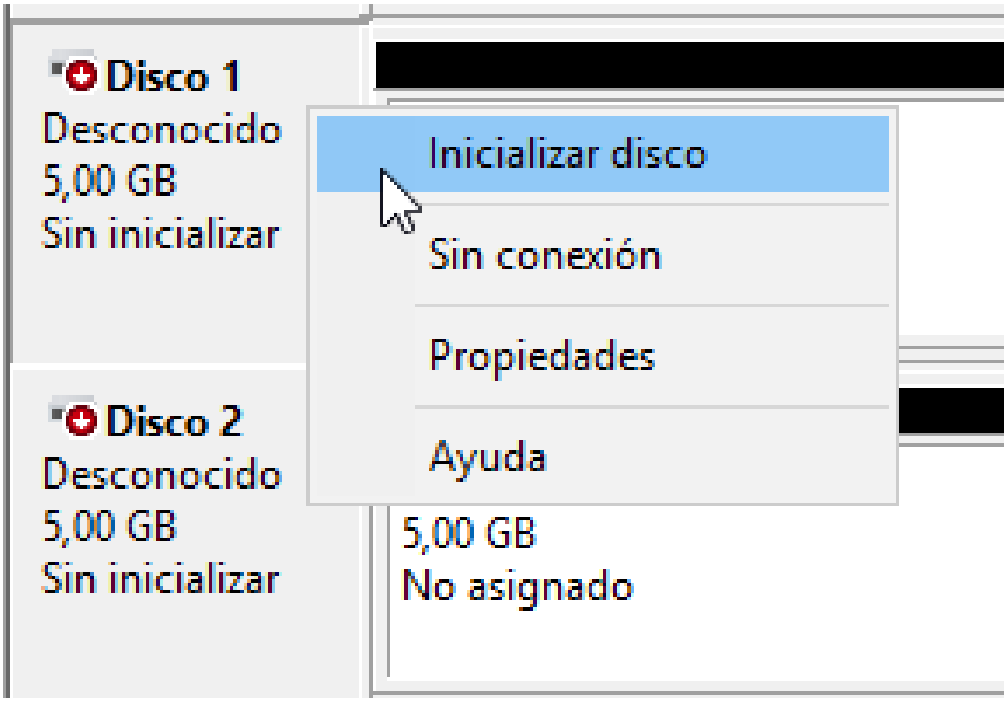


9.1.2 Sistema RAID0 - Stripped

Si estuviéramos reutilizando discos debiéramos utilizar diskpart para limpiar todas las particiones. O utilizar el Administrador de Discos (que puede ser bastante más lento si tenemos varias particiones).

Para configurar el sistema RAID 0 lo primero que debemos hacer es inicializar los discos. Para ello, hacemos clic sobre uno de ellos y seleccionamo *Inicializar disco*. Al hacerlo debemos seleccionar los discos que queremos que formen parte del RAID.

En nuestro caso seleccionamo *Disco 1* y *Disco 2*, utilizamos GPT como formato de partición para no tener limitaciones en tanto a particiones que sí podríamos llegar a tener con MBR.



Después debemos convertir los discos a discos dinámicos. Para hacerlo, basta con seleccionar el disco correspondiente, hacer clic derecho sobre el nombre y marcar la opción *Convertir en disco dinámico*. Al igual que cuando hemos incializado los discos, el asistente nos permite convertir varios en un mismo paso. Seleccionamos ambos discos con los que estamos trabajando.

Para crear y formatear el RAID0 podemos segur los pasos descritos en este vídeo:

9.1.3 Sistema RAID1 - Espejo

Para configurar el sistema RAID 1 lo primero que debemos hacer es inicializar los discos. Para ello, hacemos clic sobre uno de ellos y seleccionamo *Inicializar disco*. Al hacerlo debemos seleccionar los discos que queremos que formen parte del RAID.

En nuestro caso seleccionamo *Disco 3* y *Disco 5* (debido a un error en la creación el disco 4 tiene solo 500MB en lugar ed 5GB), utilizamos GPT como formato de partición para no tener limitaciones en tanto a particiones que sí podríamos llegar a tener con MBR.

En el siguiente vídeo podemos ver el proceso completo de inicialización de los discos y configuración del RAID1 en espejo.

9.1.4 Sistema RAID5 - Distribuido

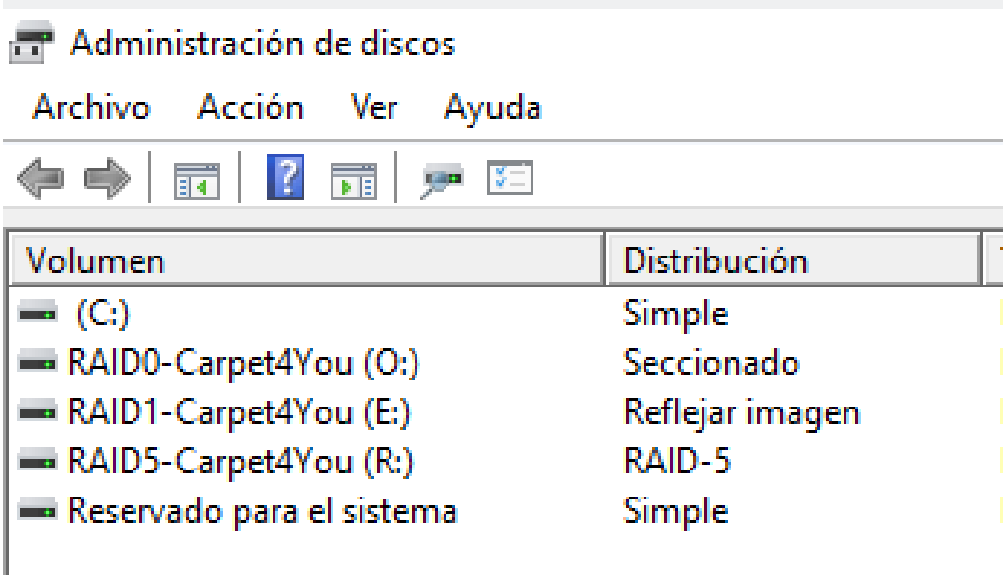
Para configurar el sistema RAID 5 lo primero que debemos hacer es inicializar los discos. Para ello, hacemos clic sobre uno de ellos y seleccionamo *Inicializar disco*. Al hacerlo debemos seleccionar los discos que queremos que formen parte del RAID.

En nuestro caso seleccionamo *Disco 6*, *Disco 7* y *Disco 8* (debido a un error en la creación el disco 4 tiene solo 500MB en lugar ed 5GB), utilizamos GPT como formato de partición para no tener limitaciones en tanto a particiones que sí podríamos llegar a tener con MBR.

En el siguiente vídeo podemos ver cómo crear un volumen RAID5:

9.1.5 Resultado

En la siguiente imagen podemos ver el resultado de los pasos mostrados en esta página:



9.2 RAID en Linux Ubuntu Server 18.04

9.2.1 Configuración de la MV

Se utilizará una máquina virtual con Windows Server 2019 como sistema operativo. Se le asignan 4 GB de RAM y 4 vCPUs. En tanto a la red, se configuran 1 adaptadores virtual:

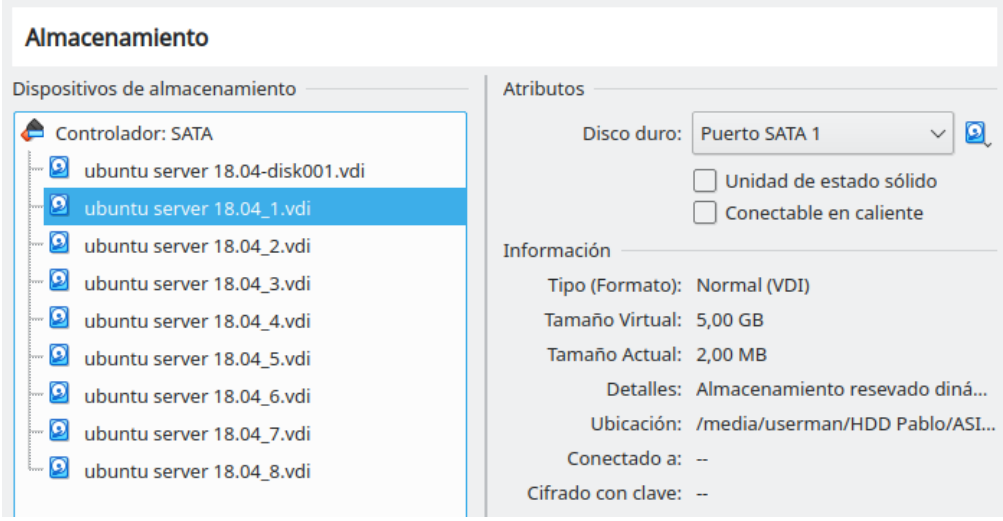
- Adaptador 1, configurado en modo NAT para la conexión a internet.

En tanto al usuario administrador utiliza la (poco segura) combinación *user:user*.

Se añaden 9 discos virtuales a la máquina:

- El disco principal de 50GB, donde almacenaremos el sistema operativo.
- 8 discos de 5GB que utilizaremos para configurar los sistemas RAID.

La configuración por tanto es la siguiente:



Una vez hemos arrancado la máquina podemos utilizar el comando *lsblk* para ver la lista de dispositivos conectados al equipo.

```
user@server-carpet:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0 88,5M  1 loop /snap/core/7270
sda      8:0    0  160G  0 disk
├─sda1   8:1    0    1M  0 part
├─sda2   8:2    0    4G  0 part [SWAP]
└─sda3   8:3    0  156G  0 part /
sdb      8:16   0    5G  0 disk
sdc      8:32   0    5G  0 disk
sdd      8:48   0    5G  0 disk
sde      8:64   0    5G  0 disk
sdf      8:80   0    5G  0 disk
sdg      8:96   0    5G  0 disk
sdh      8:112  0    5G  0 disk
sdi      8:128  0    5G  0 disk
```

Para ver el estado de los RAID (gestionado por *mdadm*) utilizamos el siguiente comando:

```
user@server-carpet:~$ cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
unused devices: <none>
```

Como podemos ver, no tenemos (de momento) ninguno configurado.

9.2.2 RAID0 - Stripped

Creación del array

```
user@server-carpet:~$ sudo mdadm --create --verbose \
/dev/raid0-carpet4you --level=0 --raid-devices=2 /dev/sdb /dev/sdc

mdadm: chunk size defaults to 512K
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/raid0-carpet4you started.
```

Las opciones de este comando son:

- **mdadm**, es el comando en sí, nos sirve para gestionar toda la configuración relativa a RAIDs.
- **–create**, indicamos a *mdadm* que queremos crear uno nuevo, puesto que también podríamos borrarlos o modificarlos.
- **–verbose**, para que nos muestre detalles sobre las acciones que está realizando.
- **/dev/raid0-carpet4you**, este es el dispositivo de bloque que vamos a crear.
- **/–level=0**, nivel de RAID con el que vamos a configurar el nuevo dispositivo lógico.
- **–raid-devices=2**, número de dispositivos que vamos a agregar al RAID.
- **/dev/sdb /dev/sdc**, los dispositivos que vamos a utilizar.

Si ahora vemos la información de *mdstat* veremos el nuevo dispositivo creado.

```
user@server-carpet:~$ cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
raid0-carpet4you : active raid0 sdc[1] sdb[0]
    10475520 blocks super 1.2 512k chunks
unused devices: <none>
```

Crear sistema de archivos y montar

Creamos el sistema de archivos en el nodo RAID;

```
user@server-carpet:~$ sudo mkfs.ext4 -F /dev/raid0-carpet4you
    mke2fs 1.44.1 (24-Mar-2018)
    Creating filesystem with 2618880 4k blocks and 655360 inodes
    Filesystem UUID: 0d3d57e0-8bf2-4d1e-8289-c3996ecdf606
    Superblock backups stored on blocks:
            32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

    Allocating group tables: done
    Writing inode tables: done
    Creating journal (16384 blocks): done
    Writing superblocks and filesystem accounting information: done
```

Creamos la carpeta donde montaremos el sistema de archivos:

```
user@server-carpet:~$ sudo mkdir -p /mnt/raid0-carpet4you
```

Montamos el dispositivo RAID en nuestro sistema de archivos:

```
user@server-carpet:~$ sudo mount /dev/raid0-carpet4you /mnt/raid0-carpet4you
```

Comprobaciones

Para ver el sistema de archivos resultante podemos ejecutar el siguiente comando:

```
user@server-carpet:~$ df -h /dev/raid0-carpet4you
Filesystem      Size  Used Avail Use% Mounted on
/dev/raid0-carpet4you        9,8G   37M  9,3G   1% /mnt/raid0-carpet4you
```

Automontaje en inicio

Para estar seguros de que al reiniciar el equipo el sistema reconoce el RAID con las mismas características debemos actualizar el archivo `/etc/mdadm/mdadm.conf`

```
user@server-carpet:~$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm/mdadm.conf
ARRAY /dev/raid0-carpet4you metadata=1.2 name=server-carpet:0␣
↪UUID=5f784e4c:b5877144:918ac136:c341cb10
```

También debemos actualizar `initframs`, que es el archivo de RAM que se carga durante el arranque del sistema:

```
user@server-carpet:~$ sudo update-initramfs -u
```

Por último, debemos actualizar el archivo `/etc/fstab`:

```
user@server-carpet:~$ echo '/dev/raid0-carpet4you /mnt/raid0-carpet4you ext4 defaults,
↪nofail,discard 0 0' | sudo tee -a /etc/fstab
```

9.2.3 RAID1 - Espejo

Creación del array

```
user@server-carpet:~$ sudo mdadm --create --verbose \
/dev/raid0-carpet4you --level=1 --raid-devices=2 /dev/sdd /dev/sde


mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/raid1-carpet4you started.
```

Las opciones de este comando son:

- **mdadm**, es el comando en sí, nos sirve para gestionar toda la configuración relativa a RAIDs.
- **–create**, indicamos a *mdadm* que queremos crear uno nuevo, puesto que también podríamos borrarlos o modificarlos.
- **–verbose**, para que nos muestre detalles sobre las acciones que está realizando.
- **/dev/raid1-carpet4you**, este es el dispositivo de bloque que vamos a crear.
- **/–level=1**, nivel de RAID con el que vamos a configurar el nuevo dispositivo lógico.
- **–raid-devices=2**, número de dispositivos que vamos a agregar al RAID.

- **/dev/sdd /dev/sde**, los dispositivos que vamos a utilizar.

Si ahora vemos la información de *mdstat* veremos el nuevo dispositivo creado.

```
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
raid1-carpet4you : active raid1 sde[1] sdd[0]
  5237760 blocks super 1.2 [2/2] [UU]

raid0-carpet4you : active raid0 sdc[1] sdb[0]
  10475520 blocks super 1.2 512k chunks

unused devices: <none>
```

Crear sistema de archivos y montar

Creamos el sistema de archivos en el nodo RAID;

```
user@server-carpet:~$ sudo mkfs.ext4 -F /dev/raid1-carpet4you
    mke2fs 1.44.1 (24-Mar-2018)
    Creating filesystem with 1309440 4k blocks and 327680 inodes
    Filesystem UUID: 5f929cc1-7c5e-4107-a71a-e9cbb296c5f3
    Superblock backups stored on blocks:
            32768, 98304, 163840, 229376, 294912, 819200, 884736

    Allocating group tables: done
    Writing inode tables: done
    Creating journal (16384 blocks): done
    Writing superblocks and filesystem accounting information: done
```

Creamos la carpeta donde montaremos el sistema de archivos:

```
user@server-carpet:~$ sudo mkdir -p /mnt/raid1-carpet4you
```

Montamos el dispositivo RAID en nuestro sistema de archivos:

```
user@server-carpet:~$ sudo mount /dev/raid1-carpet4you /mnt/raid1-carpet4you
```

Comprobaciones

Para ver el sistema de archivos resultante podemos ejecutar el siguiente comando:

```
user@server-carpet:~$ df -h /dev/raid1-carpet4you
Filesystem      Size  Used Avail Use% Mounted on
/dev/raid1-carpet4you        4,9G   20M  4,6G   1% /mnt/raid1-carpet4you
```

Automontaje en inicio

Para estar seguros de que al reiniciar el equipo el sistema reconoce el RAID con las mismas características debemos actualizar el archivo `/etc/mdadm/mdadm.conf`

```
user@server-carpet:~$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm/mdadm.conf
ARRAY /dev/raid0-carpet4you metadata=1.2 name=server-carpet:0␣
↪UUID=5f784e4c:b5877144:918ac136:c341cb10

ARRAY /dev/raid1-carpet4you metadata=1.2 name=server-carpet:1␣
↪UUID=089e4962:1c5da6a4:6fd12683:de775a6c
```

También debemos actualizar `initframs`, que es el archivo de RAM que se carga durante el arranque del sistema:

```
user@server-carpet:~$ sudo update-initramfs -u
```

Por último, debemos actualizar el archivo `/etc/fstab`:

```
user@server-carpet:~$ echo '/dev/raid1-carpet4you /mnt/raid1-carpet4you ext4 defaults,
↪nofail,discard 0 0' | sudo tee -a /etc/fstab
```

9.2.4 RAID5 - Espejo

Creación del array

```
user@server-carpet:~$ sudo mdadm --create --verbose \
/dev/raid5-carpet4you --level=5 --raid-devices=4 /dev/sdf /dev/sdg /dev/sdh /dev/sdi

mdadm: layout defaults to left-symmetric
mdadm: layout defaults to left-symmetric
mdadm: chunk size defaults to 512K
mdadm: size set to 5237760K
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/raid5-carpet4you started.
```

Las opciones de este comando son:

- **mdadm**, es el comando en sí, nos sirve para gestionar toda la configuración relativa a RAIDs.
- **–create**, indicamos a *mdadm* que queremos crear uno nuevo, puesto que también podríamos borrarlos o modificarlos.
- **–verbose**, para que nos muestre detalles sobre las acciones que está realizando.
- **/dev/raid5-carpet4you**, este es el dispositivo de bloque que vamos a crear.
- **/–level=5**, nivel de RAID con el que vamos a configurar el nuevo dispositivo lógico.
- **–raid-devices=4**, número de dispositivos que vamos a agregar al RAID.
- **/dev/sdf /dev/sdg /dev/sdh /dev/sdi**, los dispositivos que vamos a utilizar.

Si ahora vemos la información de *mdstat* veremos el nuevo dispositivo creado.

```
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
raid5-carpet4you : active raid5 sdi[4] sdh[2] sdg[1] sdf[0]
    15713280 blocks super 1.2 level 5, 512k chunk, algorithm 2 [4/3] [UUU_]
    [=>...................]  recovery =  6.6% (350524/5237760) finish=4.8min␣
↪speed=16691K/sec

raid1-carpet4you : active raid1 sde[1] sdd[0]
    5237760 blocks super 1.2 [2/2] [UU]

raid0-carpet4you : active raid0 sdc[1] sdb[0]
    10475520 blocks super 1.2 512k chunks

unused devices: <none>
```

Crear sistema de archivos y montar

Creamos el sistema de archivos en el nodo RAID;

```
user@server-carpet:~$ user@server-carpet:~$ sudo mkfs.ext4 -F /dev/raid5-carpet4you
    mke2fs 1.44.1 (24-Mar-2018)
    Creating filesystem with 3928320 4k blocks and 983040 inodes
    Filesystem UUID: fb134669-8c3e-42a6-b406-53f1a32c91cb
    Superblock backups stored on blocks:
            32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208

    Allocating group tables: done
    Writing inode tables: done
    Creating journal (16384 blocks): done
    Writing superblocks and filesystem accounting information: done
```

Creamos la carpeta donde montaremos el sistema de archivos:

```
user@server-carpet:~$ sudo mkdir -p /mnt/raid5-carpet4you
```

Montamos el dispositivo RAID en nuestro sistema de archivos:

```
user@server-carpet:~$ sudo mount /dev/raid5-carpet4you /mnt/raid5-carpet4you
```

Comprobaciones

Para ver el sistema de archivos resultante podemos ejecutar el siguiente comando:

```
user@server-carpet:~$ df -h /dev/raid5-carpet4you
Filesystem      Size  Used Avail Use% Mounted on
/dev/raid5-carpet4you         15G   41M   14G   1% /mnt/raid5-carpet4you
```

Automontaje en inicio

Para estar seguros de que al reiniciar el equipo el sistema reconoce el RAID con las mismas características debemos actualizar el archivo `/etc/mdadm/mdadm.conf`

```
user@server-carpet:~$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm/mdadm.conf
ARRAY /dev/raid0-carpet4you metadata=1.2 name=server-carpet:0
    UUID=5f784e4c:b5877144:918ac136:c341cb10
ARRAY /dev/raid1-carpet4you metadata=1.2 name=server-carpet:1
    UUID=089e4962:1c5da6a4:6fd12683:de775a6c
ARRAY /dev/raid5-carpet4you metadata=1.2 name=server-carpet:2
    UUID=dc70161b:a4c632d6:fee7cbaa:33c7f703
```

También debemos actualizar `initframs`, que es el archivo de RAM que se carga durante el arranque del sistema:

```
user@server-carpet:~$ sudo update-initramfs -u
```

Por último, debemos actualizar el archivo `/etc/fstab`:

```
user@server-carpet:~$ echo '/dev/raid5-carpet4you /mnt/raid5-carpet4you ext4 defaults,
↪nofail,discard 0 0' | sudo tee -a /etc/fstab
```

9.2.5 Ver detalles de un RAID

Para ver los detalles de un RAID en Ubuntu podemos utilizar el siguiente comando, indicando el dispositivo de tipo bloque que representa al RAID.

```
user@server-carpet:~$ sudo mdadm --detail /dev/raid5-carpet4you
/dev/raid5-carpet4you:
        Version : 1.2
    Creation Time : Mon Oct 25 11:41:35 2021
        Raid Level : raid5
        Array Size : 15713280 (14.99 GiB 16.09 GB)
    Used Dev Size : 5237760 (5.00 GiB 5.36 GB)
    Raid Devices : 4
    Total Devices : 4
    Persistence : Superblock is persistent

    Update Time : Mon Oct 25 11:46:20 2021
            State : active
    Active Devices : 4
Working Devices : 4
    Failed Devices : 0
    Spare Devices : 0

            Layout : left-symmetric
        Chunk Size : 512K

Consistency Policy : resync

            Name : server-carpet:2  (local to host server-carpet)
            UUID : dc70161b:a4c632d6:fee7cbaa:33c7f703
            Events : 39
```

(continué en la próxima página)

(proviene de la página anterior)

```
    Number   Major   Minor   RaidDevice State
    0       8       80        0      active sync   /dev/sdf
    1       8       96        1      active sync   /dev/sdg
    2       8      112        2      active sync   /dev/sdh
    4       8      128        3      active sync   /dev/sdi
```

9.3 Recuperación de la información de RAID

Para este apartado vamos a crear una serie de datos en el RAID 5 configurado de forma previa.

9.3.1 Almacenar datos

Descargamos el libro completo de *El Quijote* varias veces:

```
user@server-carpet:~$ wget https://gist.githubusercontent.com/jsdario/
↪6d6c69398cb0c73111e49f1218960f79/raw/8d4fc4548d437e2a7203a5aeeace5477f598827d/el_
↪quijote.txt >> el_quijote.txt
```

9.3.2 Desconectar disco

Debemos configurar en VirtualBox que nuestros discos son desconectables en caliente.

Al desconectar desde la interfaz de VirtualBox el disco vemos lo siguiente:

```
user@server-carpet:~$ sudo mdadm --detail /dev/md2
/dev/md2:
        Version : 1.2
    Creation Time : Mon Oct 25 11:41:35 2021
        Raid Level : raid5
        Array Size : 15713280 (14.99 GiB 16.09 GB)
    Used Dev Size : 5237760 (5.00 GiB 5.36 GB)
    Raid Devices : 4
    Total Devices : 3
    Persistence : Superblock is persistent

    Update Time : Mon Oct 25 12:07:43 2021
            State : clean, degraded
    Active Devices : 3
Working Devices : 3
    Failed Devices : 0
    Spare Devices : 0

            Layout : left-symmetric
        Chunk Size : 512K

Consistency Policy : resync

```

(continué en la próxima página)

(proviene de la página anterior)

```
24              Name : server-carpet:2  (local to host server-carpet)
25              UUID : dc70161b:a4c632d6:fee7cbaa:33c7f703
26              Events : 43
27
28      Number   Major   Minor   RaidDevice State
29      0       8       80        0      active sync   /dev/sdf
30      -       0        0        1      removed
31      2       8      112        2      active sync   /dev/sdh
32      4       8      128        3      active sync   /dev/sdi
```

Como podemos ver en las líneas 12 y 25 de la salida del comando anterior, el estado del raid es *degradado* y no se encuentra el disco 1, aparece como eliminado (*removed*).

9.3.3 Recuperación de la información

Guardar la información del superbloque

Una de las acciones más útiles que podemos hacer antes de nada es guardar la información guardada en los superbloques del RAID en cada dispostivo antes de que el disco fallara.

Para hacerlo podemos ejecutar el siguiente comando:

```
user@server-carpet:~$ sudo mdadm --examine /dev/sdf >> raid.status
user@server-carpet:~$ sudo mdadm --examine /dev/sdh >> raid.status
user@server-carpet:~$ sudo mdadm --examine /dev/sdi >> raid.status
```

Esta información puede sernos útil en futuros pasos.

Comprobar que los datos siguen siendo accesibles

Para hacerlo basta con navegar al punto de montaje del dispostivo RAID y listar o navegar por los archivos. Siempre teniendo en cuenta que cuánto menos modifiquemos, mejor.

```
user@server-carpet:~$ cd /mnt/md2/
user@server-carpet:/mnt/md2$ ll
total 23852
drwxr-xr-x 3 user user    4096 oct 25 12:02 ./
drwxr-xr-x 5 root root    4096 oct 25 11:43 ../
-rw-rw-r-- 1 user user       0 oct 25 12:02 el_quijote.txt
-rw-rw-r-- 1 user user 1060259 oct 25 12:02 el_quijote.txt.1
-rw-rw-r-- 1 user user 1060259 oct 25 12:02 el_quijote.txt.10
-rw-rw-r-- 1 user user 1060259 oct 25 12:02 el_quijote.txt.11
-rw-rw-r-- 1 user user 1060259 oct 25 12:02 el_quijote.txt.12
[...]
```

Añadir nuevo disco a RAID

```
user@server-carpet:~$ sudo mdadm --manage /dev/md2 --add /dev/sdg
```

Al hacerlo veremos como se durante unos segundos el sistema se recompondrá, replicando los datos entre los discos.

```
user@server-carpet:~$ sudo mdadm --manage /dev/md2 --add /dev/sdg
mdadm: added /dev/sdg
user@server-carpet:~$ sudo mdadm -D /dev/md2
/dev/md2:
           Version : 1.2
     Creation Time : Mon Oct 25 11:41:35 2021
        Raid Level : raid5
        Array Size : 15713280 (14.99 GiB 16.09 GB)
     Used Dev Size : 5237760 (5.00 GiB 5.36 GB)
      Raid Devices : 4
     Total Devices : 4
       Persistence : Superblock is persistent

       Update Time : Mon Oct 25 20:20:55 2021
             State : clean, degraded, recovering
    Active Devices : 3
   Working Devices : 4
    Failed Devices : 0
     Spare Devices : 1

            Layout : left-symmetric
        Chunk Size : 512K

Consistency Policy : resync

    Rebuild Status : 23% complete

              Name : server-carpet:2  (local to host server-carpet)
              UUID : dc70161b:a4c632d6:fee7cbaa:33c7f703
            Events : 54

    Number   Major   Minor   RaidDevice State
       0       8       80        0      active sync   /dev/sdf
       5       8       96        1      spare rebuilding   /dev/sdg
       2       8      112        2      active sync   /dev/sdh
       4       8      128        3      active sync   /dev/sdi
user@server-carpet:~$
```

9.1. *RAID en Windows Server 2019*
9.2. *RAID en Linux Ubuntu Server 18.04*
9.3. *Recuperación de la información de RAID*

CAPÍTULO 10

Servidor NAS

10.1 Descargar y comprobar OpenMediaVault

10.1.1 Descargar OpenMediaVault

Podemos descargar dicho sistema operativo desde el siguiente enlace: https://www.openmediavault.org/download.html.

En la página anterior veremos un enlace hacia SourceForge, donde podremos descargar la ISO y los archivos para la verificación.

10.1.2 Comprobar ISO OpenMediaVault en Ubuntu

Suma de comprobación MD5

```
user@server-carpet:~$ md5sum -c openmediavault_5.6.13-amd64.iso.md5

openmediavault_5.6.13-amd64.iso: La suma coincide
```

Suma de comprobación SHA256

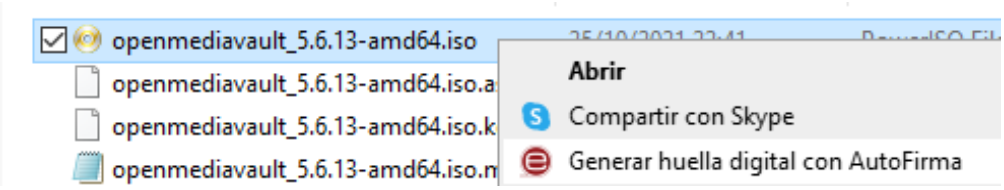
```
user@server-carpet:~$ sha256sum -c openmediavault_5.6.13-amd64.iso.sha256

openmediavault_5.6.13-amd64.sha256: La suma coincide
```

Comprobación mediante firma

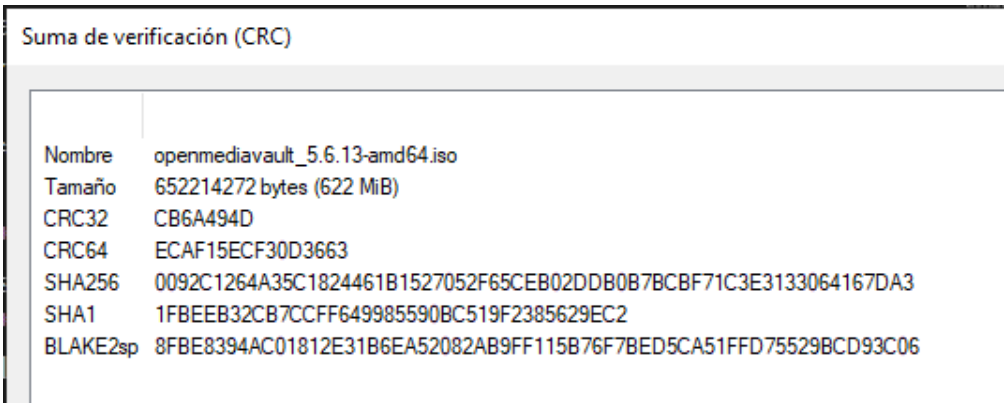
```
user@server-carpet:~$ gpg --import  openmediavault_5.6.13-amd64.iso.key

user@server-carpet:~$ gpg --verify openmediavault_5.6.13-amd64.iso.asc openmediavault_5.
↪6.13-amd64.iso

    gpg: Firmado el mié 25 ago 2021 21:56:54 CEST
    gpg:                usando RSA clave D67506C878E08A94FD7E009424863F0C716B980B
    gpg: Firma correcta de "OpenMediaVault.org (OpenMediaVault packages archive)
↪<packages@openmediavault.org>" [desconocido]
    gpg: ATENCIÓN: ¡Esta clave no está certificada por una firma de confianza!
    gpg:          No hay indicios de que la firma pertenezca al propietario.
    Huellas dactilares de la clave primaria: D675 06C8 78E0 8A94 FD7E  0094 2486 3F0C␣
↪716B 980B
```

10.1.3 Comprobar ISO OpenMediaVault en Windows

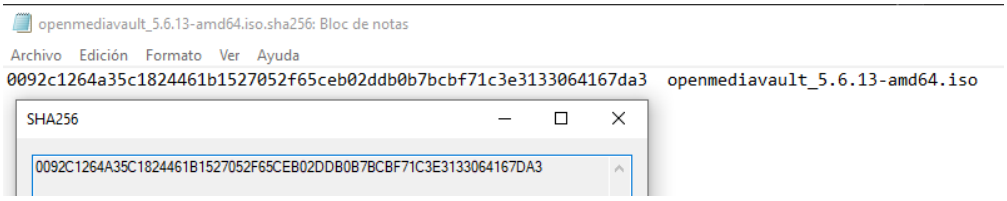
Una vez ha terminado de descargar el archivo .iso vamos a verificarlo. Para hacerlo, utilizaremos el programa autofirma que tiene capacidad de generar checksums.



Si tuviéramos la aplicación de 7z instalada también podríamos generar las huellas digitales del archivo .iso.



Si comparamos las salidas de SHA256 veremos que coinciden:



10.2 Instalar y configurar OpenMediaVault

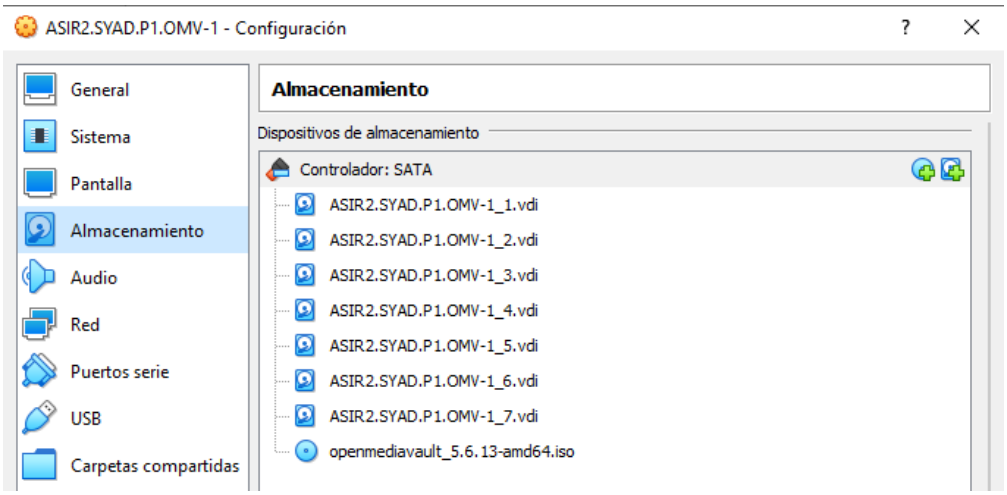
10.2.1 Configuración de la MV

Llamaremos a la máquina virtual *ASIR2.SYAD.P1.OMV-1*. Será tipo Linux, versión Debian 64bits. Asignaremos 4GB de memoria RAM y no añadiremos durante la creación ningún disco duro, pues lo haremos después.

En tanto a la red, se configuran 2 adaptadores virtuales:

- Adaptador 1, configurado en modo NAT para la conexión a internet.
- Adaptador 2, confiugrado en modo solo-anfitrión, para la conexión vía web y a los servicios.

Sobre los discos, se crean los siguientes discos virtuales:



10.2.2 Instalación del SO

La instalación del Sistema Operativo OpenMediaVault es realmente sencilla, de lo que podríamos denominar «Siguiente, Siguiente, Siguiente». Los únicos datos que nos solicita el programa son la contraseña del usuario *root*, algunos datos sobre la red (si bien intenta la autoconfiguración por DHCP) y la réplica de APT de Debian que queremos utilizar para la actualización e instalación de los paquetes necesarios.

En el siguiente GIF animado podemos ver el proceso, pantalla a pantalla.

Nota: Si accedes a esta documentación desde la versión PDF, el GIF es accesible desde este enlace

10.2.3 Dominio para el NAS

La IP asignada a la máquina virtual es la 192.168.56.111. Vamos a añadir un registro tipo A en nas.corp.carpet4you.site con la IP como contenido.

Vamos a comprobar el registro con el comando *dig*:

```
user@server-carpet:~$ dig nas.corp.carpet4you.site.
    ; <<>> DiG 9.11.5-P4-5.1+deb10u5-Debian <<>> nas.corp.carpet4you.site.
    ;; global options: +cmd
    ;; Got answer:
    ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3770
    ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

    ;; OPT PSEUDOSECTION:
    ; EDNS: version: 0, flags:; udp: 512
    ;; QUESTION SECTION:
    ;nas.corp.carpet4you.site.      IN      A

    ;; ANSWER SECTION:
    nas.corp.carpet4you.site. 3600  IN      A       192.168.56.111

    ;; Query time: 17 msec
    ;; SERVER: 169.254.169.254#53(169.254.169.254)
    ;; WHEN: Mon Oct 25 21:48:32 UTC 2021
    ;; MSG SIZE  rcvd: 69
```

10.2.4 Primer acceso al panel de gestión web

Si ahora navegamos hasta la dirección nas.corp.carpet4you.site veremos el panel de administración web de OpenMedia Vault.

El usuario por defecto es `admin` y la contraseña `openmediavault`

Cambiar contraseña de panel web

Una de las acciones que debemos realizar antes de configurar OpenMediaVault es cambiar la contraseña, que como hemos visto es muy básica.

Para cambiarlo:

Generar certificado SSL/TLS y utilizar HTTPS

Para generar el certificado SSL y utilizarlo en la web debemos seguir los pasos descritos en el siguiente vídeo:

Si ahora accedemos a la web podremos ver nuestro certificado:

10.3 Configuración de RAID inicial

Nota:

La interfaz se encuentra en inglés.
En el caso de consultar la versión PDF, puedes ver los vídeos haciendo clic en los enlaces previos a cada uno.

El proceso de creación de RAID es medianamente sencillo:

1. Inicializar los discos
2. Crear RAID
    1. Indicando nombre
    2. Seleccionar nivel de RAID
    3. Seleccionar dispositivos
3. Crear sistema de archivos en dispositivo RAID
4. Montar sistema de archivos RAID
5. (Opcional) Crear carpeta compartida en el sistema de archivos.

10.3.1 RAID 1

Crear el RAID

Se puede ver la creación del RAID 1 en el siguiente vídeo:

Crear el sistema de archivos:

Se puede ver la creación del sistema de archivos en el siguiente vídeo:

10.3.2 RAID 5

Para crear el RAID5 y el sistema de archivos seguimos los pasos descritos en el siguiente víeo. También hemos creado la carpeta compartida para el *home*:

10.3.3 Crear usuario

Para crear un usuario seguimos los siguientes pasos:

1. Navegamos desde el menú lateral hasta *Users*
2. Hacemos clic, en el menú superior, en la opción *Add*.
3. **Rellenamos los datos necesarios para la creación del usuario:**
    1. Configuramos el nombre para el usuario
    2. Escribimos un correo electrónico para el usuario
    3. Definimos una contraseña (*Clave_00* en nuestro caso) para el usuario.

4. Definimos una *shell* para nuestro usuario. Como no queremos que pueda iniciar sesión mediante SSH seleccionamos `/usr/sbin/nologin` .

4. Hacemos clic en *Save*. Aplicamos los cambios.

Configurar la carpeta *home*

Debemos indicar a OpenMediaVault dónde se van a guardar los datos del *home* de los usuarios. Para hacerlo:

1. Navegamos desde el menú lateral hasta *Users*
2. En la barra superior seleccionamos *Settings*
3. Aquí marcamos *Enable*
4. Seleccionamos la carpeta compartida *home* que hemos creado anteriormente.
5. Hacemos clic en *Save*. Aplicamos los cambios.

10.4 Servicio SMB/CIFS

Nota: La interfaz se encuentra en Inglés.

10.4.1 Crear carpeta

Crearemos la carpeta *SMB-Carpet4You* y la compartiremos con nuestro usuario. Para hacerlo, seguiremos los siguientes pasos:

1. Entramos al panel de control web de OMV.
2. En el menú de la izquierda, seleccionamos *Shared folders*. Hacemos clic en *Add* para crear una nueva carpeta compartida.
3. Escribimos los detalles de la nueva carpeta que estamos creando: nombre (*SMB-Carpet4You*). Seleccionamos el sistema de archivos deseado, *RAID5FS*. En Path, si no se autocompleta, introduciremos el valor deseado.
4. Hacemos clic en guardar. Salvamos los cambios desde el botón de la parte superior.

10.4.2 Permisos de carpeta

Ya con la carpeta creada, debemos dar permisos a los usuarios para que puedan acceder y/o editar el contenido de la misma.

Debemos tener en cuenta que tenemos dos controles de acceso: el sistema de permisos POSIX del propio Linux y el ACL de la carpeta compartida.

Para modificar los permisos de ACL, seleccionamos la carpeta compartida y después hacemos clic en *ACL*.

En el menú superior, marcamos que *usuario* tenga acceso a la carpeta. Además, le hacemos propietario de la misma. También damos permisos al grupo.

Seleccionamos que los permisos sean recursivos.

10.4.3 Configurar servicio SMB

En el menú de la izquierda, seleccionamos el servicio SMB/CIFS.

Por defecto está apagado, *encendemos* el interruptor. Activamos los directorios *home* de los usuarios.

Por seguridad, marcamos la opción de registrar la actividad de los usuarios.

Compartir una carpeta por SMB

En la misma pantalla en la que nos encontrábamos, seleccionamos *Shares* en la parte superior de la pantalla. Hacemos clic en *Add*.

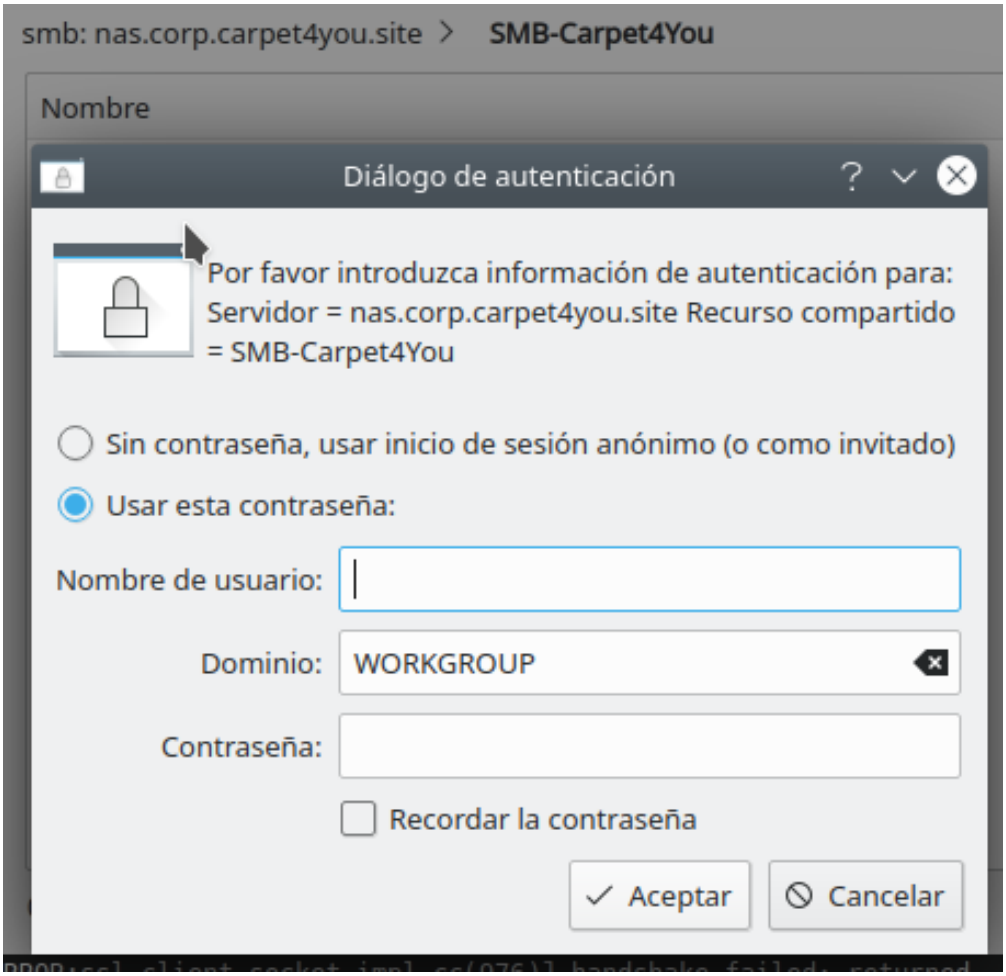
Marcamos la compartición como activada, en *Shared folder* marcamos la carpeta que hemos creado previamente, *SMB-Carpet4You*.

No cambiamos ningún parámetro más. Hacemos clic en Save y aplicamos los cambios.

10.4.4 Acceder a la carpeta compartida

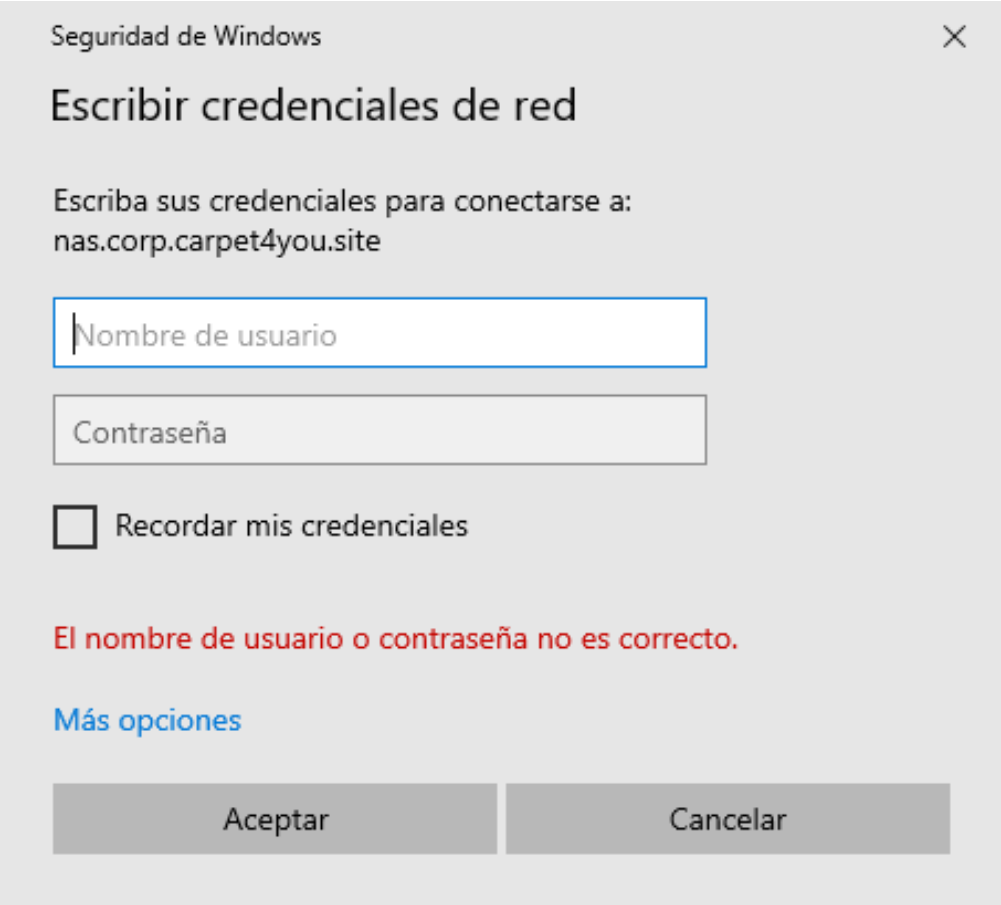
Desde nuestra máquina escribimos `smb://nas.corp.carpet4you.site`.

Nos pedirá el usuario y contraseña.

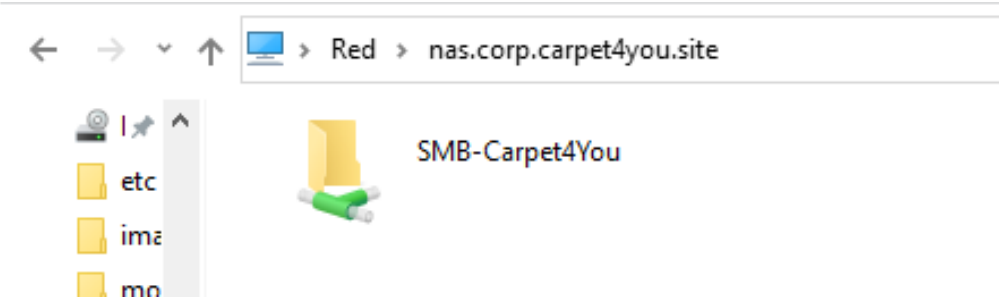


En Windows, podemos introducir `\\nas.corp.carpet4you.site` en la barra del explorador de archivos para acceder a la carpeta.

Nos pedirá las credenciales:



Cuando introduzcamos las credenciales correctas, accederemos al recurso compartido:



10.5 Servicio NFS

Nota: La interfaz se encuentra en Inglés.

10.5.1 Crear carpeta

Crearemos la carpeta *NFS-Carpet4You* y la compartiremos con nuestro usuario.

Para hacerlo, seguiremos los siguientes pasos:

1. Entramos al panel de control web de OMV.
2. En el menú de la izquierda, seleccionamos *Shared folders*. Hacemos clic en *Add* para crear una nueva carpeta compartida.
3. Escribimos los detalles de la nueva carpeta que estamos creando: nombre (*NFS-Carpet4You*). Seleccionamos el sistema de archivos deseado, *RAID5FS*. En Path, si no se autocompleta, introduciremos el valor deseado.
4. Hacemos clic en guardar. Salvamos los cambios desde el botón de la parte superior.

10.5.2 Permisos de carpeta

Ya con la carpeta creada, debemos dar permisos a los usuarios para que puedan acceder y/o editar el contenido de la misma.

Debemos tener en cuenta que tenemos dos controles de acceso: el sistema de permisos POSIX del propio Linux y el ACL de la carpeta compartida.

Para modificar los permisos de ACL, seleccionamos la carpeta compartida y después hacemos clic en *ACL*.

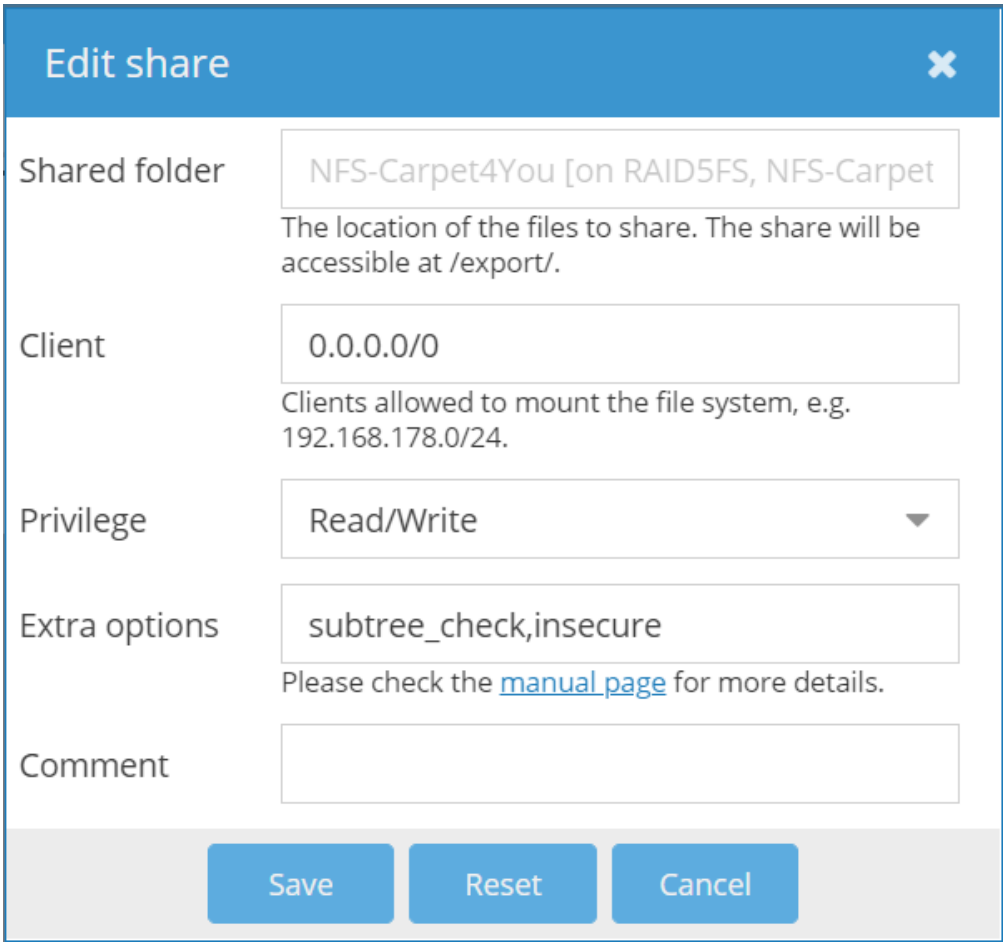
En el menú superior, marcamos que *usuario* tenga acceso a la carpeta. Además, le hacemos propietario de la misma. También damos permisos al grupo.

Seleccionamos que los permisos sean recursivos.

10.5.3 Configurar servicio NFS

En el menú de la izquierda, seleccionamos el servicio NFS. Por defecto está apagado, *encendemos* el interruptor y hacemos clic en *Save*.

En la misma pantalla en la que nos encontrábamos, seleccionamos *Shares* en la parte superior de la pantalla. Hacemos clic en *Add*.



10.5.4 Montar carpeta NFS

Para montar la carpeta debemos ejecutar el siguiente comando:

```
user@server-carpet:~$ mkdir /mnt/carpet
user@server-carpet:~$ mount -t nfs4 nas.corp.carpet4you.site:NFS-Carpet4You /mnt/carpet
```

10.6 Servicio FTP

Nota: La interfaz se encuentra en Inglés.

10.6.1 Crear carpeta

Crearemos la carpeta *FTP-Carpet4You* y la compartiremos con nuestro usuario.

Para hacerlo, seguiremos los siguientes pasos:

1. Entramos al panel de control web de OMV.
2. En el menú de la izquierda, seleccionamos *Shared folders*. Hacemos clic en *Add* para crear una nueva carpeta compartida.
3. Escribimos los detalles de la nueva carpeta que estamos creando: nombre (*FTP-Carpet4You*). Seleccionamos el sistema de archivos deseado, *RAID5FS*. En Path, si no se autocompleta, introduciremos el valor deseado.
4. Hacemos clic en guardar. Salvamos los cambios desde el botón de la parte superior.

10.6.2 Permisos de carpeta

Ya con la carpeta creada, debemos dar permisos a los usuarios para que puedan acceder y/o editar el contenido de la misma.

Debemos tener en cuenta que tenemos dos controles de acceso: el sistema de permisos POSIX del propio Linux y el ACL de la carpeta compartida.

Para modificar los permisos de ACL, seleccionamos la carpeta compartida y después hacemos clic en *ACL*.

En el menú superior, marcamos que *usuario* tenga acceso a la carpeta. Además, le hacemos propietario de la misma. También damos permisos al grupo.

Seleccionamos que los permisos sean recursivos.

10.6.3 Configurar servicio FTP

En el menú de la izquierda, seleccionamos el servicio FTP. Por defecto está apagado, *encendemos* el interruptor y hacemos clic en *Save*.

En tanto a las modificaciones de configuración debemos:

- Modificar el puerto para usar el 990 (es el que utiliza FTP seguro)
- Activamos SPF pasivo, manteniendo los puertos por defecto.
- Activamos el log de transferencias, para tener un registro en caso de auditoría.

Advertencia: Debemos tener en cuenta que los puertos deben estar abiertos. OpenMediaVault lo hace de forma automática.

En la pestaña *SSL/TLS* modificamos/activamos las siguientes configuraciones:

- Activamos las conexiones SSL/TLS con el interruptor.
- Selecciomos el certificado que queremos utilizar para encriptar las comunicaciones. En nuestro caso, hemos seleccionado el expedido por Let's Encrypt.
- Marcamos como requerida la conexión segura.
- Activamos la opción *No session reuse required*.

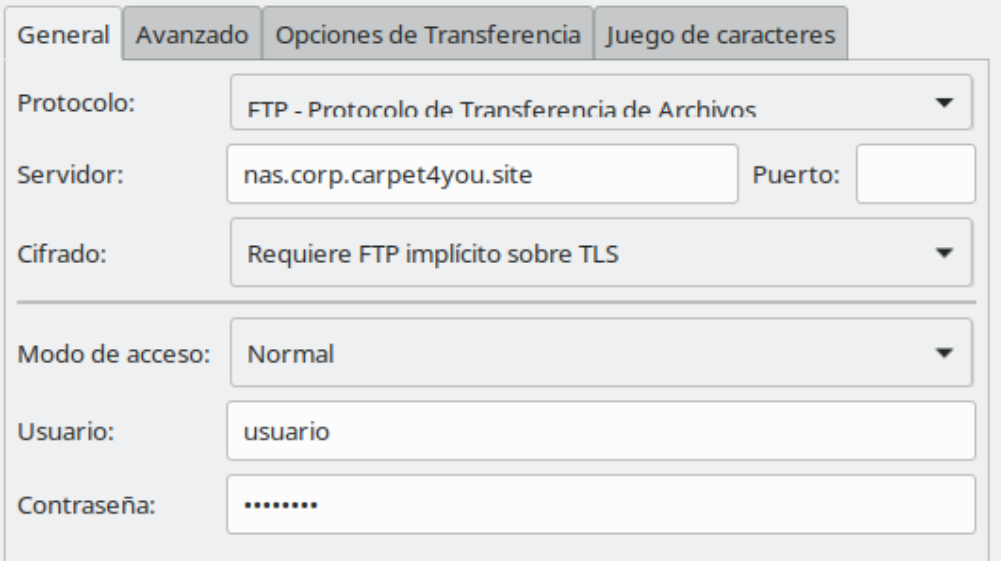
Guardamos los cambios haciendo clic en el botón *Save*-

En la misma pantalla en la que nos encontrábamos, seleccionamos *Shares* en la parte superior de la pantalla. Hacemos clic en *Add*.

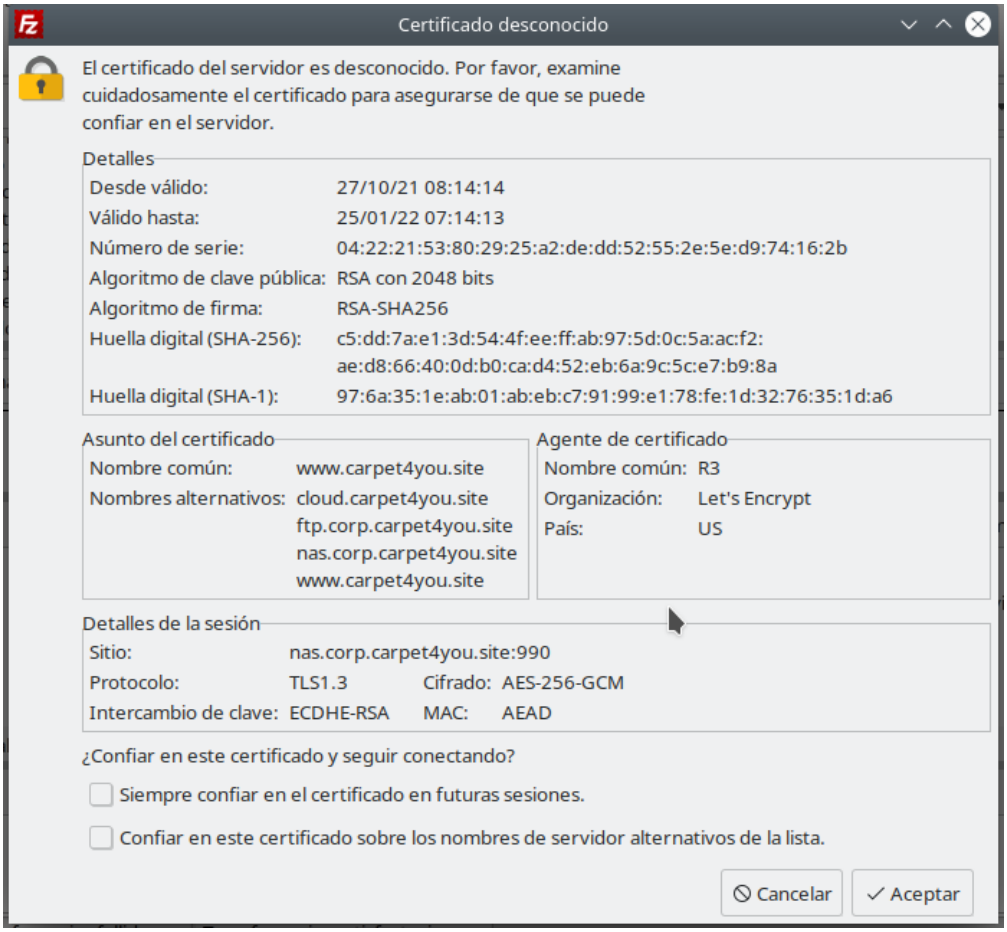
Seleccionamos la carpeta *FTP-Carpet4You* que hemos creado anteriormente.

10.6.4 Acceder a la carpeta

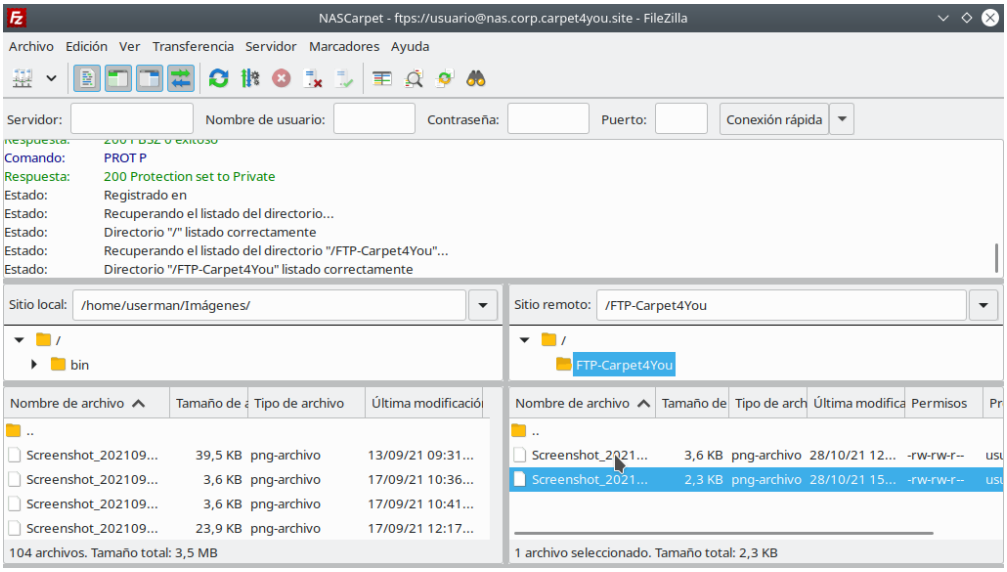
Utilizaremos la aplicación *FileZilla* para acceder a la carpeta compartida.



Cuando nos conectamos vemos el certificado:



Podemos listar y añadir archivos sin problemas:



10.7 Servicio SSH

10.7.1 Configuración del servicio

Nota: La interfaz se encuentra en Inglés.

Para acceder a la configuración del servicio SSH debemos navegar desde el menú izquierdo a Services > SSH.

Desde aquí podemos cambiar las siguientes opciones: * Activar o desactivar el servicio utilizando el interruptor. * Permitir, o no, el inicio de sesión como root. Lo más recomendable sería deshabilitarlo. * Permitir, o no, el inicio la contraseña como método de inicio de sesión; así como el método de clave pública. * (Entre otras que no comentaremos, como *tunneling* y compresión).

Importante:

Como sabemos, las posibles configuraciones SSH son mucho más amplias. Para añadir otras opciones no recogidas en la interfaz directamente podemos utilizar el cuadro de texto *Extra options*.

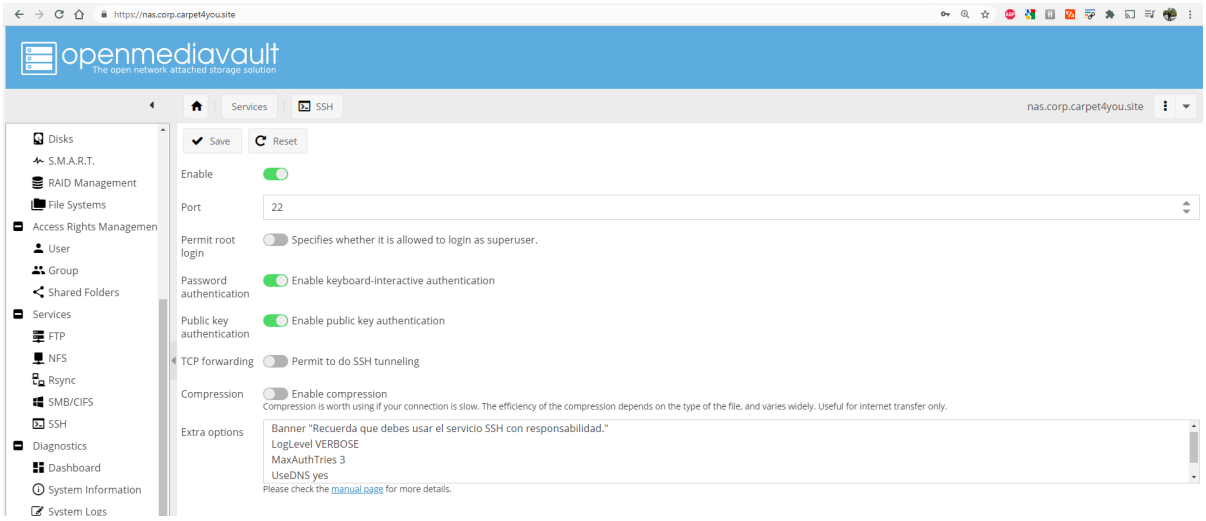
En este cuadro podemos añadir cualquier de las directivas que acepta el archivo `/etc/ssh/sshd_config`. Podemos ver una lista completa de dichas directivas en este enlace.

Durante esta práctica se han configurado las siguientes opciones extra:

```
Banner "Recuerda que debes usar el servicio SSH con responsabilidad."
LogLevel VERBOSE
MaxAuthTries 3
UseDNS yes
```

Una vez realizadas las configuraciones, debemos guardarlas y aplicarlas.

En la siguiente imagen tenemos un ejemplo de configuración:



10.7.2 Configuración de usuarios

Podemos gestionar los usuarios del sistema desde *Home* > *Acces Rights management* > *Users*. Aquí veremos una lista de usuarios. Haciendo doble clic sobre su nombre podremos editarlo.

Para usuario `usuario` de forma previa habíamo deshabilitado el acceso ssh y el intérprete de comando lo habíamos fijado como `/usr/sbin/nologin`. Por tanto, este no podría iniciar sesión.

Además de revertir estos cambios, es necesario añadir el usuario al grupo *ssh*. Para modificar la pertenencia a grupos del usuario debemos utilizar las segunda pestaña superior en la ficha del usuario. Basta marcar/desmarcar las casillas para modificar este ajuste.

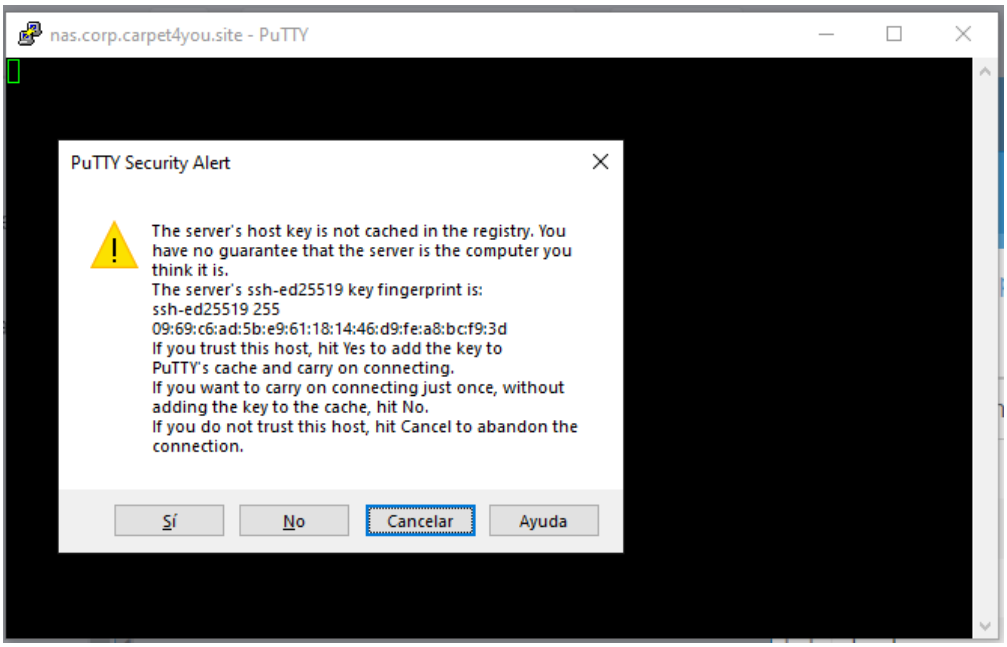
Utilizando la tercera pestaña superior en la ficha del usuario podemos ver y gestionar las claves públicas de este.

10.7.3 Conexión al servidor SSH

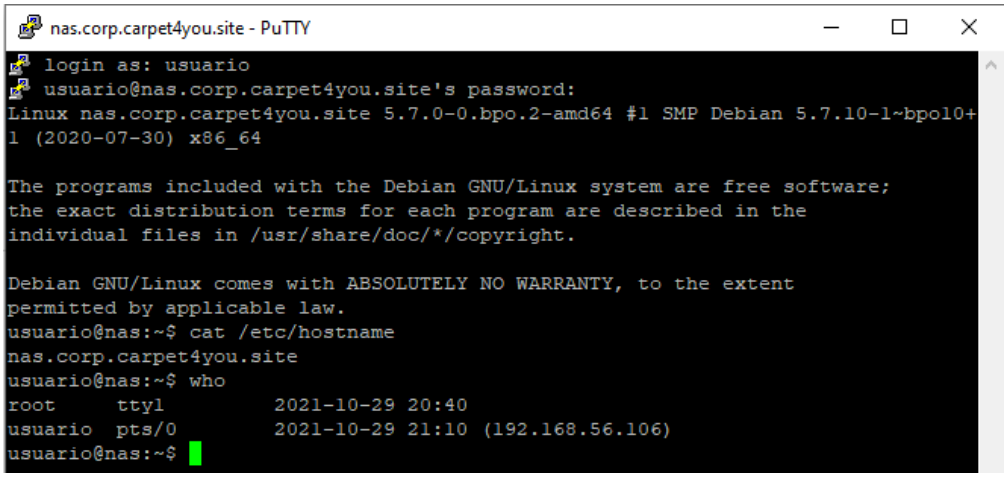
Windows

Para la conexión desde Windows utilizaremos el programa *Putty*. Basta con definir el host de conexión (IP o nombre de dominio) y el puerto.

Si es la primera vez que nos conectamos veremos el siguiente aviso:



Nos solicitará usuario y contraseña e iniciaremos sesión:



Linux

En linux utilizaremos el siguiente comando:

```
pablo@carpet:~$ ssh usuario@nas.corp.carpet4you.site
```

10.8 Servicio SSH autenticado con clave pública-privada

10.8.1 Configuración del servicio

Nota: La interfaz se encuentra en Inglés.

Para acceder a la configuración del servicio SSH debemos navegar desde el menú izquierdo a Services > SSH.

Ya hemos visto en el apartado alterior algunas de las modificaciones que podíamos realizar. Para esta práctica vamos a activar la autenticación SSH mediante infraestructura de clave pública.

En el apartado de configuración debemos modificar algunos ajustes:

- Desactivar la autenticación por contraseña. Solo queremos que se pueda iniciar sesión utilizando la clave pública.
- Activar, si no lo estuviera ya el interruptor de *Public Key Authentication*.

Truco: Es altamente recomendable cambiar el puerto por uno no estándar. En este caso no se va a realizar, aunque es un *must-do* para añadir una capa de seguridad adicional a nuestro servidor. Al igual que deshabilitar el usaurio root.

Cabe una mención especial a la posibilidad de activar la autenticación en dos factores para SSH. A través de este enlace se puede obtener más información.

Una vez realizadas las modificaciones desde la interfaz web, guardamos los cambios y los aplicamos.

10.8.2 Generación de claves

Usaremos el usuario «user» para este ejercicio.

Para generar un par de claves nuevo debemos utilizar el siguientes comando:

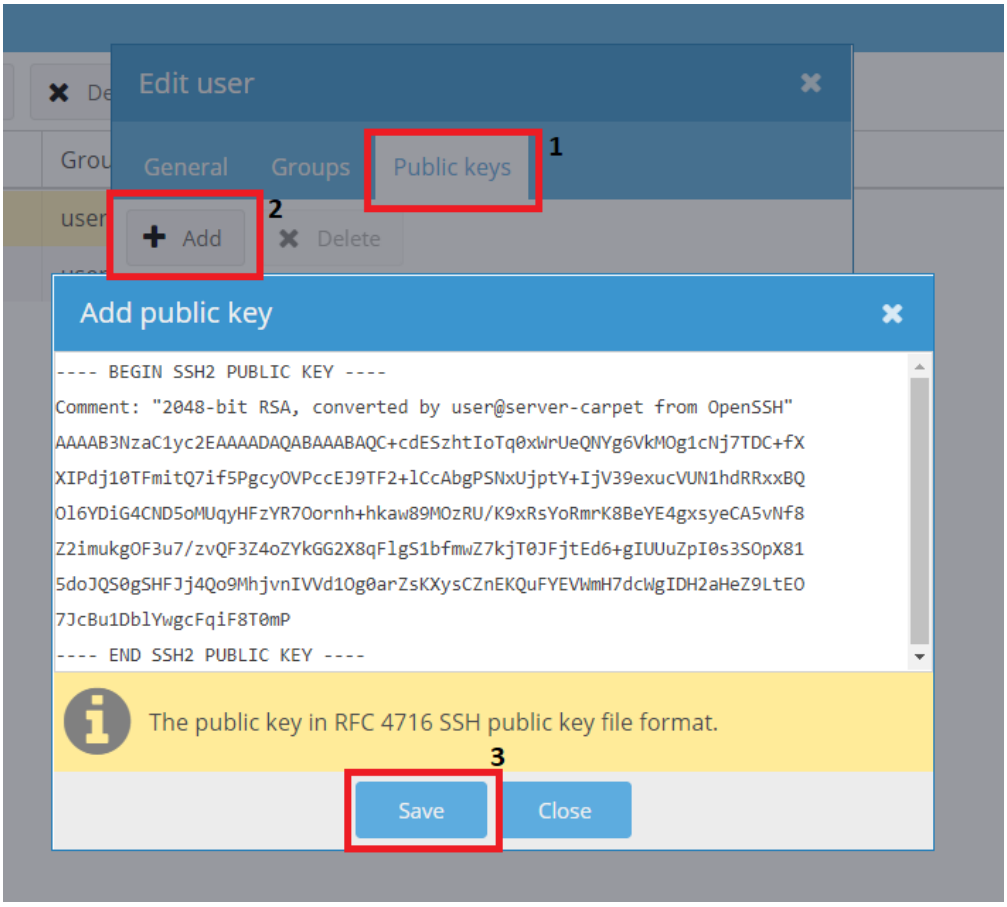
```
pablo@carpet:~$ ssh-keygen -t rsa
    Generating public/private rsa key pair.
    Enter file in which to save the key (/home/user/.ssh/id_rsa): user
    Enter passphrase (empty for no passphrase):
    Enter same passphrase again:
    Your identification has been saved in user.
    Your public key has been saved in user.pub.
    The key fingerprint is:
    SHA256:J4Fc6i7vVuZNatQmOxlKGGSyR4Ax0mluvHyhEBLyxAE user@server-carpet
    The key's randomart image is:
    +---[RSA 2048]----+
    |EB++    .        |
    |*+* +. +         |
    |.=.*  + .        |
    |. = +.   .       |
    | + + +. S..      |
    |  + o.. *o+      |
    |   ....* X       |
    |     oo B .      |
    |     oo. .       |
    +----[SHA256]-----+


    # Movemos las claves a la carpeta .ssh de nuestro equipo cliente para tenerlas␣
↪localizadas.
    user@carpet:~$ mv user .ssh/
    user@carpet:~$ mv user.pub .ssh/
```

OpenMediaVault necesita que la clave pública sea introducida en un formato consecuente con el estandar RFC4716. Después de crearla necesitamos ejecutar el siguiente comando:

```
pablo@carpet:~$ ssh-keygen -e -f ~/.ssh/user.pub
    ---- BEGIN SSH2 PUBLIC KEY ----
    Comment: "2048-bit RSA, converted by user@server-carpet from OpenSSH"
    AAAAB3NzaC1yc2EAAAADAQABAAABAQC+cdESzhtIoTq0xWrUeQNYg6VkMOg1cNj7TDC+fX
    XIPdj10TFmitQ7if5PgcyOVPccEJ9TF2+lCcAbgPSNxUjptY+IjV39exucVUN1hdRRxxBQ
    Ol6YDiG4CND5oMUqyHFzYR7Oornh+hkaw89MOzRU/K9xRsYoRmrK8BeYE4gxsyeCA5vNf8
    Z2imukgOF3u7/zvQF3Z4oZYkGG2X8qFlgS1bfmwZ7kjT0JFjtEd6+gIUUuZpI0s3SOpX81
    5doJQS0gSHFJj4Qo9MhjvnIVVd1Og0arZsKXysCZnEKQuFYEVWmH7dcWgIDH2aHeZ9LtEO
    7JcBu1DblYwgcFqiF8T0mP
    ---- END SSH2 PUBLIC KEY ----
```

10.8.3 Añadir claves al perfil del usuario

Debemos copiar la clave pública generada en el paso anterior. Es importante copiar la salida del comando de transformación (`ssh-keygen -e -f ~/.ssh/user.pub`) y no el contenido iniciar del archivo.



Para añadir la clave al perfil del usaurio nos desplazamos en el menú de la izquierda al apartado *Users*. Aquí, hacemos doble clic sobre el usuario que queremos modificar para acceder a sus ajustes.

Una vez en la ficha debemos hacer clic sobre la pestaña *Public Keys* (identificador *1* en la imagen). Aquí haremos clic en *Add* para añadir una nueva (identificador *2* en la imagen).

En el nuevo cuadro de diálogo quee nos muestra la aplicación debemos introducir la clave pública en el formato RFC4716. Si no lo hacemos así ni siquiera nos permitirá guardar la nueva clave.

Es importante también comprobar que el usuario forma parte del grupo `ssh`. De lo contrario, se le denegará el acceso.

Una vez introducida, hacemos clic en *Save*. Guardamos el usuario, los cambios y los aplicamos para que surtan efecto en el sistema.

10.8.4 Inicio de sesión remoto con clave

```
pablo@carpet:~$ ssh user@nas.corp.carpet4you.site -i .ssh/user
    The authenticity of host 'nas.corp.carpet4you.site (192.168.56.113)' can't be␣
↪established.
    ECDSA key fingerprint is SHA256:gLGmOzGi1mWOOKmf6dhc7xH2Ttm+ostwtN/cERjrrz0.
    Are you sure you want to continue connecting (yes/no)? yes
    Warning: Permanently added 'nas.corp.carpet4you.site,192.168.56.113' (ECDSA) to the␣
↪list of known hosts.
    #[Aquí da un error "feo" que procederemos a solucionar a continuación]
```

¡ERROR ENCONTRADO!

Error:

Hay un bug en OpenMediaVault al realizar la importación desde la GUI web.
Más información en este enlace
En mi caso, los *logs* del error generado se encuentran en este otro enlace

En la *issue* se comenta también un error de permisos:

```
root@nas:/var/lib/openmediavault/ssh/authorized_keys# cd /
root@nas:/# ls -lah
total 72K
drwxrwxr-x  20 root root 4,0K oct 26 12:35 .
drwxrwxr-x  20 root root 4,0K oct 26 12:35 ..
lrwxrwxrwx   1 root root    7 oct 26 12:34 bin -> usr/bin
drwxr-xr-x   3 root root 4,0K oct 26 13:41 boot
drwxr-xr-x  17 root root 3,4K oct 30 13:50 dev
drwxrwxr-x  94 root root 4,0K oct 30 14:35 etc
drwxr-xr-x   3 root root 4,0K oct 27 23:19 export
drwxr-xr-x   2 root root 4,0K jul 10  2020 home
lrwxrwxrwx   1 root root   35 oct 26 12:34 initrd.img -> boot/initrd.img-5.7.0-0.bpo.2-amd64
lrwxrwxrwx   1 root root   35 oct 26 12:34 initrd.img.old -> boot/initrd.img-5.7.0-0.bpo.2-amd64
lrwxrwxrwx   1 root root    7 oct 26 12:34 lib -> usr/lib
lrwxrwxrwx   1 root root    9 oct 26 12:34 lib32 -> usr/lib32
lrwxrwxrwx   1 root root    9 oct 26 12:34 lib64 -> usr/lib64
lrwxrwxrwx   1 root root   10 oct 26 12:34 libx32 -> usr/libx32
drwx------   2 root root  16K oct 26 12:34 lost+found
drwxr-xr-x   3 root root 4,0K sep 21  2020 media
drwxr-xr-x   3 root root 4,0K oct 29 08:33 mnt
drwxr-xr-x   2 root root 4,0K sep 21  2020 opt
dr-xr-xr-x 211 root root    0 oct 30 13:49 proc
drwx------   6 root root 4,0K oct 30 14:37 root
drwxr-xr-x  28 root root 1,1K oct 30 14:56 run
lrwxrwxrwx   1 root root    8 oct 26 12:34 sbin -> usr/sbin
drwxr-xr-x   2 root root 4,0K sep 17  2020 sharedfolders
drwxr-xr-x   7 root root 4,0K oct 26 13:46 srv
dr-xr-xr-x  13 root root    0 oct 30 13:49 sys
drwxrwxrwt   8 root root  160 oct 30 14:39 tmp
drwxr-xr-x  13 root root 4,0K oct 26 12:35 usr
drwxr-xr-x  12 root root 4,0K oct 26 12:35 var
lrwxrwxrwx   1 root root   32 oct 26 12:35 vmlinuz -> boot/vmlinuz-5.7.0-0.bpo.2-amd64
lrwxrwxrwx   1 root root   32 oct 26 12:35 vmlinuz.old -> boot/vmlinuz-5.7.0-0.bpo.2-amd64
```

Viendo los *logs*, parece que además de la ruta `/var/lib/openmediavault/ssh/authorized_keys/user` (donde se genera el error de permisos, `Authentication refused: bad ownership or modes for directory /`) intenta buscar la clave pública en el siguiente archivo: `/srv/dev-disk-by-id-md-name-nas-RAID5Carpet4You/home/user/.ssh/authorized_keys`.

Vamos a probar a añadir a esta ruta la clave. Antes de nada, debemos crear el directorio `.ssh/`, pues este no existe en el home del usuario. Aquí debemos crear el archivo `authorized_keys`.

Copiaremos el archivo `/var/lib/openmediavault/ssh/authorized_keys/user` al nuevo archivo y reiniciamos el servicio SSH.

```
root@nas: cp /var/lib/openmediavault/ssh/authorized_keys/user /srv/dev-disk-
↪by-id-md-name-nas-RAID5Carpet4You/home/user/.ssh/authorized_keys
```

Por defecto el archivo tiene los permisos `-rw-------` y esto nos dará (me ha dado, de hecho) problemas a continuación. Los cambiaremos con el comando `chmod 644 authorized_keys` a `-rw-r--r--`.

También debe ser el usuario el propietario del archivo, como podemos ver en este enlace. Para hacerle propietario utilizamos el comando `chown user:users authorized_keys`.

Ahora en los *logs* si probamos la conexión de nuevo podemos ver «cosas» diferentes que tiene «mucha mejor pinta»:

```
Oct 30 15:24:53 nas sshd[16530]: debug1: trying public key file /srv/dev-
↪disk-by-id-md-name-nas-RAID5Carpet4You/home/user/.ssh/authorized_keys
Oct 30 15:24:53 nas sshd[16530]: debug1: fd 4 clearing O_NONBLOCK
Oct 30 15:24:53 nas sshd[16530]: debug1: /srv/dev-disk-by-id-md-name-nas-
↪RAID5Carpet4You/home/user/.ssh/authorized_keys:1: matching key found: RSA␣
↪SHA256:wpOSevL3o4r9SNzrh0WDGhlXb1aHzgfS+ZB29YkRofI
Oct 30 15:24:53 nas sshd[16530]: debug1: /srv/dev-disk-by-id-md-name-nas-
↪RAID5Carpet4You/home/user/.ssh/authorized_keys:1: key options: agent-
↪forwarding port-forwarding pty user-rc x11-forwarding
Oct 30 15:24:53 nas sshd[16530]: Accepted key RSA␣
↪SHA256:wpOSevL3o4r9SNzrh0WDGhlXb1aHzgfS+ZB29YkRofI found at /srv/dev-disk-
↪by-id-md-name-nas-RAID5Carpet4You/home/user/.ssh/authorized_keys:1
Oct 30 15:24:53 nas sshd[16530]: debug1: restore_uid: 0/0
Oct 30 15:24:53 nas sshd[16530]: Postponed publickey for user from 192.168.
↪56.109 port 54142 ssh2 [preauth]
Oct 30 15:24:59 nas sshd[16530]: debug1: userauth-request for user user␣
↪service ssh-connection method publickey [preauth]
[...]
Oct 30 15:24:59 nas sshd[16530]: debug1: PAM: establishing credentials
Oct 30 15:24:59 nas sshd[16530]: pam_unix(sshd:session): session opened for␣
↪user user by (uid=0)
```

En el terminal cliente podemos ver la conexión establecida:

```
user@server-carpet:~$ ssh user@nas.corp.carpet4you.site -i .ssh/user
Enter passphrase for key '.ssh/user':
Linux nas.corp.carpet4you.site 5.7.0-0.bpo.2-amd64 #1 SMP Debian 5.7.10-1~bpo10+1 (2020-07-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Oct 30 15:24:59 2021 from 192.168.56.109
$ who
root     ttyl         2021-10-30 15:04
root     pts/0        2021-10-30 15:05 (192.168.56.106)
user     pts/1        2021-10-30 15:27 (192.168.56.109)
```

10.9 Servicio Rsync

10.9.1 Configuración del servicio

Nota: La interfaz se encuentra en Inglés.

Para acceder a la configuración del servicio Rsync debemos navegar desde el menú izquierdo a Services > Rsync.

Aquí, en la parte superior, vemos dos pestañas: *Jobs* y *Server*. Seleccionamos *Server* para configurarlo.

Jobs para configurar trabajos como **cliente** Rsync y *Server* para que OpenMediaVault actúe como **servidor** Rsync ofreciendo módulos a clientes.

Dentro de *Server* hay dos opciones: *Settings* y *Modules*. En la «jerga» de Rsync, los módulos son las carpetas compartidas

Para **activar el servicio Rsync** debemos marcar el interruptor. El puerto lo mantendremos en el por defecto.

Al igual que con SSH, podemos añadir opciones extra no contempladas en la GUI. Las posibles modificaciones están recogidas en este enlace.

10.9.2 Habilitar módulo

Para gestionar los módulos («carpetas compartidas») de Rsync, debemos navegar hasta *Services > Rsync > Server > Modules*.

Hacemos clic en *Add* y completamos los datos que nos solicita la interfaz:

Add module

General | Users

Enable

Shared folder: home [on RAID5FS, home/]
The location of the files to share.

Name: home
The name of the share.

User: nobody
This option specifies the user name that file transfers to and from that module should take place.

Group: users
This option specifies the group name that file transfers to and from that module should take place.

Use chroot: Enable chroot.
If this option is set, the daemon will chroot to the shared folder path before starting the file transfer with the client. Then it is not possible to map users and groups by name and the daemon is not being able to follow symbolic links that are either absolute or outside of the new root path.

Authenticate users: Enable user authentication
If set then the client will be challenged to supply a username and password to connect to the module.

Read only: Set read only
If this option is set, then any attempted uploads will fail.

Write only: Set write only
If this option is set, then any attempted downloads will fail.

List: Enable module listing
This option determines if this module should be listed when the client asks for a listing of available modules.

Max. connections: 0
This option specifies the maximum number of simultaneous connections. 0 means no limit.

Hosts allow
This option is a comma, space, or tab delimited set of hosts which are permitted to access this module. You can specify the hosts by name or IP number. Leave this field empty to use default settings.

Hosts deny
This option is a comma, space, or tab delimited set of host which are NOT permitted to access this module. Where the lists conflict, the allow list takes precedence. In the event that it is necessary to deny all by default, use the keyword ALL (or the netmask 0.0.0.0/0) and then explicitly specify to the hosts allow parameter those hosts that should be permitted access. Leave this field empty to use default settings.

Comment

Save | Reset | Cancel

En esta misma ventana, desde la pestaña *Users* añadimos a nuestro usuario. (Si no lo hacemos no dejará guardarlo. Eso sí, no nos avisará de cuál es el error).

10.9.3 Conexión desde el cliente

Desde el equipo cliente:

```
user@server-carpet:~$ rsync ^C
user@server-carpet:~$ mkdir ./prueba
user@server-carpet:~$ echo "Hola esto es una prueba" > prueba/hola.txt

user@server-carpet:~$ rsync -avh ./prueba user@nas.corp.carpet4you.site::home
Password: # [Introducimos contraseña]
sending incremental file list
prueba/
prueba/hola.txt

sent 164 bytes  received 39 bytes  81.20 bytes/sec
total size is 24  speedup is 0.12
```

10.10 Servicio Rsync automatizado

En el enunciado del ejercicio se nos solicita que la tarea de sincronización Rsync se ejecute de forma automática cada 15 minutos.

Para hacerlo debemos:
1) Utilizar una clave SSH para autenticarnos contra Rsync.
2) Programar una tarea *cron* para la ejecución de la sincronización de forma automatizada.

10.10.1 Generar clave SSH

Por motivos de seguridad **no vamos a usar la misma clave SSH**. Por motivos intrínsecos a la ejecución del comando (debe ejecutarse de forma automática, sin interacción del usuario) la clave no debe tener contraseña simétrica.

Desde el cliente, vamos a generarla. uando nos pida introducir contraseña, haremos clic en Intro para no fijar ninguna:

```
pablo@cliente:~$ ssh-keygen -t rsa
```

La guardaremos en `~/.ssh/backup`.

10.10.2 Copiar clave pública a servidor

Como ya hemos visto en el apartado de *Servicio SSH autenticado con clave pública-privada*, ocurren cosas raras al intentar añadir las claves de un usuario desde la GUI web.

Iniciando en el propio servidor (mediante SSH, por ejemplo), añadimos la clave publica al archivo `/srv/dev-disk-by-id-md-name-nas-RAID5Carpet4You/home/user/.ssh/authorized_keys`.

Después de copiarla tendremos, al menos, dos clave: * La clave pública para el inicio SSH «típico». * La clave pública que utilizaremos para la autenticación contra Rsync.

Veamos un ejemplo:

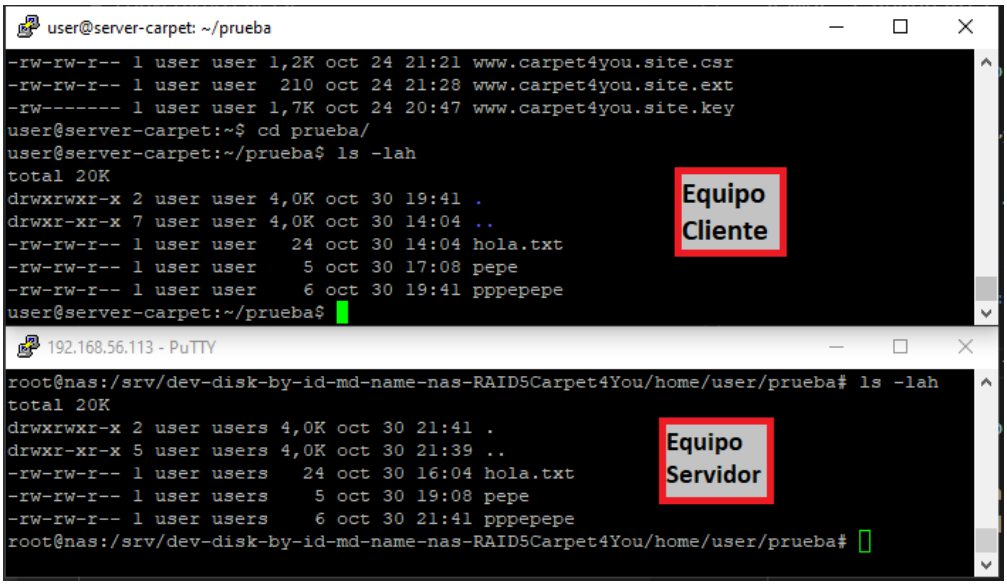
```
ssh-rsa␣
↪AAAAB3NzaC1yc2EAAAADAQABAAABAQC+cdESzhtIoTq0xWrUeQNYg6VkMOg1cNj7TDC+fXXIPdj10TFmitQ7if5PgcyOVPccEJ9TF
↪K9xRsYoRmrK8BeYE4gxsyeCA5vNf8Z2imukgOF3u7/
↪zvQF3Z4oZYkGG2X8qFlgS1bfmwZ7kjT0JFjtEd6+gIUUuZpI0s3SOpX815doJQS0gSHFJj4Qo9MhjvnIVVd1Og0arZsKXysCZnEKQ

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDayMy/MPci3iiY+bVSuB7/Ankdmxcijnef0AY1hfdOmI5xz7f/
↪I6DJ/xdkskqhXOl0OgB2kyOnaIys6drCC1+rNyOTuWemg/
↪Hn8XRgcudGWmyMQ8XYUwrWyitGHa2LTdHAiLM0i1LX67svACVWInAS7MPCn02uIfr5eBzH3moQoTjsVlvcLj4pnUAVQPgDqqI1nf6
↪YF7+hJ6eakeFOSrD/
↪ZvaWb+zDdC+RdM3qwOe669iIhiK7O9lwLf7NCuhvXo1eqkMGj+Ocf9OnyNWUKzdqdEqAELV7mioU2qgE8vq+WtYb/
↪eODTgGzys/TfXCn7m+B user@server-carpet
```

10.10.3 Probar conexión a carpeta

Para comprobar si funciona Rsync debemos generar algunos archivos y después comprobar si se copian.

```
user@cliente:~$ sudo rsync -avRh -e "ssh -i /home/user/.ssh/backup"  prueba/ user@nas.
↪corp.carpet4you.site:/srv/dev-disk-by-id-md-name-nas-RAID5Carpet4You/home/user/
```

Este es el resultado:



10.10.4 Tarea cron

Añadiremos la tarea crontab con el siguiente comando:

```
user@cliente:~$ sudo su #Necesitamos que la tarea la ejecute root
user@cliente:~$ crontab -e

# En el archivo que se nos abre añadimos el siguiente comando:
    */15 * * * * sudo rsync -aRh -e "ssh -i /home/user/.ssh/backup"  /home/user/prueba␣
↪user@nas.corp.carpet4you.site:/srv/dev-disk-by-id-md-name-nas-RAID5Carpet4You/home/
↪user/
```

(continué en la próxima página)

(proviene de la página anterior)

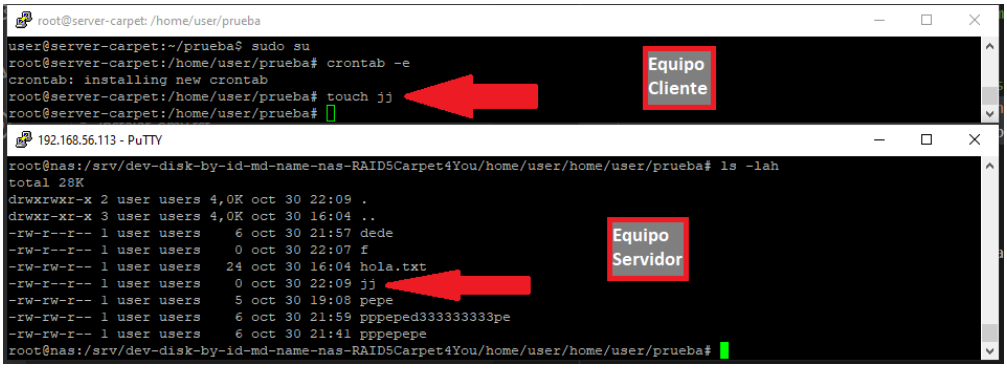
10.10.5 Comprobación cron

Crearemos algún archivo en la carpeta prueba y veremos si se copia en el servidor.

Truco:

Puede ser útil cambiar el cron para que se ejecute cada minuto durante las pruebas.
Para configurar la programación de cron, esta página es muy útil.

¡Funciona!



10.10.6 Limitar acceso desde IP cliente

Como medida de seguridad adicional, limitaremos el uso de la clave pública. Indicaremos que únicamente se pueda utilizar desde el equipo cliente. Para identificar al equipo usaremos su clave pública.

```
from="192.168.56.109" ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDayMy/MPci3iiY+bVSuB7/
↪Ankdmxcijnef0AY1hfdOmI5xz7f/I6DJ/xdkskqhXOl0OgB2kyOnaIys6drCC1+rNyOTuWemg/
↪Hn8XRgcudGWmyMQ8XYUwrWyitGHa2LTdHAiLM0i1LX67svACVWInAS7MPCn02uIfr5eBzH3moQoTjsVlvcLj4pnUAVQPgDqqI1nf6
↪YF7+hJ6eakeFOSrD/
↪ZvaWb+zDdC+RdM3qwOe669iIhiK7O9lwLf7NCuhvXo1eqkMGj+Ocf9OnyNWUKzdqdEqAELV7mioU2qgE8vq+WtYb/
↪eODTgGzys/TfXCn7m+B user@server-carpet
```

Solo para valientes

Cabe la posibilidad de restringir, mediante otra anotación en el archivo `authorized_keys`, qué comandos puede ejecutar el usuario.

10.1. *Descargar y comprobar OpenMediaVault*
10.2. *Instalar y configurar OpenMediaVault*
10.3. *Configuración de RAID inicial*
10.4. *Servicio SMB/CIFS*

10.5. *Servicio NFS*
10.6. *Servicio FTP*
10.7. *Servicio SSH*
10.8. *Servicio SSH autenticado con clave pública-privada*
10.9. *Servicio Rsync*
10.10. *Servicio Rsync automatizado*

CAPÍTULO 11

NextCloud («Nube»)

11.1 Instalación de Sistema Operativo

11.1.1 Configuración de la MV

Llamaremos a la máquina virtual *ASIR2.SYAD.P1.NextCloud*. Será tipo Linux, versión Ubuntu 20.04 64bits. Asignaremos 4GB de memoria RAM y no añadiremos durante la creación ningún disco duro, pues lo haremos después.

En tanto a la red, se configuran 2 adaptadores virtuales:

- Adaptador 1, configurado en modo NAT para la conexión a internet.
- Adaptador 2, confiugrado en modo solo-anfitrión, para la conexión vía web y a los servicios.

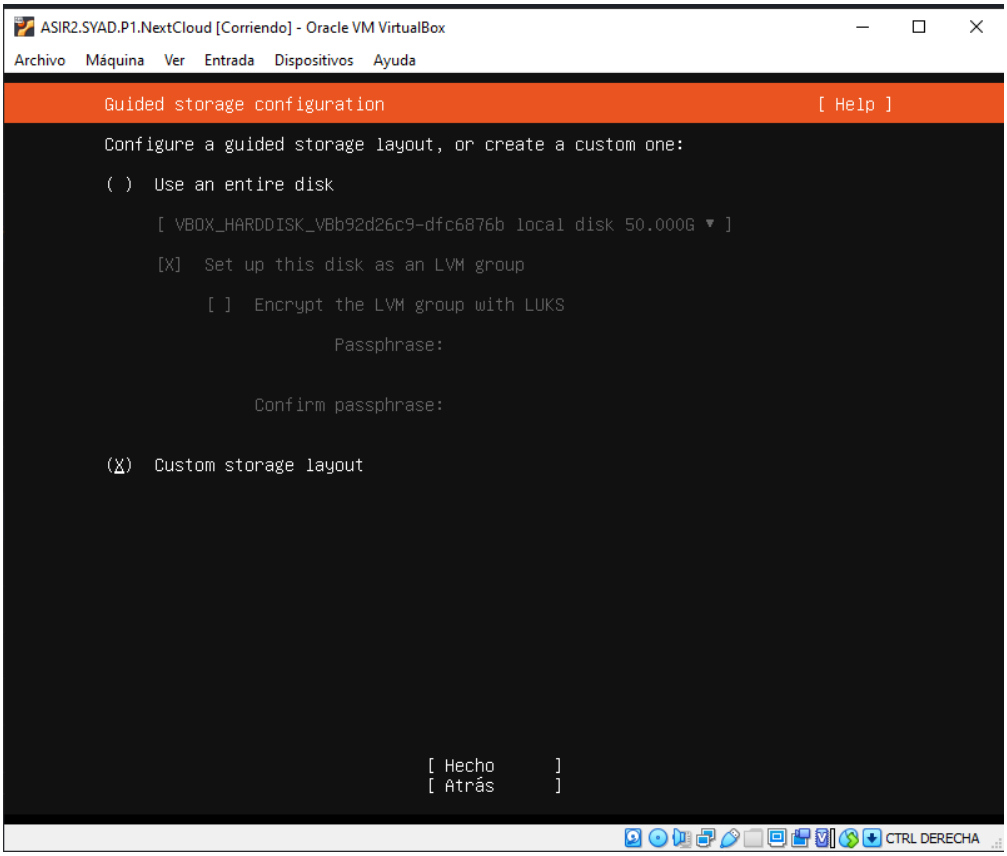
Sobre los discos, se crean los siguientes discos virtuales:

- 1 disco duro virtual de 10 Gb, que será donde instalaremos el arranque.
- 2 discos duros virtuales de 50 Gb. En estos instalaremos el sistema operativo, configurándolos en RAID 1 para la instalación del SO.
- 3 discos duros virtuales de 200 Gb. Sobre estos configuraremos RAID 5 para alojar los datos.

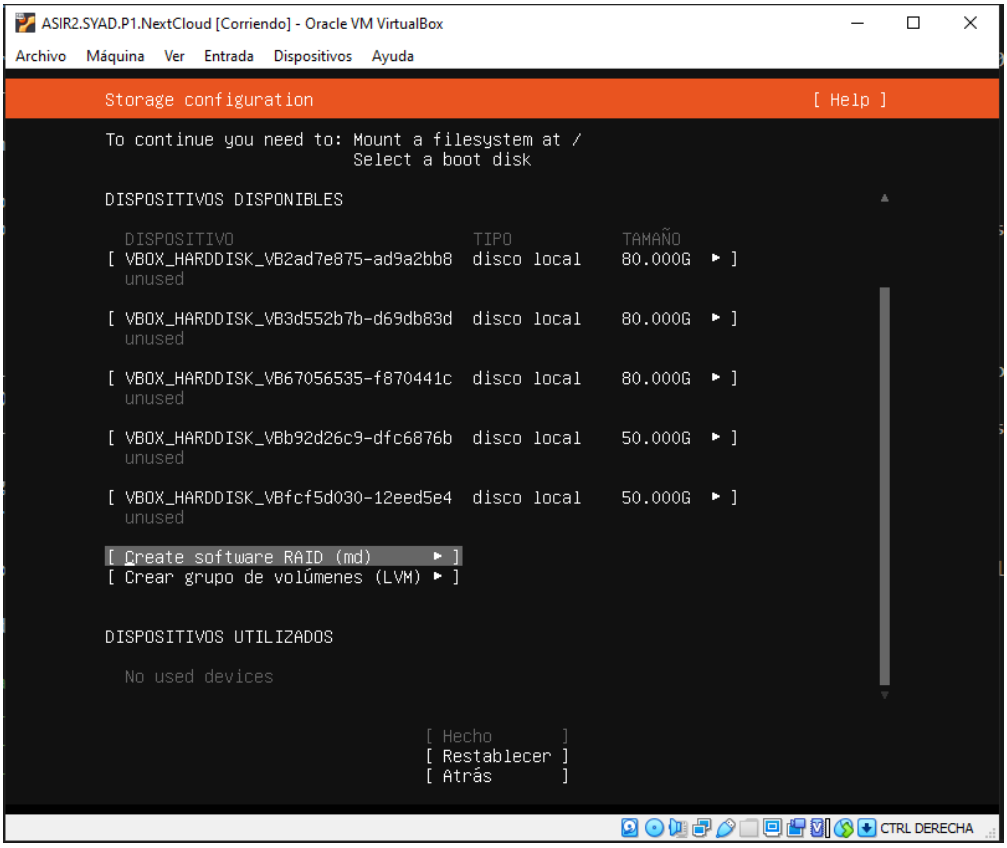
Configuración RAID 0 para SO

Puesto que considero bastante interesante la configuración del RAID 0 durante la instación, lo incluiremos en esta guía. Puede ser muy útil esta guía

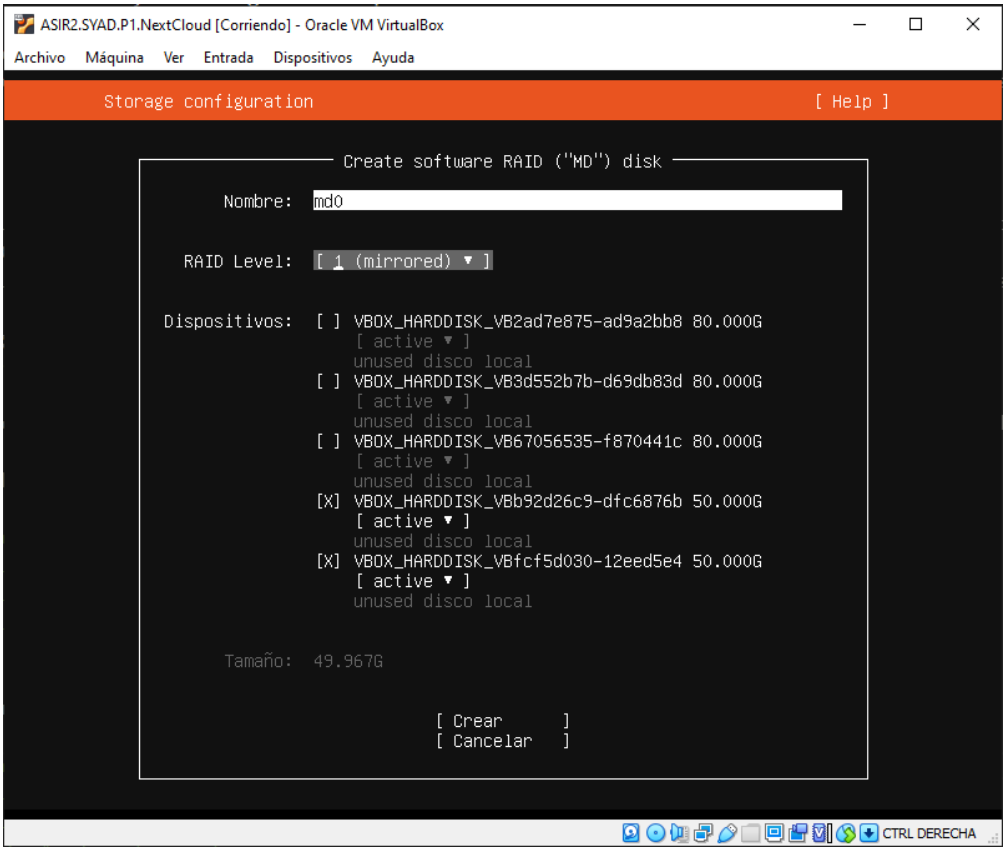
Llegados a la siguiente pantalla, hacemos clic en *Custom storage layout*:



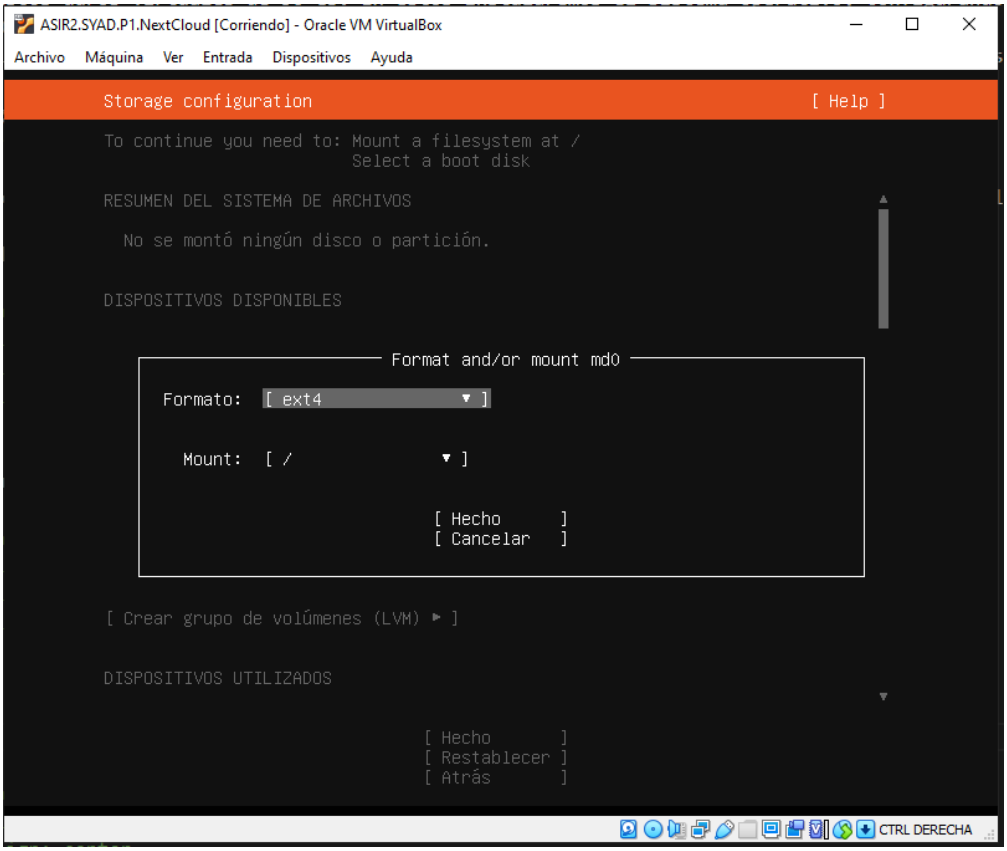
Marcamos que queremos configurar un RAID:



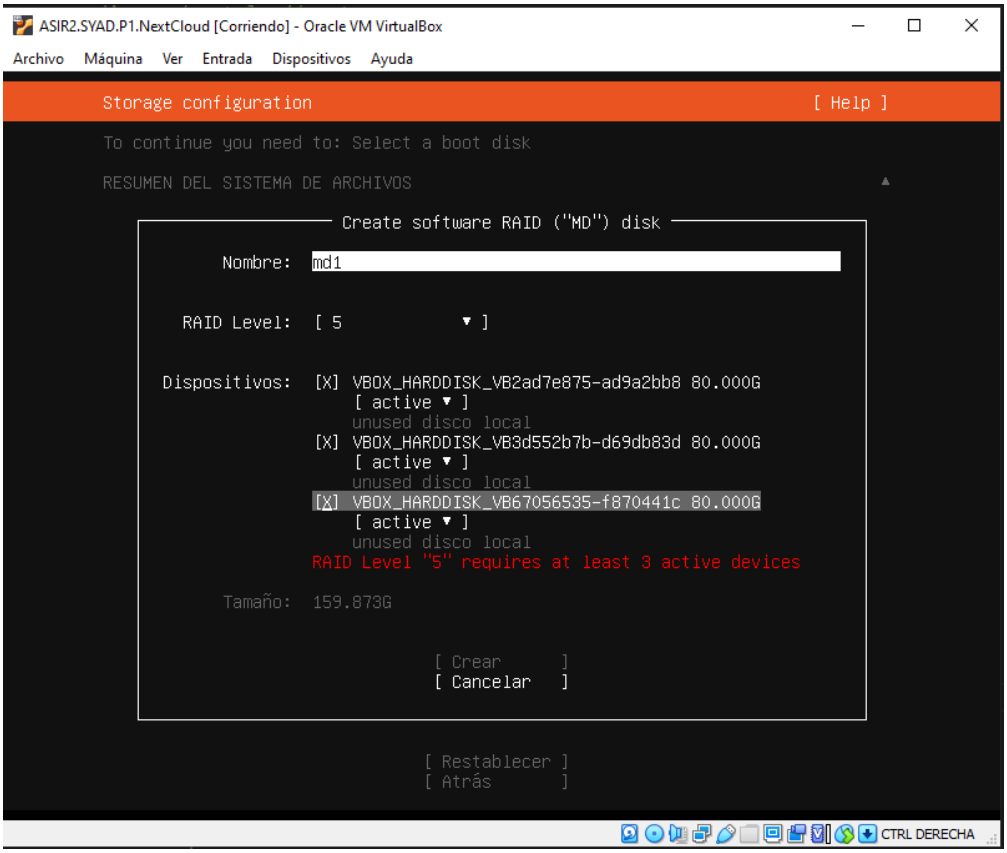
En la configuración del RAID, seleccionamos el nivel de RAID deseado y los discos destino.



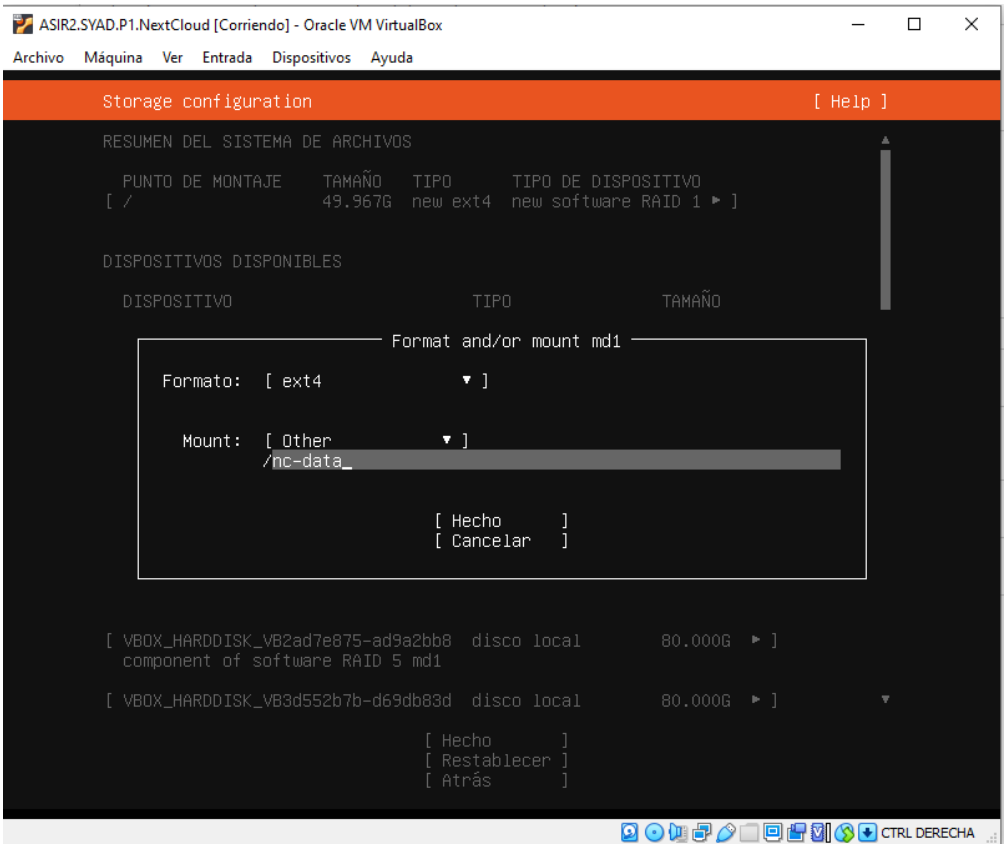
De nuevo en el resumen de discos, en el menú del RAID, hacemos clic en formatear. Utilizamos ext4 como sistema de archivos y / como punto de montaje.



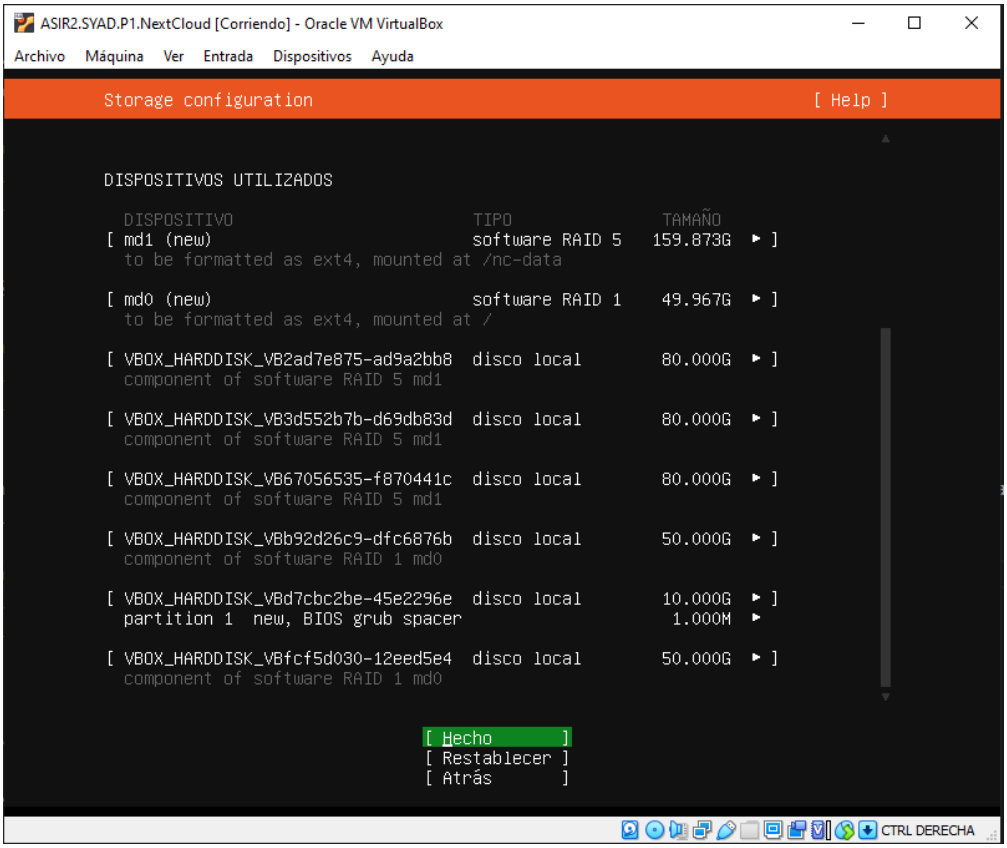
También aprovecharemos para crear el RAID 5 para los datos:



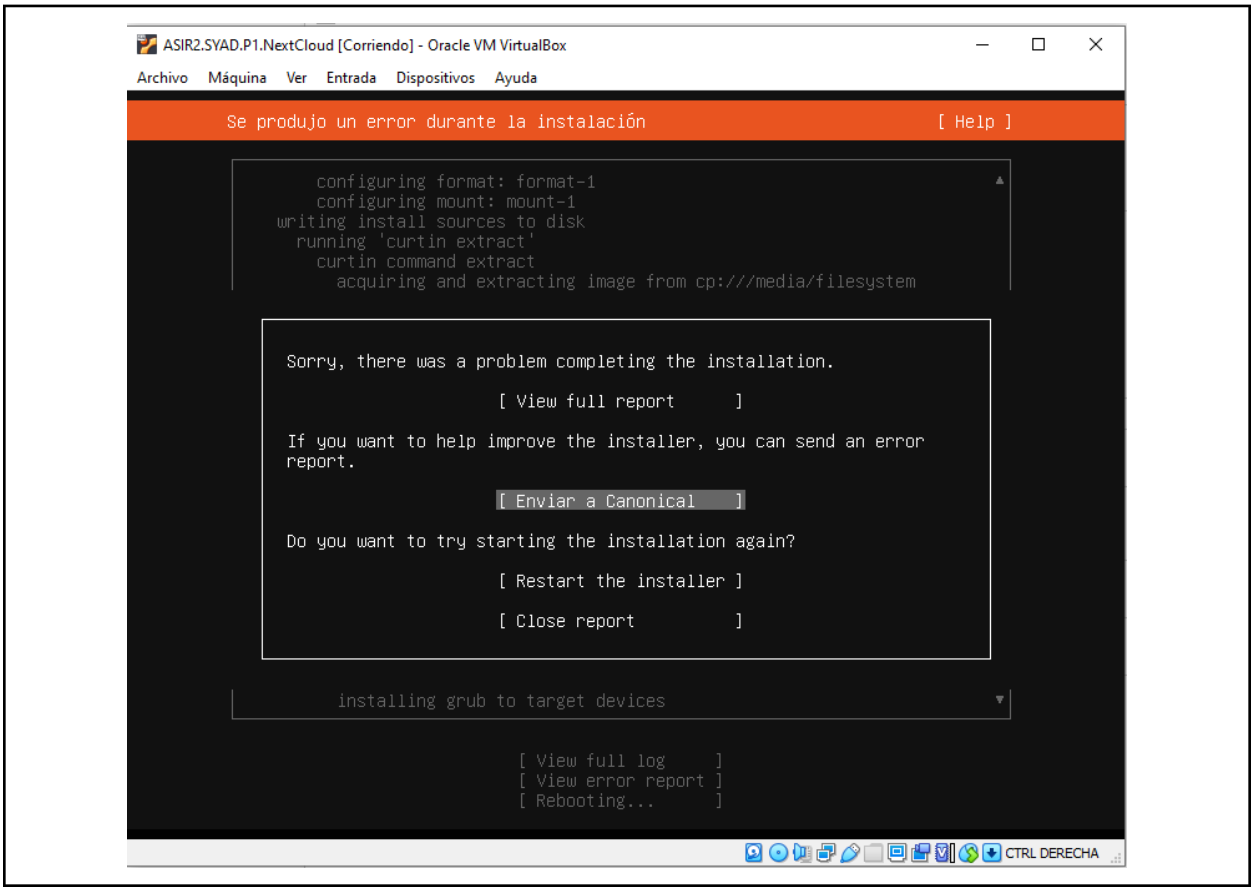
Indicamos que sea el disco de 10 Gb el que se utilizará para el *boot device*. También indicamos que el RAID 5 sea utilizado para los datos, y montado en la ruta `/nc-data`:



El resultado de los discos es el siguiente:



Error: Tras la segunda vez dando error en la instalación, se instala en un solo disco, sin RAID:



11.2 Instalación NextCloud

11.2.1 Paquetes necesarios

Instalaremos los siguientes paquetes desde la terminal:

```
sudo apt update
sudo apt install apache2 mariadb-server libapache2-mod-php7.4
sudo apt install php7.4-gd php7.4-mysql php7.4-curl php7.4-mbstring php7.4-intl
sudo apt install php7.4-gmp php7.4-bcmath php-imagick php7.4-xml php7.4-zip
```

11.2.2 Crear base de datos

NextCloud almacena la información en una base de datos MySQL/MariaDB.

Iniciaremos el proceso e iniciaremos sesión en el administrador de la base de datos para proceder a craer la base de datos que NextCloud usará:

```
# Iniciar el proceso, si no lo estuviera
sudo /etc/init.d/mysql start

# Iniciar sesión con el usuario root
sudo mysql -uroot -p
```

```
CREATE USER 'nc_pablo_oAb30'@'localhost' IDENTIFIED BY 'nc_pablo_pw_6BN6';
CREATE DATABASE IF NOT EXISTS nextcloud CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;
GRANT ALL PRIVILEGES ON nextcloud.* TO 'nc_pablo_oAb30'@'localhost';
```

Salimos, pues el propio NextCloud creará las tablas en la primera conexión:

```
quit;
```

11.2.3 Descargar NextCloud

Descargaremos la última versión d NextCloud:

1. Accedemos a la página de descarga de NextCloud.
2. Seleccionamos la versión *Server* y hacemos clic en *Download for Server*.
3. En la parte inferior de la página, haremos clic en el botón *Details and download options*.
4. En nuestro caso, utilizaremos el archivo tar comprimido y descargaremos:

- El instalador, la suma MD5 y la suma SHA256.
- Descargaremos la clave GPG de NextCloud y la firma .asc.

```
mkdir nextcloud-temp
cd nextcloud-temp
wget https://download.nextcloud.com/server/releases/nextcloud-22.2.0.tar.bz2
wget https://download.nextcloud.com/server/releases/nextcloud-22.2.0.tar.bz2.md5
wget https://download.nextcloud.com/server/releases/nextcloud-22.2.0.tar.bz2.sha256
wget https://download.nextcloud.com/server/releases/nextcloud-22.2.0.tar.bz2.asc
wget https://nextcloud.com/nextcloud.asc
```

Verificación del archivo:

```
pablo@cloud:~/nextcloud-temp$ md5sum -c nextcloud-22.2.0.tar.bz2.md5
nextcloud-22.2.0.tar.bz2: OK
pablo@cloud:~/nextcloud-temp$ sha256sum -c nextcloud-22.2.0.tar.bz2.sha256
nextcloud-22.2.0.tar.bz2: OK
```

Importación de la clave de NextCloud:

```
pablo@cloud:~/nextcloud-temp$ gpg --import nextcloud.asc
    gpg: directory '/home/pablo/.gnupg' created
    gpg: keybox '/home/pablo/.gnupg/pubring.kbx' created
    gpg: /home/pablo/.gnupg/trustdb.gpg: trustdb created
    gpg: key D75899B9A724937A: public key "Nextcloud Security <security@nextcloud.com>"␣
↪imported
    gpg: Total number processed: 1
    gpg:               imported: 1
```

Verificación de la firma:

```
pablo@cloud:~/nextcloud-temp$ gpg --verify nextcloud-22.2.0.tar.bz2.asc nextcloud-22.2.0.
↪tar.bz2
    gpg: Signature made Wed Sep 29 21:24:40 2021 UTC
    gpg:                using RSA key 28806A878AE423A28372792ED75899B9A724937A
    gpg: Good signature from "Nextcloud Security <security@nextcloud.com>" [unknown]
    gpg: WARNING: This key is not certified with a trusted signature!
    gpg:          There is no indication that the signature belongs to the owner.
    Primary key fingerprint: 2880 6A87 8AE4 23A2 8372  792E D758 99B9 A724 937A
```

11.2.4 Extracción de archivos

Usaremos el siguiente comando, teniendo en cuenta que puede tardar un poco, al ser bastantes archivos:

```
pablo@cloud:~/nextcloud-temp$ tar -xjvf nextcloud-22.2.0.tar.bz2
```

Copiamos el contenido a la raíz del servidor web:

```
pablo@cloud:~/nextcloud-temp$ cp -r nextcloud /var/www
```

11.2.5 Configuración servidor web

Crearemos el archivo `/etc/apache2/sites-available/nextcloud.conf`, añadiendo el siguiente contenido:

```
<VirtualHost *:80>
DocumentRoot /var/www/nextcloud/
ServerName  cloud.carpet4you.site

<Directory /var/www/nextcloud/>
    Require all granted
    AllowOverride All
    Options FollowSymLinks MultiViews

    <IfModule mod_dav.c>
    Dav off
    </IfModule>
</Directory>
</VirtualHost>
```

Activamos el sitio y reiniciamos Apache:

```
a2ensite nextcloud.conf
systemctl reload apache2
```

Activamos una serie de módulos necesarios:

```
a2enmod rewrite
a2enmod headers
a2enmod env
a2enmod dir
a2enmod mime
```

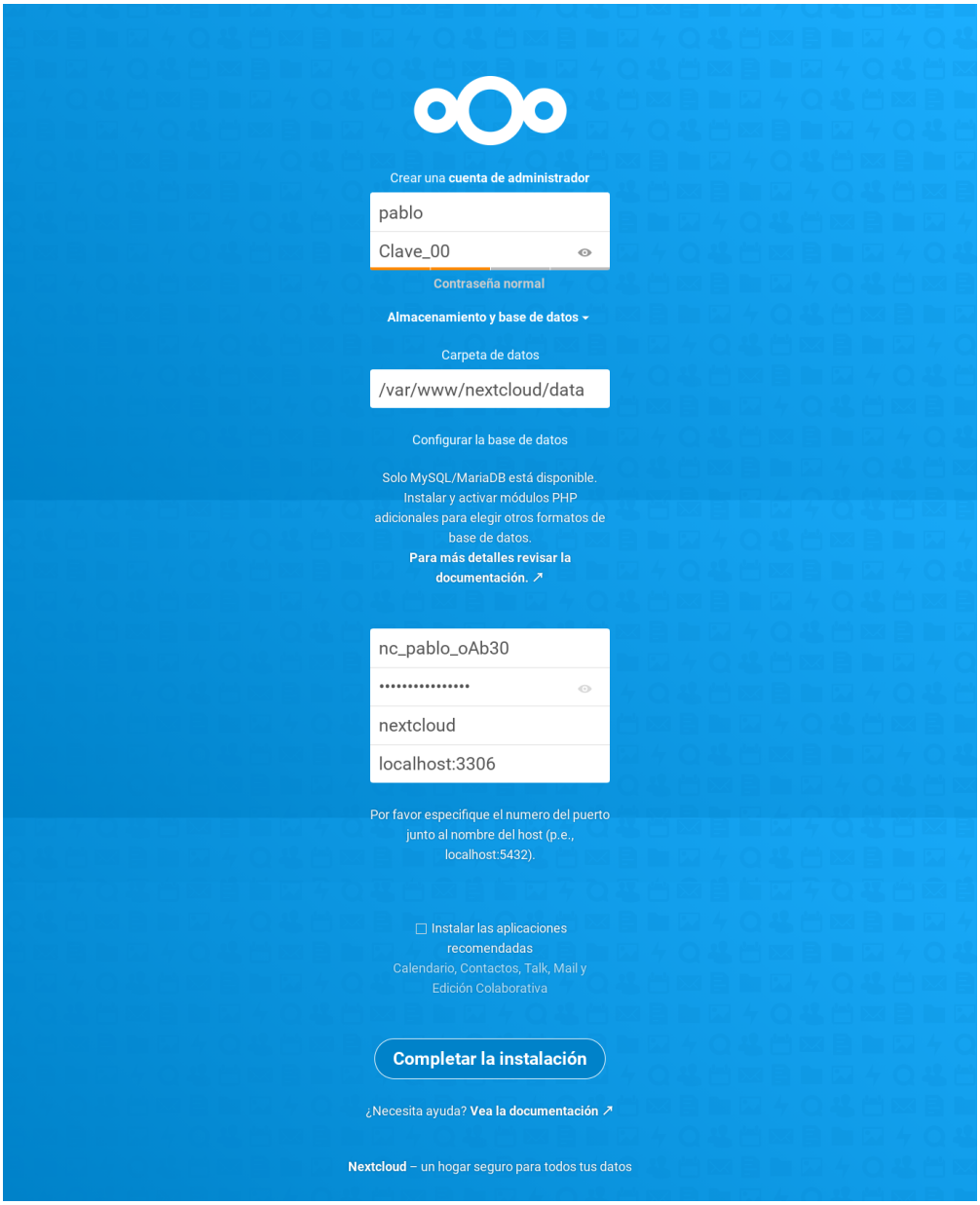
Cambiamos de propiedad los archivos:

```
chown -R www-data:www-data /var/www/nextcloud/
```

11.2.6 Primer acceso

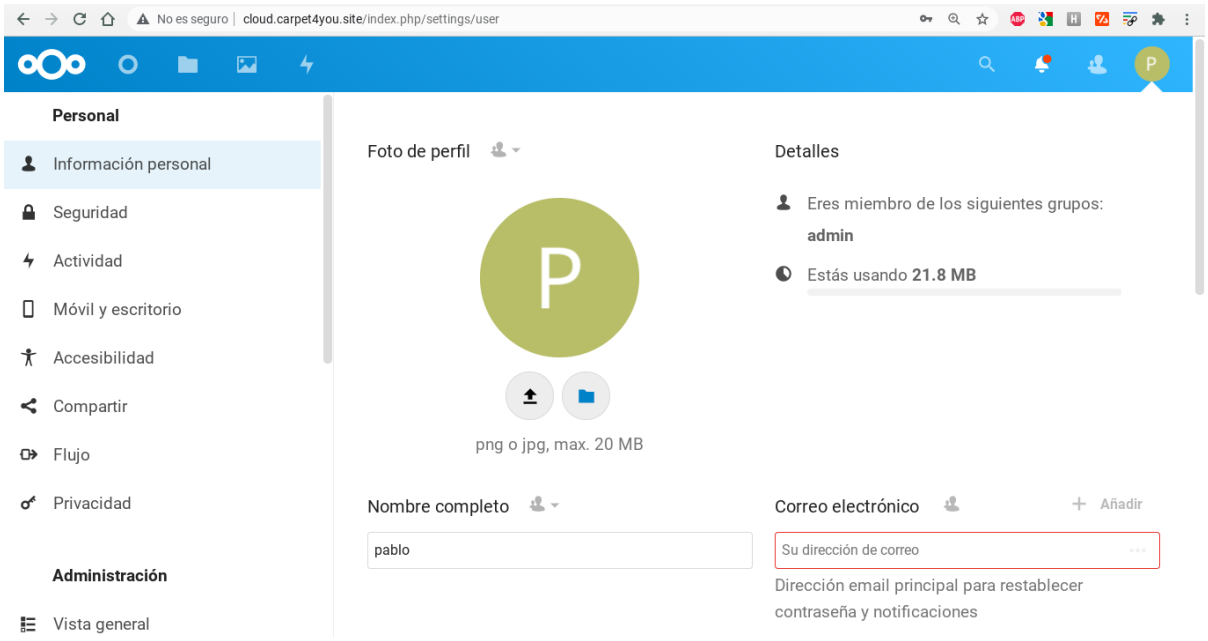
Añadiremos un registro A en cloud.carpet4you.site con la IP de la máquina virtual.

Al acceder a esta dirección, deberemos escribir los detalles de acceso a la base de datos:



Nota: no indicamos que instale Talk, Mail, Contacts ni Edición Colaborativa; pues lo haremos posteriormente.

En unos segundos estaremos dentro:



11.3 Securizar Nextcloud con SSL/TLS

Descargamos los certificados:

```
sudo mkdir /etc/certificados
cd /etc/certificados
wget https://raw.githubusercontent.com/gonzaleztroyano/ASIR2-SYAD-P1/main/public/cert-
↪letsencrypt/fullchain1.pem
wget https://raw.githubusercontent.com/gonzaleztroyano/ASIR2-SYAD-P1/main/public/cert-
↪letsencrypt/privkey1.pem
```

Modificamos el archivo `/etc/apache2/sites-available/nextcloud.conf` para que tenga el siguiente contenido:

```
<IfModule mod_ssl.c>
<VirtualHost *:80>
DocumentRoot /var/www/nextcloud/
ServerName  cloud.carpet4you.site

<Directory /var/www/nextcloud/>
    Require all granted
    AllowOverride All
    Options FollowSymLinks MultiViews

    <IfModule mod_dav.c>
    Dav off
    </IfModule>
</Directory>
RewriteEngine on
RewriteCond %{SERVER_NAME} =cloud.carpet4you.site
```

(continué en la próxima página)

(proviene de la página anterior)

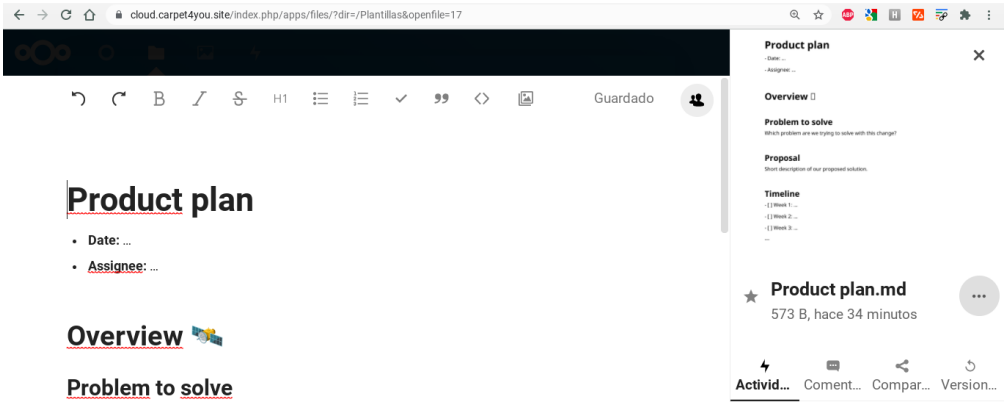
```
RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]
</VirtualHost>
```

En el archivo `/etc/apache2/sites-available/nextcloud-le-ssl.conf` añadimos:

```
<IfModule mod_ssl.c>
    <VirtualHost *:443>
    DocumentRoot /var/www/nextcloud/
    ServerName  cloud.carpet4you.site

    <Directory /var/www/nextcloud/>
        Require all granted
        AllowOverride All
        Options FollowSymLinks MultiViews

        <IfModule mod_dav.c>
        Dav off
        </IfModule>
    </Directory>

SSLCertificateFile /etc/letsencrypt/live/cloud.carpet4you.site/fullchain.pem
SSLCertificateKeyFile /etc/letsencrypt/live/cloud.carpet4you.site/privkey.pem
Include /etc/letsencrypt/options-ssl-apache.conf
</VirtualHost>
</IfModule>
```

Nota: Se ha utilizado certbot para la obtención del certificado Let's Encrypt y para la configuración de Apache.

Ya podemos acceder a la pagina mediante SSL:



11.4 Eliminar *index.php* de las URL

Activamos dos módulos de Apache:

```
sudo a2enmod rewrite
sudo a2enmod env
```

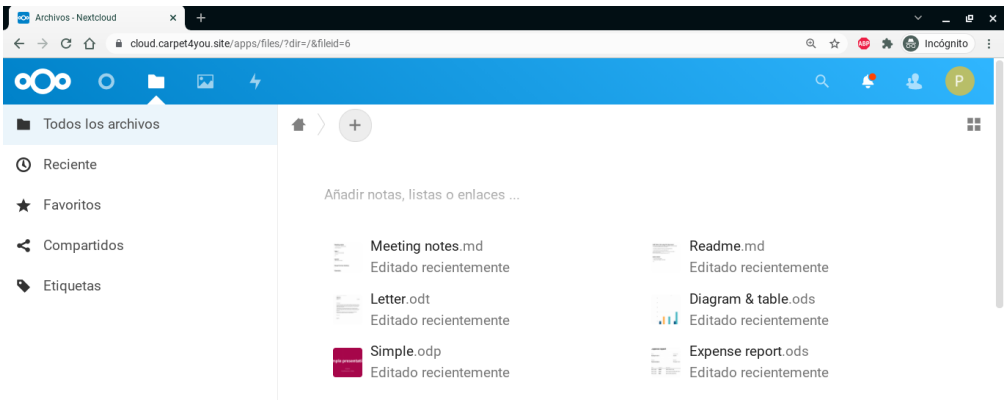
En el archivo `/var/www/nextcloud/config/config.php`

```
'overwrite.cli.url' => 'https://cloud.carpet4you.site/',
'htaccess.RewriteBase' => '/',
```

Ejecutamos:

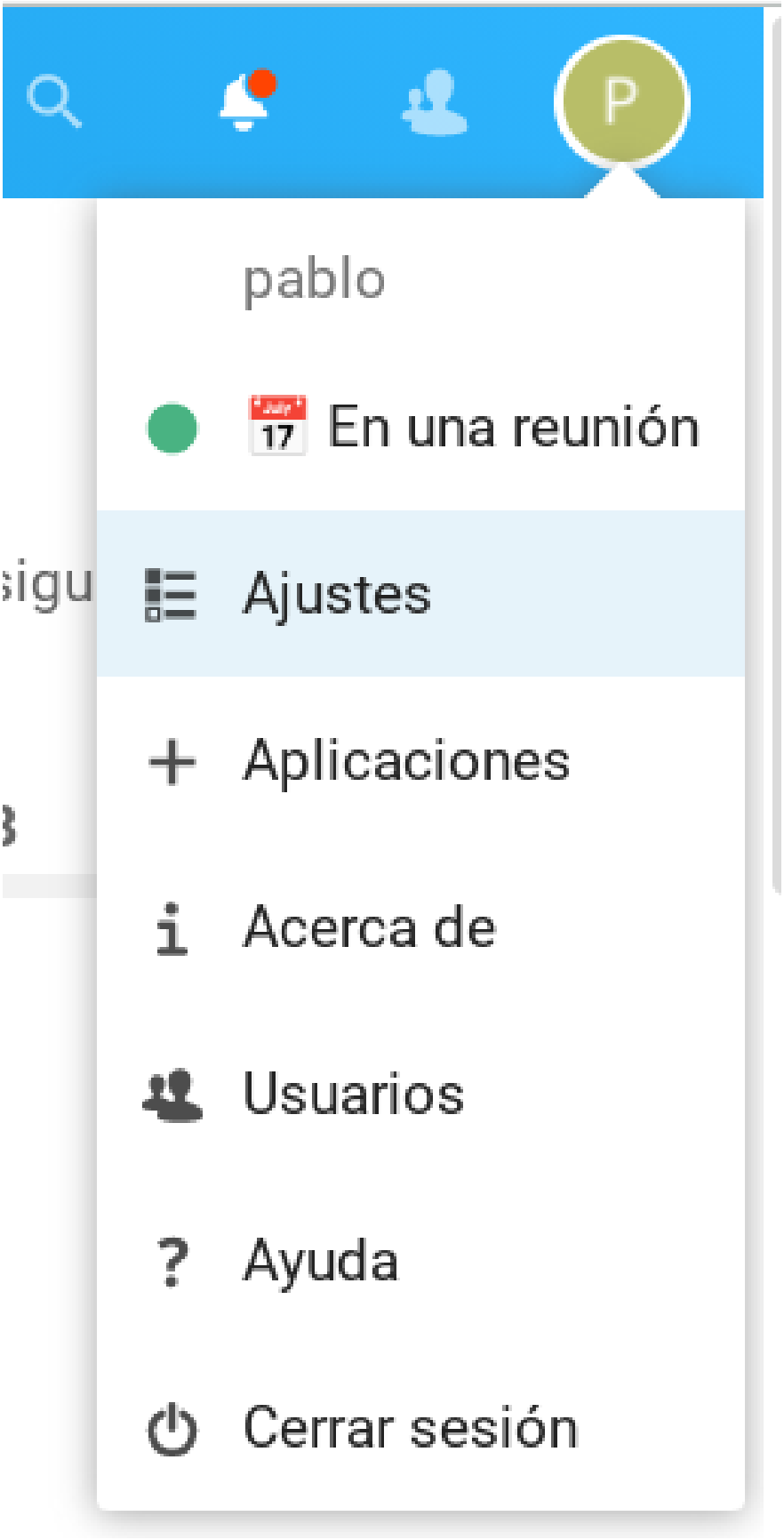
```
sudo -u www-data php /var/www/nextcloud/occ maintenance:update:htaccess
```

Ahora ya podemos ver la URL sin «index.php» en la misma:

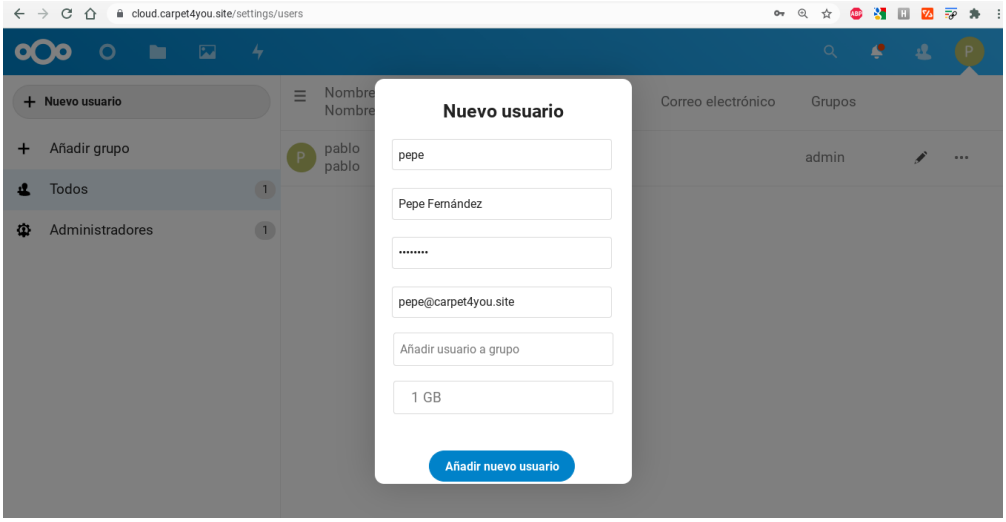


11.5 Creación de usuarios en NextCloud

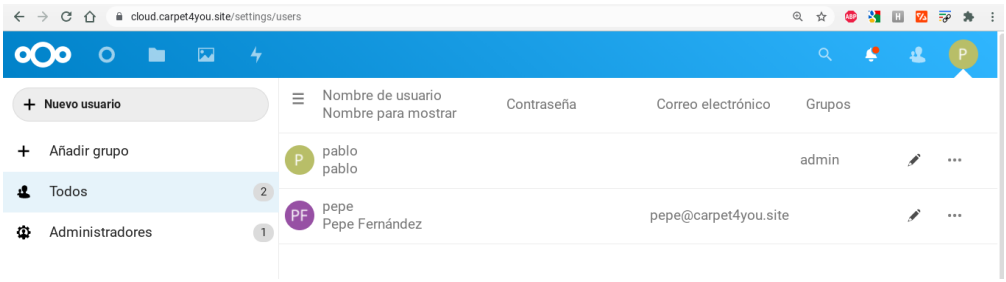
Para gestionar nuestra instancia de NextCloud debemos hacer clic en nuestra foto de perfil (que será previsiblemente la inicial de nuestro nombre de usuario). Entre las opciones que aparecen al hacerlo, debemos seleccionar *Usuarios*:


P
pablo
En una reunión
Ajustes
Aplicaciones
Acerca de
Usuarios
Ayuda
Cerrar sesión

En el botón de la parte superior izquierda, seleccionamos *Nuevo usuario*. Nos aparecerá una ventana en la que debemos introducir los datos para el nuevo usuario:



Después de guardar el usuario, ya lo podremos ver en la pantalla de gestión de usuarios:



11.6 Sincronización de datos cliente con NextCloud

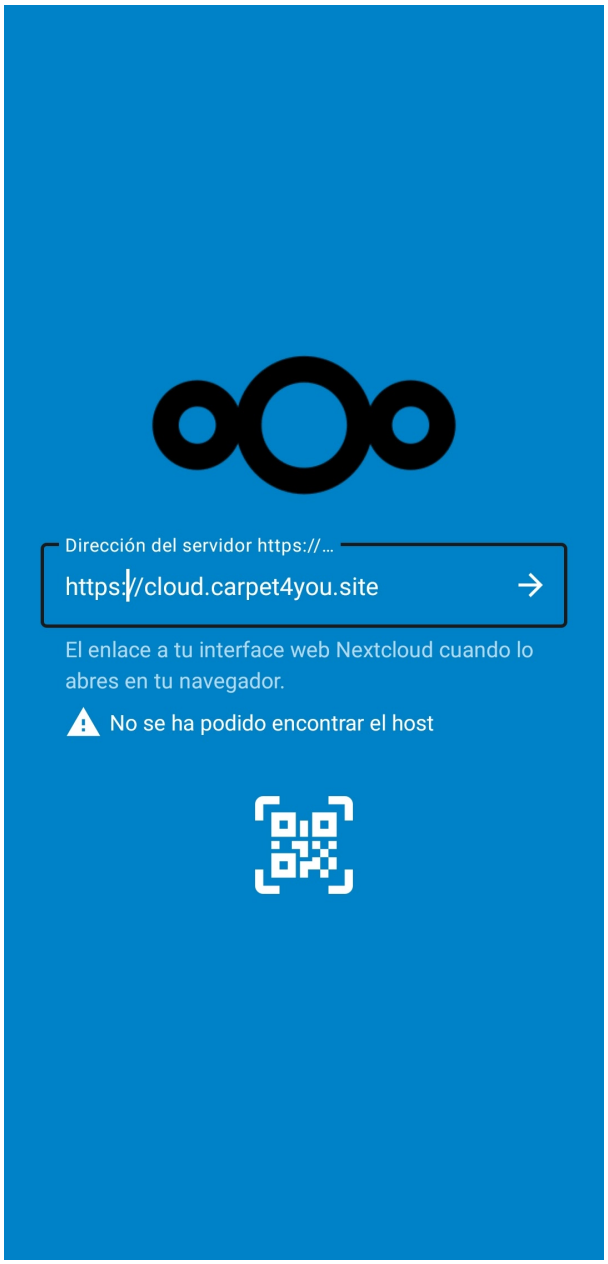
Descargamos la aplicación:

- Cliente android.
- Cliente iOS.
- Cliente Windows 10.
- Cliente macOS.
- Cliente Linux.

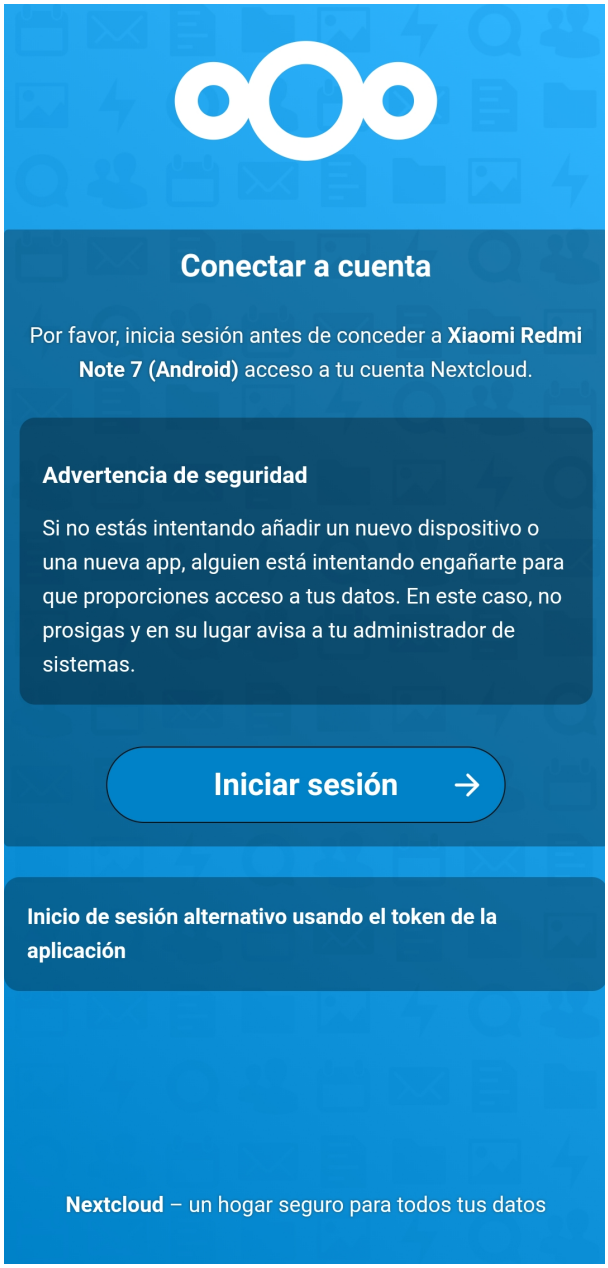
Nota: Las pruebas se realizarán con un cliente Android.

1. Instalar la aplicación.
2. Al lanzar la aplicación, veremos las opciones. Seleccionamos *Iniciar sesión*.

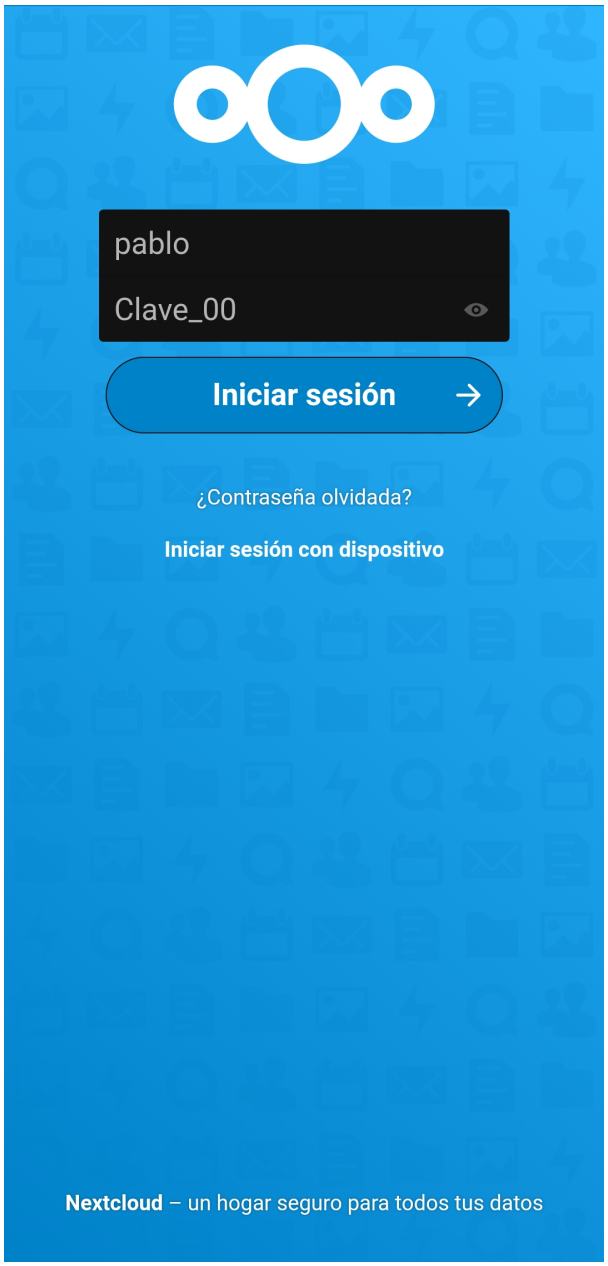
3. Completamos la URL de nuestra instancia de NextCloud.



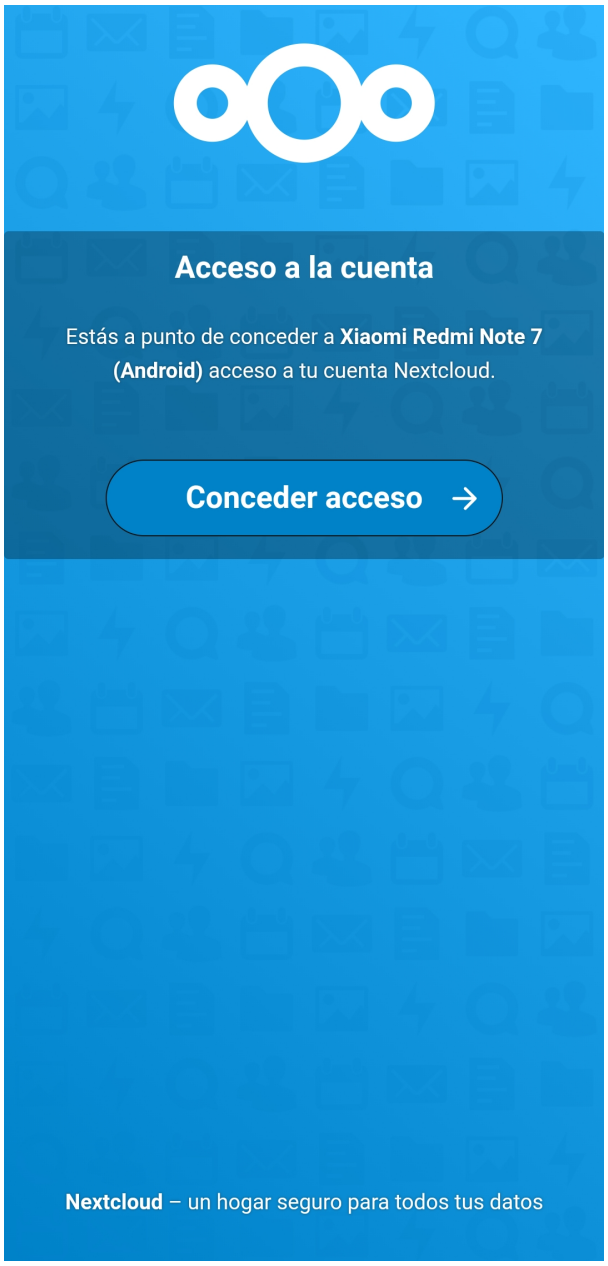
4. Nos muestra la advertencia de que vamos a proceder a añadir un nuevo dispositivos. Haemos clic en *Iniciar sesión*



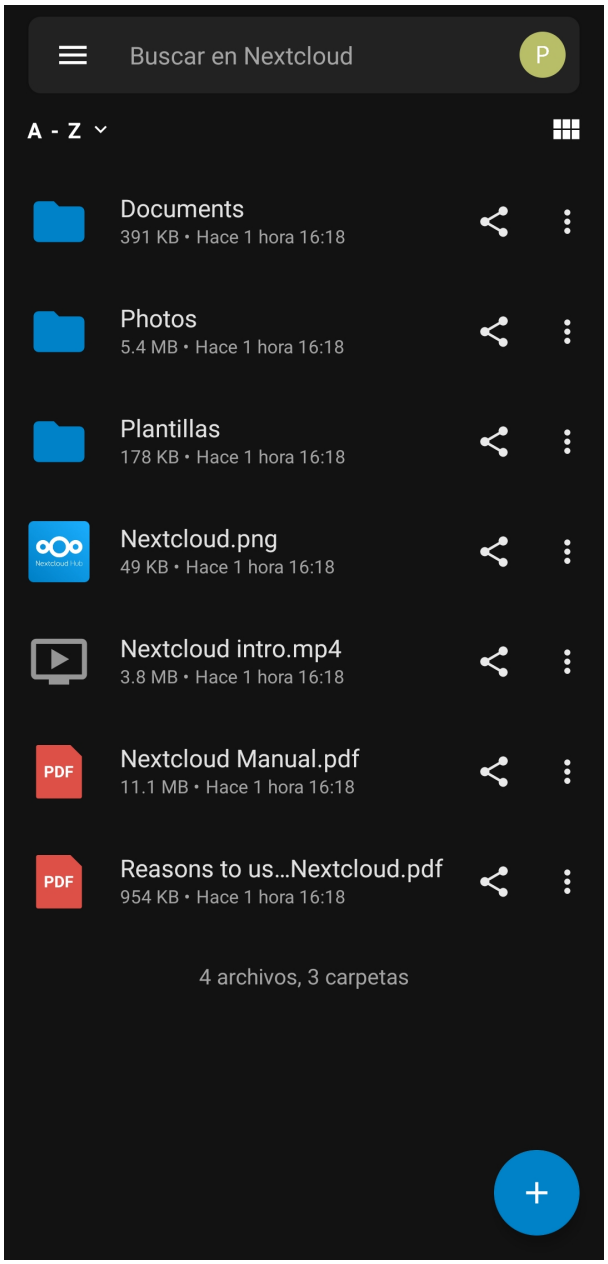
5. Completamos nuestros datos de inicio de sesión:



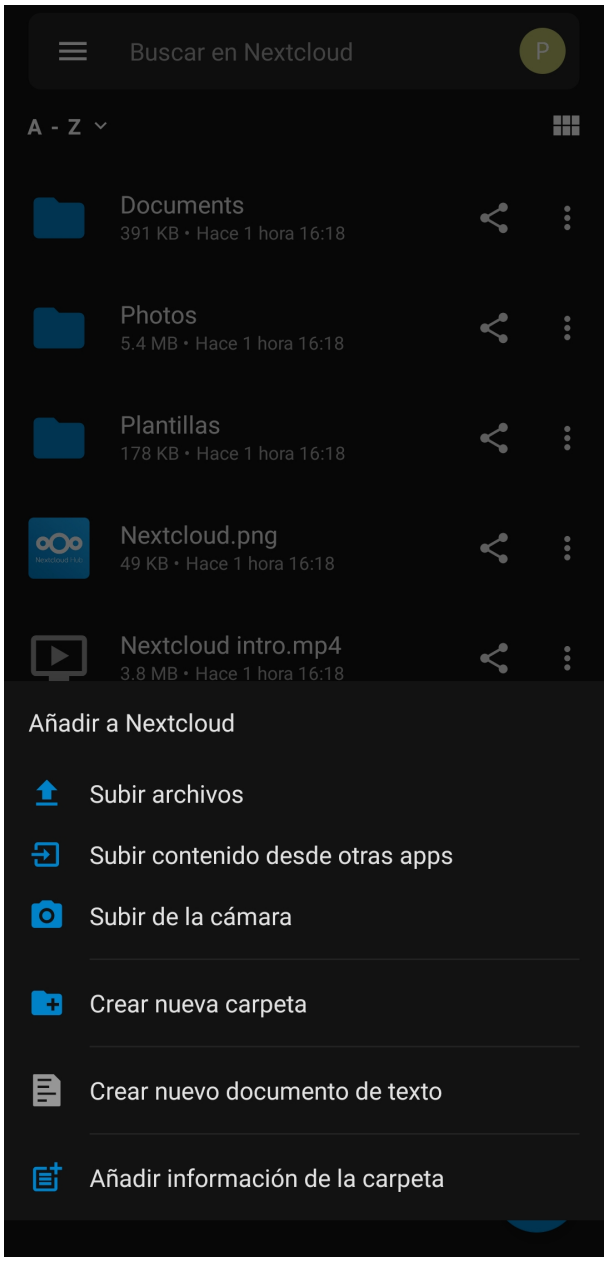
6. Debemos dar acceso a la aplicación a nuestra cuenta:



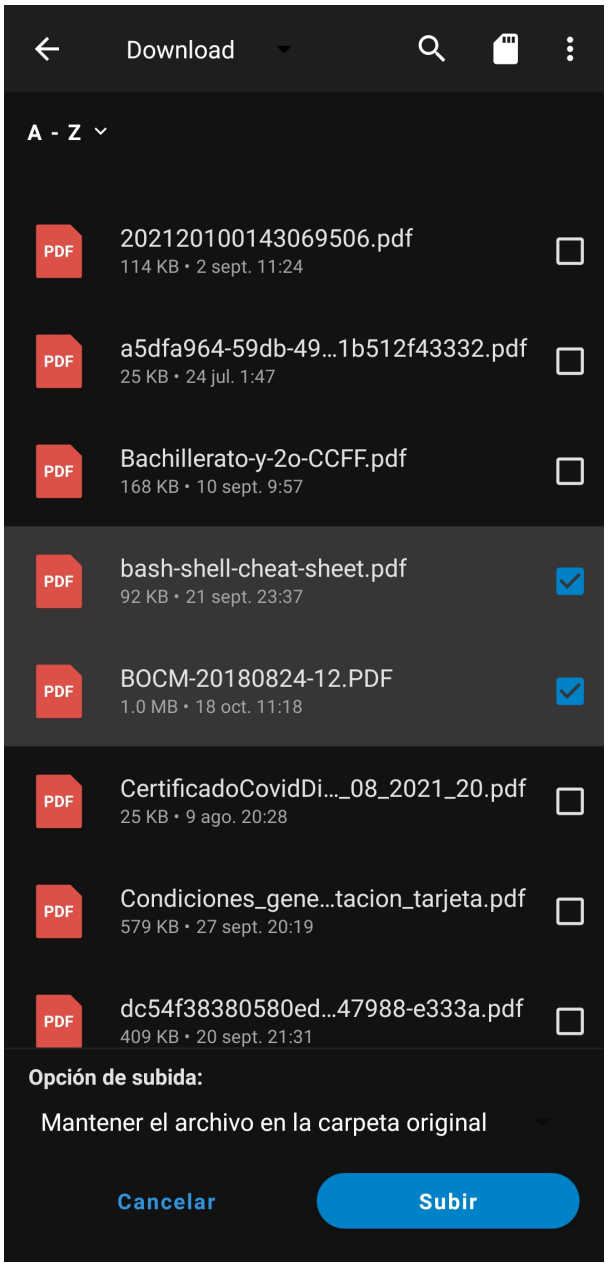
7. Veremos nuestros archivos:



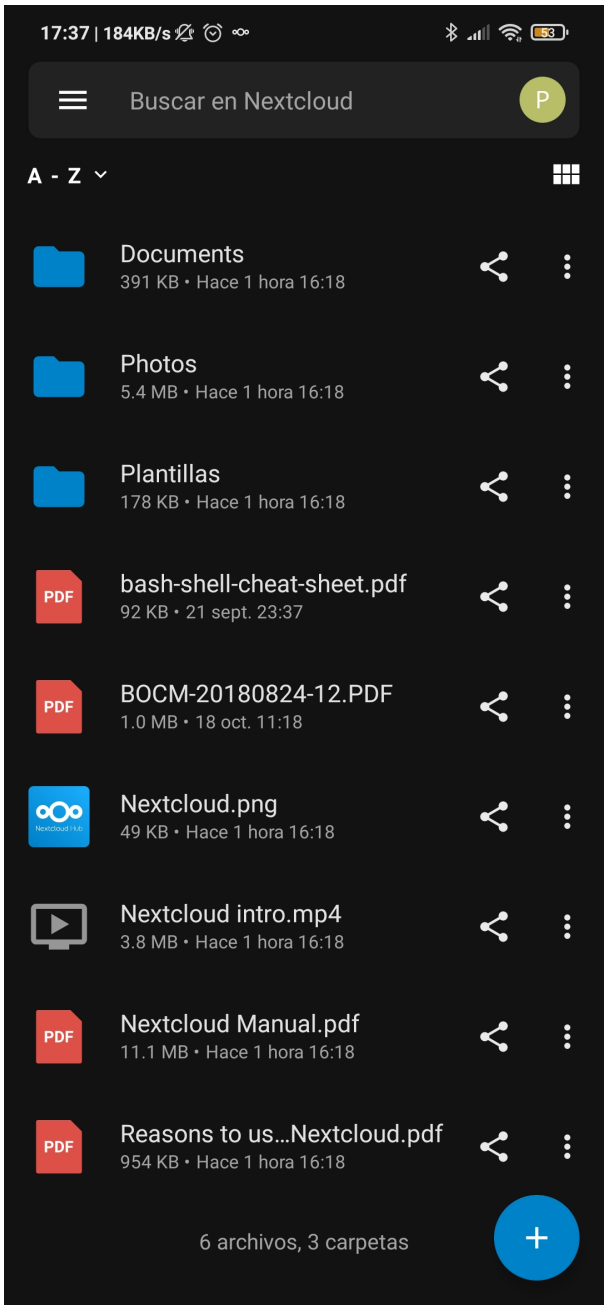
8. Si hacemos clic en el **+** de la esquina inferior derecha de la pantalla, se nos desplegarán las opciones para crear/subir archivos. Seleccionamos *Subir archivos*.



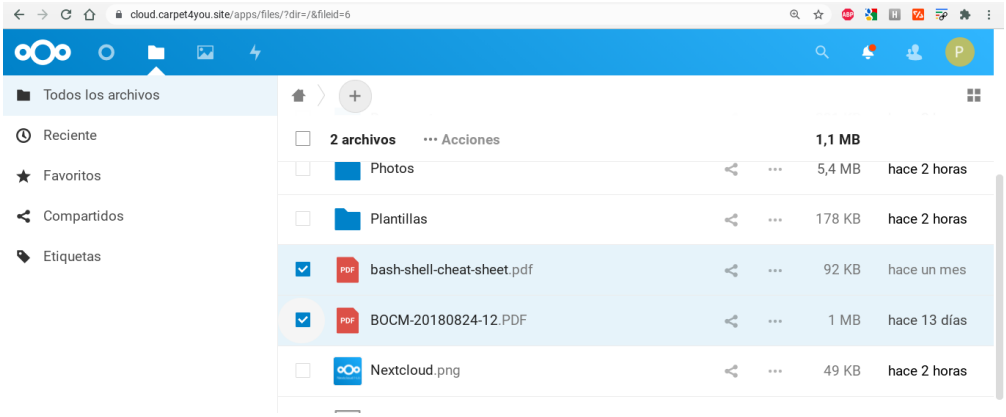
9. Navegamos en nuestro dispositivos hasta que localicemos los archivos que queremos subir y los seleccionamos. Hacemos clic en *Subir*:



10. Ya los podemos ver desde nuestra aplicación móvil:



11. Si ahora recargamos nuestro navegador web, veremos los archivos:



11.7 Instalar OnlyOffice en NextCloud

11.7.1 Instalación de servidor OnlyOffice

Nota: Vamos a instalar el servidor de OnlyOffice en Docker para la práctica nos es suficiente. No estamos en un entorno de producción.

Instalamos docker:

```
# Desinstalar versiones antiguas, si las hubiera
sudo apt remove docker docker-engine docker.io containerd runc

# Actualizar paquetes en los repos
sudo apt update

# Instalar dependencias
sudo apt install ca-certificates curl gnupg lsb-release

# Descargar clave GPG de Docker
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/
↪share/keyrings/docker-archive-keyring.gpg

# Añadir el repositorio de docker
echo \
"deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-archive-
↪keyring.gpg] https://download.docker.com/linux/ubuntu \
$(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null

# Instalar el motor Docker
sudo apt update
sudo apt install docker-ce docker-ce-cli containerd.io
```

Iniciar el contenedor docker:

```
sudo docker run -i -t -d -p 8443:443 \
    -v /app/onlyoffice/DocumentServer/logs:/var/log/onlyoffice  \
    -v /app/onlyoffice/DocumentServer/data:/var/www/onlyoffice/Data  \
    -v /app/onlyoffice/DocumentServer/lib:/var/lib/onlyoffice \
    -v /app/onlyoffice/DocumentServer/rabbitmq:/var/lib/rabbitmq \
    -v /app/onlyoffice/DocumentServer/redis:/var/lib/redis \
    -v /app/onlyoffice/DocumentServer/db:/var/lib/postgresql  onlyoffice/documentserver
```

Deberán descargarse y descomprimirse varios archivos, que juntos formarán la imagen del contenedor. Para ver si está funcionando usamos el comando:

```
sudo docker container list
```

Importante: Debemos utilizar como puerto externo (el primero de la combinación docker, 8443) del contenedor uno que no esté en uso por ningún otro proceso.

Alojar las rutas indicadas en nuestro propio sistema de archivos nos ayudará a «debuguear» problemas.

Más información sobre la imagen docker de Onlyoffice en este enlace

11.7.2 Generar certificados para el servidor

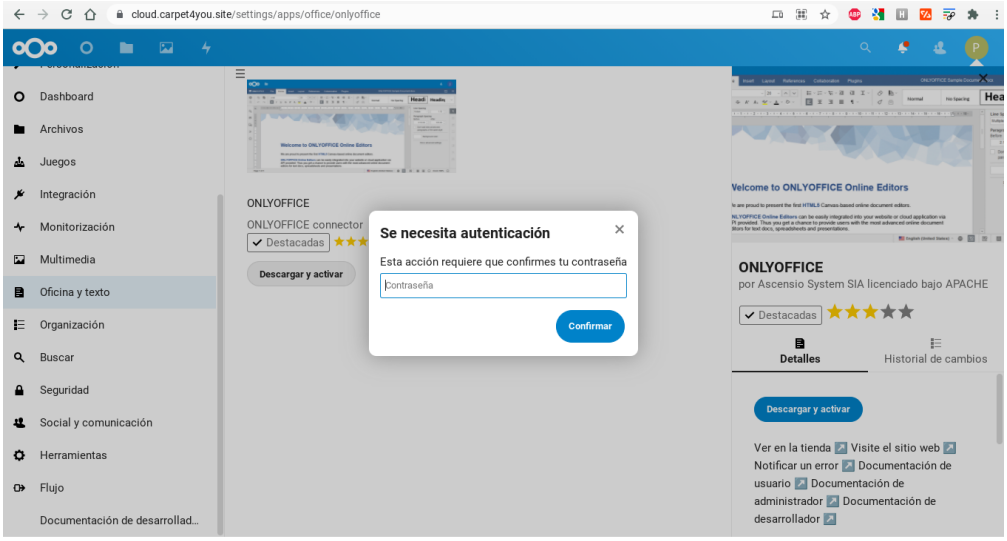
```
openssl genrsa -out tls.key 2048
openssl req -new -key tls.key -out tls.csr
openssl x509 -req -days 90 -in tls.csr -signkey tls.key -out tls.crt
openssl dhparam -out dhparam.pem 2048
mkdir -p /app/onlyoffice/DocumentServer/data/certs
cp tls.key /app/onlyoffice/DocumentServer/data/certs/
cp tls.crt /app/onlyoffice/DocumentServer/data/certs/
cp dhparam.pem /app/onlyoffice/DocumentServer/data/certs/
chmod 400 /app/onlyoffice/DocumentServer/data/certs/tls.key
```

11.7.3 Aplicación en NextCloud

Instalaremos la aplicación desde el *Marketplace* de Nextcloud

https://cloud.carpet4you.site/settings/apps/office/onlyoffice

Hacemos clic en *Descargar e Instalar*.

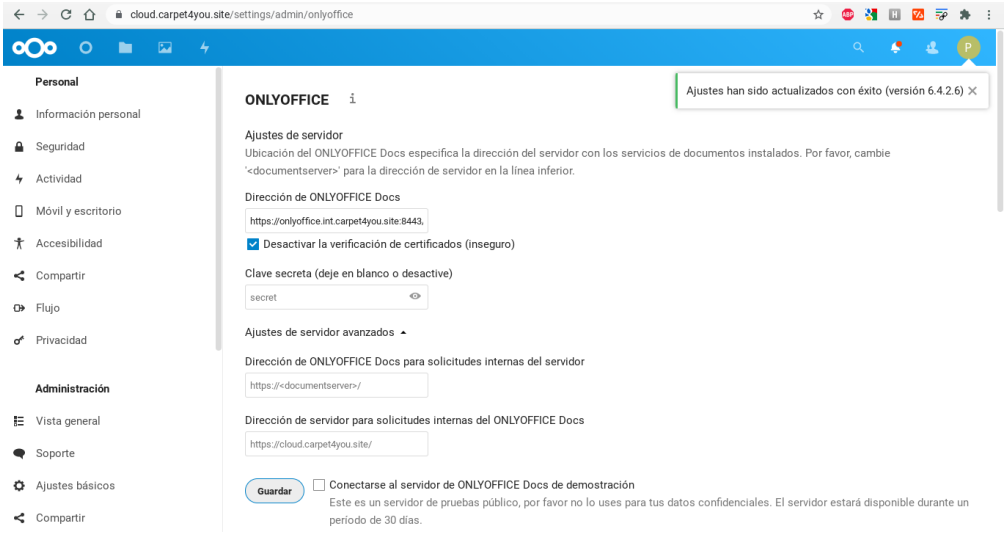


11.7.4 Conectar NextCloud con OnlyOffice

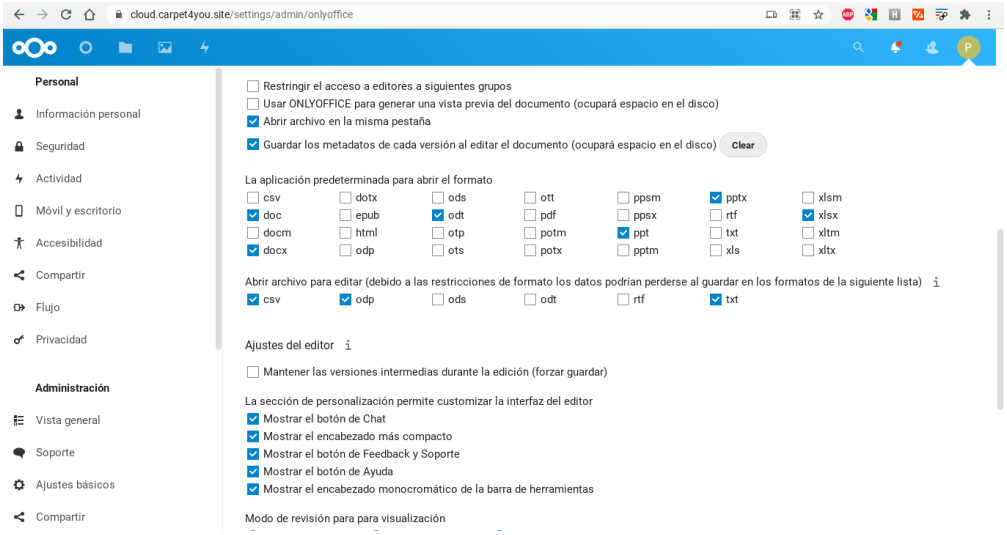
Navegamos hasta los ajustes (<URL_de_nuestro_nextcloud>/settings/admin/onlyoffice) y aquí introducimos la dirección de conexión de nuestro servidor Onlyoffice::

```
https://onlyoffice.int.carpet4you.site:8443/
```

Veremos un mensaje de confirmación, si todo ha ido bien:



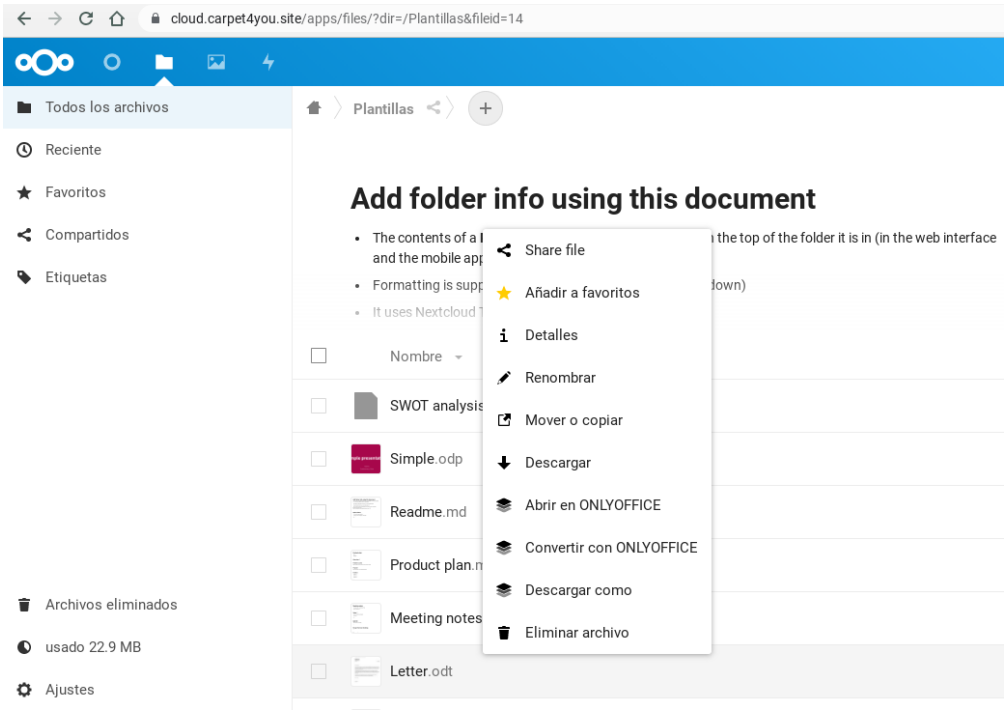
En la parte inferior podemos ver los ajustes de la aplicación:



11.8 Editar archivos con OnlyOffice

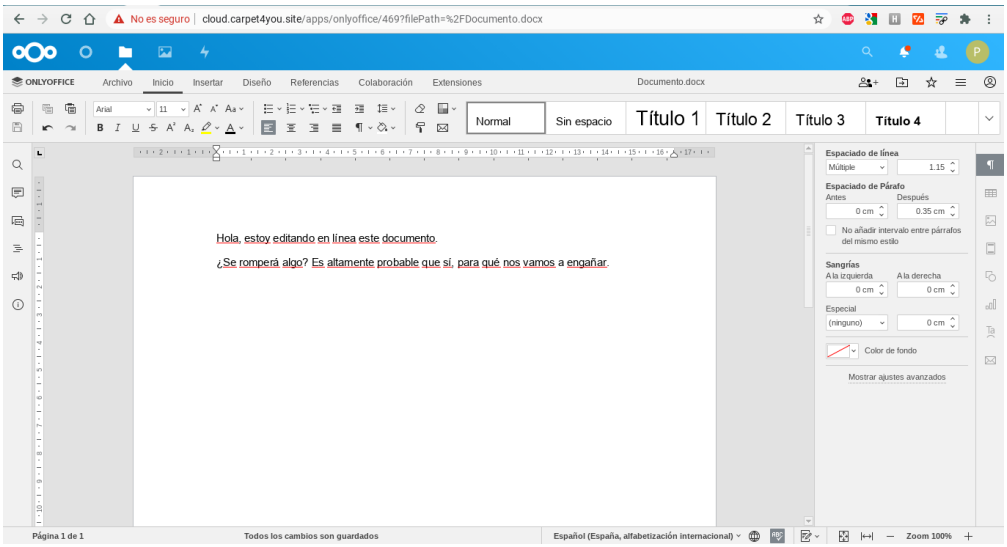
Una vez tenemos configuradas y conectadas las instancias de NextCloud y OnlyOffice, podemos editar archivos directamente desde la web, sin necesidad de instalar software adicional.

Para editar un archivo existente basta con abrir el menú contextual, haciendo clic derecho, de un archivo. Aquí veremos las opciones relativas a OnlyOffice:



También podemos crear un nuevo documento, utilizando el + de la esquina superior izquierda. Haciendo doble clic

sobre este lo abriremos:



Nota: Al estar trabajando con un certificado autofirmado aparece una advertencia.

11.1. *Instalación de Sistema Operativo*
11.2. *Instalación NextCloud*
11.3. *Securizar Nextcloud con SSL/TLS*
11.4. *Eliminar index.php de las URL*
11.5. *Creación de usuarios en NextCloud*
11.6. *Sincronización de datos cliente con NextCloud*
11.7. *Instalar OnlyOffice en NextCloud*
11.8. *Editar archivos con OnlyOffice*

CAPÍTULO 12

Sync & Backup

12.1 Sincronización entre la *home* y NextCloud

Nota: Los archivos se están copiando desde la carpeta home de los usuarios del equipo, no desde la home de OpenMediaVault. Para copiar/sincronizar estas carpetas sería suficiente con cambiar las rutas pertinentes

12.1.1 Estructura de archivos

En una instalación mediante paquetes APT, como es la nuestra, la carpeta por defecto donde se guardan los datos de los usuarios está localizada en la ruta `/var/www/nextcloud/data/`.

Dentro de este directorio, encontraremos una carpeta para cada usuario. Dentro de dicha carpeta, tendremos una carpeta, llamada `data` (junto con otras), donde se guardará los datos:

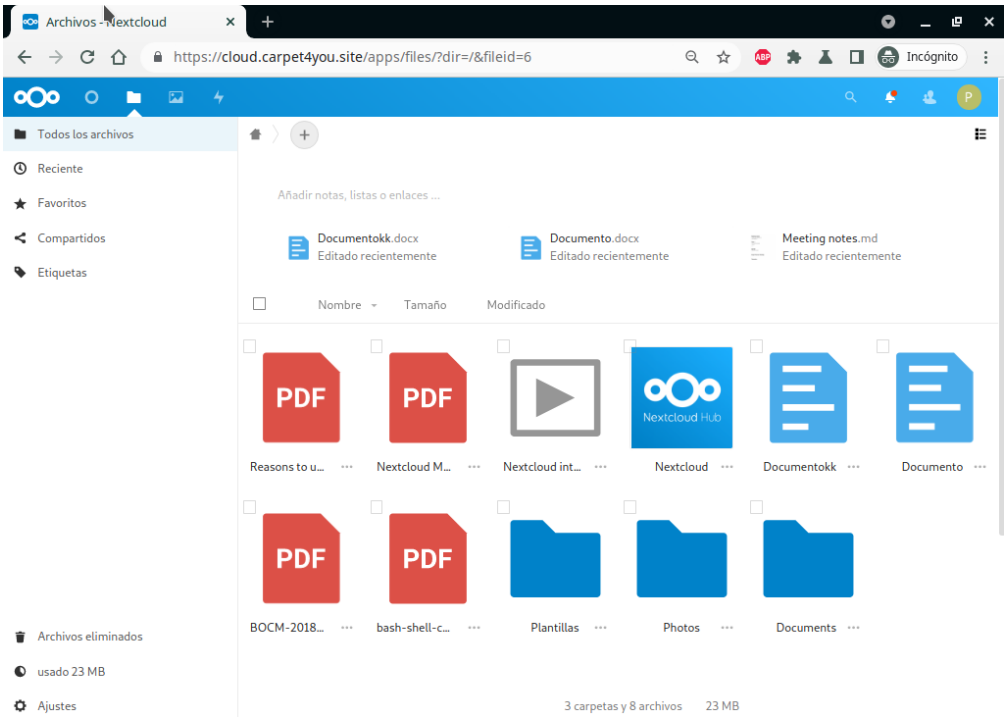
```
pablo@nextcloud-server:/var/www/nextcloud/data/pablo# tree -L 2
.
├── cache
├── files
│   ├── BOCM-20180824-12.PDF
│   ├── Documento.docx
│   ├── Documentokk.docx
│   ├── Documents
│   ├── Nextcloud Manual.pdf
│   ├── Nextcloud intro.mp4
│   ├── Nextcloud.png
│   ├── Photos
│   ├── Plantillas
│   ├── Reasons to use Nextcloud.pdf
│   └── bash-shell-cheat-sheet.pdf
```

(continué en la próxima página)

(proviene de la página anterior)

```
├── files_versions
│   └── Documento.docx.v1635706677
├── onlyoffice
│   └── 469
└── uploads
```

Como vemos, la estructura del directorio `files` es lo mismo que podemos ver desde la interfaz web.



Vamos a probar a crear una carpeta llamada `home` dentro del directorio de archivos del usuario.

Debemos cambiar los permisos y el propietario de los archivos:

```
pablo@nextcloud-server:/ chown www-data:www-data /var/www/nextcloud/data/pablo/files/home
pablo@nextcloud-server:/ chmod 755 /var/www/nextcloud/data/pablo/files/home
```

12.1.2 Copia con Rsync

Para copiar los archivos desde la *home* del usuario hacia la carpeta en NextCloud usaremos Rsync con las siguientes opciones:

```
rsync -au --exclude={.*} --chmod=755 --chown=www-data:www-data /home/pablo/ /var/www/
↪nextcloud/data/pablo/files/home/
```

Desglosemos las opciones:

- **-a**, la utilizamos para activar el formato archivo. Es una forma sencilla de aplicar recursividad y otras opciones que nos serán útiles.

- **-u**, esta opción fuerza al comando a omitir cualquier archivo que en el destino tenga una fecha de actualización posterior a la fecha en origen.
- **–exclude={.*}**, con esta opción excluimos los archivos y directorios que empiezan por `.`. Es decir, los que están ocultos.
- **–chmod=755**, estos son los permisos que se aplicarán a los archivos copiados en destino.
- **–chown=www-data:www-data**, los datos copiados serán propiedad del usuario que está ejecutando el servidor web, `www-data` en nuestro caso.
- **/home/pablo/**, es el directorio origen de los datos.
- **/var/www/nextcloud/data/pablo/files/home/**, es el directorio destino de los datos.

Ahora en el destino tenemos los datos:

```
pablo@nextcloud-server:/var/www/nextcloud/data/pablo/files# tree home/
home/
├── dhparam.pem
├── tls.crt
├── tls.csr
└── tls.key
```

12.1.3 Actualizar datos en NextCloud

Aunque físicamente estén los archivos en el directorio, NextCloud «no sabe» de su existencia, pues han sido añadidos por otro proceso. Debemos forzar un escaneo de los archivos.

Podemos hacerlo con el siguientes comando:

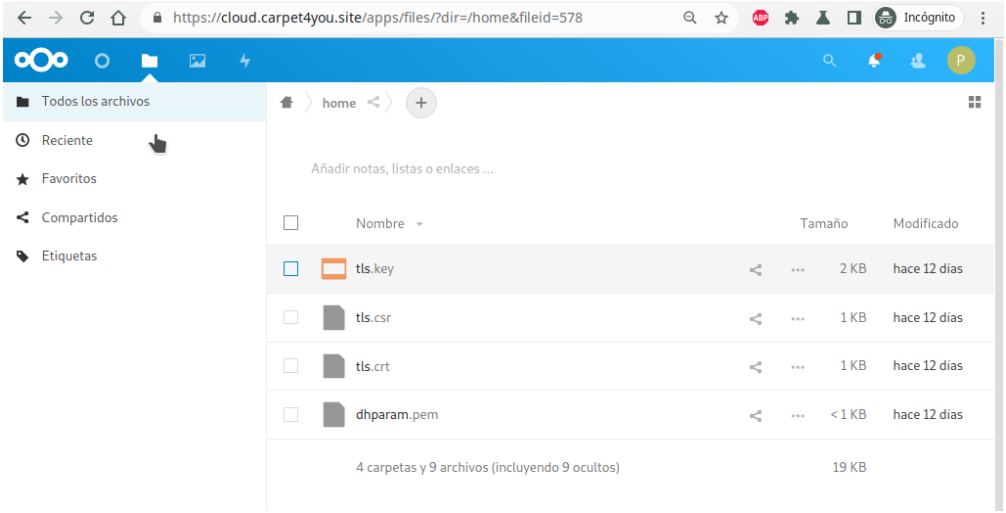
```
sudo -u www-data php ./occ files:scan --all
```

Importante: El usuario ejecutante del script php `occ` debe ser el del usuario web.

La salida del comando es la siguientes:

```
Starting scan for user 1 out of 2 (pablo)
   +---------+-------+--------------+
   | Folders | Files | Elapsed time |
   +---------+-------+--------------+
   | 18      | 49    | 00:00:00     |
   +---------+-------+--------------+
```

Si ahora accedemos desde la interfaz web veremos los archivos:



12.1.4 Sincronización en ambos sentidos

Con todo lo anterior hemos conseguido sincronizar los archivos que el usuario tenía en su home con la carpeta en NextCloud.

Para hacerlo en el otro sentido debemos modificatr ligeramente el comando anterior.

```
rsync -au --exclude={.*} --chmod=750 --chown=pablo:pablo /var/www/nextcloud/data/pablo/
↪files/home/ /home/pablo/
```

12.1.5 Automatización

Se crea un script, que será ejecutado de forma automática por el *cron*.

El script se alojará en /etc/sync.sh y tendrá el siguiente contenido:

```
inicio=$(date)

logger "Proceso de copia iniciado: $inicio"

rsync -au --exclude={.*} --chmod=755 --chown=www-data:www-data /home/pablo/ /var/www/
↪nextcloud/data/pablo/files/home/

rsync -au --exclude={.*} --chmod=750 --chown=pablo:pablo /var/www/nextcloud/data/pablo/
↪files/home/ /home/pablo/

sudo -u www-data php ./occ files:scan --all


final=$(date)

logger "Proceso de copia finalizado: $final"
```

Lo añadiremos al *cron daemon* utilizando el comando `crontab -e`.

```
0 * * * * /bin/sh /etc/sync.sh
```

Nota: El script solo funcionará para el usuario *pablo*. Para hacerlo universal habría que crear un bucle con los distintos usuarios a mantener sincronizados y sustituir en los comandos los nombres de usuario por las variables.

12.2 Copias de seguridad incrementales con tar

Nota: Para simplificar y universalizar la documentación no se utilizarán las rutas completas, sino las siguientes convenciones:

- `/home/pablo`, como carpeta de trabajo local del ususario *pablo*. Este valor cambiará según el usuario con el que se esté operando.
- `/mnt/raid1/incremental`, carpeta en el RAID 1 de OpenMediaVault donde se almacenarán las copias incrementales.
- `/mnt/raid1/diferencial`, carpeta en el RAID 1 de OpenMediaVault donde se almacenarán las copias diferenciales.

12.2.1 Primera copia

Importante: El nombre de la carpeta destino no es «BackupIncremental.», como se indica en la práctica, sino «incremental».

Para la creación de la copia completa del primer día de cada mes se utilizará el siguiente comando:

```
tar -cpvzf "/mnt/raid1/incremental/backupcompleto_`date +%d%m%Y`.tgz" /home/*
```

12.2.2 Copias incrementales

Para la creación de los siguientes backups incrementales se utilizará el siguiente comando:

```
# En la variable AYER guardamos el día de ayer.

AYER=`date -d "yesterday" '+%Y-%m-%d'`

tar -cpvzf "/mnt/raid1/incremental/backupincremental`date +%d%m%Y`.tgz" /home/* -N $AYER
```

12.2.3 Automatización del proceso de copia

Para que el primer día de mes se ejecute el backup incremental añadimos la siguiente entrada en el crontab:

```
0 3 1 * * "tar -cpvzf "/mnt/raid1/incremental/backupcompleto_`date +%d%m%Y`.tgz" /home/*"
```

Este comando se ejecutará el primer día del mes a las 3 de la mañana y creará una copia completa del contenido de /home/, guardándolo en `/mnt/raid1/incremental`, con el nombre `backupcompleto_` seguido del día de creación.

Para la copia de seguridad diaria, ejecutaremos un script, el siguiente:

```
# En la variable AYER guardamos el día de ayer.

AYER=`date -d "yesterday" '+%Y-%m-%d'`

tar -cpvzf "/mnt/raid1/incremental/backupincremental`date +%d%m%Y`.tgz" /home/* -N $AYER
```

Lo guardaremos como script en `/etc/incremental.sh` y añadiremos la siguiete línea a *crontab*, habiendo permitido que root lo ejecute:

```
0 4 * * * /bin/sh /etc/incremental.sh
```

12.3 Copias de seguridad difereciales con tar

Nota: Para simplificar y universalizar la documentación no se utilizarán las rutas completas, sino las siguientes convenciones:

- `/home/pablo`, como carpeta de trabajo local del ususario *pablo*. Este valor cambiará según el usuario con el que se esté operando.
- `/mnt/raid1/incremental`, carpeta en el RAID 1 de OpenMediaVault donde se almacenarán las copias incrementales.
- `/mnt/raid1/diferencial`, carpeta en el RAID 1 de OpenMediaVault donde se almacenarán las copias diferenciales.

Al iniciar la práctica, el estado de las carpeta *home* es el siguiente:

```
pablo@OpenMediaVault:/home/pablo# ll
total 20
drwxr-xr-x 2 pablo pablo  4096 Nov 13 16:57 ./
drwxr-xr-x 5 root  root  4096 Nov 13 16:55 ../
-rw-r--r-- 1 pablo pablo   27 Nov 13 16:57 arch1
-rw-r--r-- 1 pablo pablo   39 Nov 13 16:57 arch2
-rw-r--r-- 1 pablo pablo   50 Nov 13 16:57 arch3
```

12.3.1 Copia completa

Importante: El nombre de la carpeta destino no es «BackupDiferencial», como se indica en la práctica, sino «diferencial».

Para la creación de la copia completa del primer día de cada mes se utilizará el siguiente comando:

```
tar -cpvzf "/mnt/raid1/diferencial/backupcompleto_`date +%d%m%Y`.tgz" /home/*
```

12.3.2 Copias diferenciales

Para la creación de los siguientes backups diferenciales se utilizará el siguiente comando:

```
tar -cpvzf "/mnt/raid1/diferencial/backupdiferencial`date +%d%m%Y`.tgz" /home/* -N 13-
↪nov-2021
```

12.3.3 Automatización del proceso de copia

Para que el primer día de mes se ejecute el backup diferencial añadimos la siguiente entrada en el crontab:

```
0 3 1 * * "tar -cpvzf "/mnt/raid1/diferencial/backupcompleto_`date +%d%m%Y`.tgz" /home/*"
```

Este comando se ejecutará el primer día del mes a las 3 de la mañana y creará una copia completa del contenido de /home/, guardándolo en `/mnt/raid1/diferencial`, con el nombre `backupcompleto_` seguido del día de creación.

Para la copia de seguridad diaria, ejecutaremos un script, el siguiente:

```
# La siguiente instrucción guarda en la variable "TARCOMPLETO" la salida de los comandos␣
↪siguientes.
#   1. Para empezar, listamos el contenido de la carpeta destino.
#       Pero no lo listamos de cualquier manera, sino que lo hacemos en forma de lista (-
↪l)
#       y ordenado por fecha de modificación (-t). Además, solo sacará los archivos de␣
↪backup completo.
#   2. Con "head -1" nos quedamos solo con la primera línea de la salida.
#       Esta primera línea coincide con el último archivo modificado.
#   3. Después, cortaremos (awk) para quedarnos con la ruta al archivo.

TARCOMPLETO=`ls -lt  /mnt/raid1/diferencial/backupcompleto* | head -1 | grep␣
↪backupcompleto_ | awk '{printf $NF}'`

    # Podemos comprobar con "echo $TARCOMPLETO"

# Con el siguiente comando obtenemos la fecha de modificación del archivo anterior.
FECHA=`date -r "$TARCOMPLETO" "+%F %H:%M"`

    # Podemos comprobar con "echo $FECHA"

# Una vez ya tenemos almacenada en FECHA el punto desde el cual tenemos que hacer la␣
↪siguiente copia diferencial, ejecutamos el comando TAR:
```

(continué en la próxima página)

(proviene de la página anterior)

```
tar -cpvzf "/mnt/raid1/diferencial/backupdiferencial`date +%d%m%Y`.tgz" /home/* -N "
↪$FECHA"

    # El comando anterior creará dentro de la carpeta de copias diferenciales un nuevo␣
↪archivo con todo el contenido
    # de los directorios *home* de trabajo modificado desde la fecha del útimo completo.
```

Todo esto lo guardaremos como script en `/etc/diferencial.sh` y añadiremos la siguiete línea a *crontab*:

```
0 4 * * * /bin/sh /etc/diferencial.sh
```

12.4 Sincronizar carpetas de *backup* y NextCloud

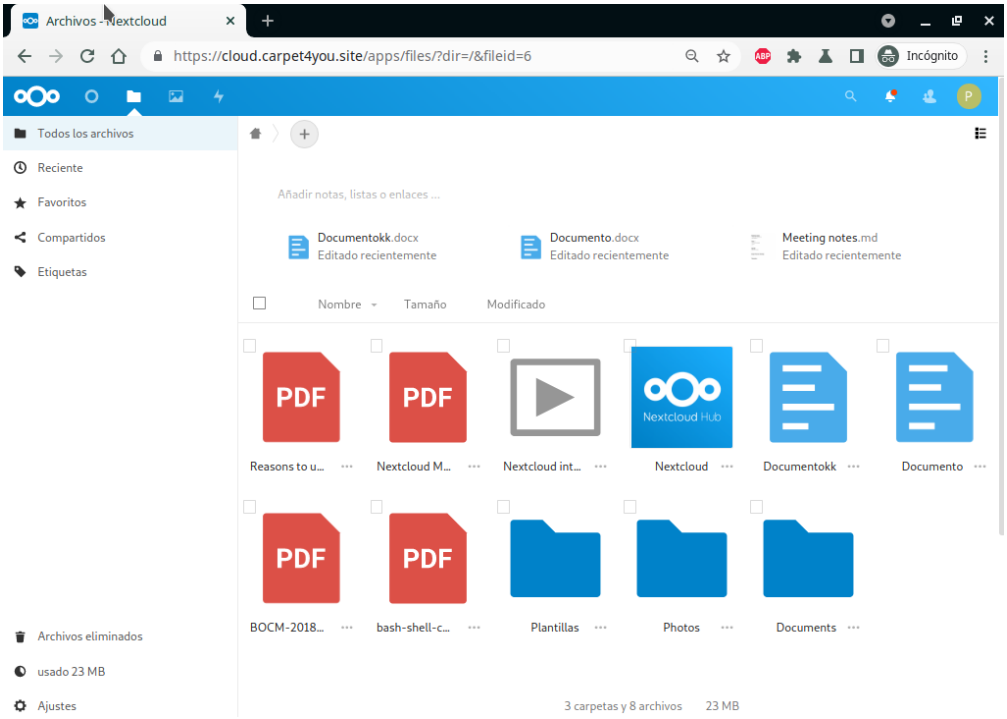
12.4.1 Estructura de archivos

En una instalación mediante paquetes APT, como es la nuestra, la carpeta por defecto donde se guardan los datos de los usuarios está localizada en la ruta `/var/www/nextcloud/data/`.

Dentro de este directorio, encontraremos una carpeta para cada usuario. Dentro de dicha carpeta, tendremos una carpeta, llamada `data` (junto con otras), donde se guardará los datos:

```
pablo@nextcloud-server:/var/www/nextcloud/data/pablo# tree -L 2
.
├── cache
├── files
│   ├── BOCM-20180824-12.PDF
│   ├── Documento.docx
│   ├── Documentokk.docx
│   ├── Documents
│   ├── Nextcloud Manual.pdf
│   ├── Nextcloud intro.mp4
│   ├── Nextcloud.png
│   ├── Photos
│   ├── Plantillas
│   ├── Reasons to use Nextcloud.pdf
│   └── bash-shell-cheat-sheet.pdf
├── files_versions
│   └── Documento.docx.v1635706677
├── onlyoffice
│   └── 469
└── uploads
```

Como vemos, la estructura del directorio `files` es lo mismo que podemos ver desde la interfaz web.



Vamos a probar a crear una carpeta llamada `backups` dentro del directorio de archivos del usuario.

Debemos cambiar los permisos y el propietario de los archivos:

```
pablo@nextcloud-server:/ chown www-data:www-data /var/www/nextcloud/data/pablo/files/
↪backups
pablo@nextcloud-server:/ chmod 755 /var/www/nextcloud/data/pablo/files/backups
```

12.4.2 Copia con Rsync

Para copiar los archivos desde la *home* del usuario hacia la carpeta en NextCloud usaremos Rsync con las siguientes opciones:

```
rsync -au --chmod=755 --chown=www-data:www-data /mnt/raid1/diferencial /var/www/
↪nextcloud/data/pablo/files/backups/

rsync -au --chmod=755 --chown=www-data:www-data /mnt/raid1/incremental /var/www/
↪nextcloud/data/pablo/files/backups/
```

Desglosemos las opciones:

- **-a**, la utilizamos para activar el formato archivo. Es una forma sencilla de aplicar recursividad y otras opciones que nos serán útiles.
- **-u**, esta opción fuerza al comando a omitir cualquier archivo que en el destino tenga una fecha de actualización posterior a la fecha en origen.
- **–chmod=755**, estos son los permisos que se aplicarán a los archivos copiados en destino.
- **–chown=www-data:www-data**, los datos copiados serán propiedad del usuario que está ejecutando el servidor web, `www-data` en nuestro caso.

- **/mnt/raid1/diferencial**, es el directorio origen de los datos.
- **/var/www/nextcloud/data/pablo/files/backups/**, es el directorio destino de los datos.

12.4.3 Actualizar datos en NextCloud

Aunque físicamente estén los archivos en el directorio, NextCloud «no sabe» de su existencia, pues han sido añadidos por otro proceso. Debemos forzar un escaneo de los archivos.

Podemos hacerlo con el siguientes comando:

```
sudo -u www-data php ./occ files:scan --all
```

Importante: El usuario ejecutante del script php `occ` debe ser el del usuario web.

12.4.4 Automatización

Se crea un script, que será ejecutado de forma automática por el *cron*.

El script se alojará en /etc/sync-backup.sh y tendrá el siguiente contenido:

```
inicio=$(date)

logger "Proceso de copia iniciado: $inicio"

rsync -au --chmod=755 --chown=www-data:www-data /mnt/raid1/diferencial /var/www/
↪nextcloud/data/pablo/files/backups/

rsync -au --chmod=755 --chown=www-data:www-data /mnt/raid1/incremental /var/www/
↪nextcloud/data/pablo/files/backups/

sudo -u www-data php ./occ files:scan --all

final=$(date)

logger "Proceso de copia finalizado: $final"
```

Nota: El proceso solo se realizará en un sentido, pues no son archivos que se deban modificar via web.

Lo añadiremos al *cron daemon* utilizando el comando `crontab -e`.

```
0 * * * * /bin/sh /etc/sync-backup.sh
```

12.1. *Servicio Rsync*
12.2. *Servicio Rsync automatizado*
12.3. *Sincronización entre la home y NextCloud*
12.4. *Copias de seguridad incrementales con tar*
12.5. *Copias de seguridad difereciales con tar*
12.6. *Sincronizar carpetas de backup y NextCloud*