



Dispositivos de almacenamiento y copias de seguridad

Objetivos

- Conocer los diferentes tipos de almacenamiento de datos, tanto locales como remotos, y la contratación en la nube.
- Analizar los riesgos e impactos de una incorrecta planificación en las copias de seguridad.
- Aprender las políticas de seguridad en el plan de continuidad del negocio y el plan de recuperación ante desastres con referencia a las copias de seguridad.
- Saber determinar qué se debe salvaguardar y cómo.
- Dominar los medios actuales para las copias de seguridad.
- Explotar las diferentes arquitecturas en el almacenamiento conectado en red.

Contenidos

- 3.1. Almacenamiento de la información
- 3.2. Copias de seguridad
- 3.3. Medios para las copias de seguridad
- 3.4. Protección, imágenes del sistema y puntos de restauración
- 3.5. Copias de seguridad en Linux
- 3.6. Seguridad en almacenamiento conectado en red

Introducción

La seguridad pasiva pretende minimizar el impacto de las amenazas en un sistema a través de medidas relativas a los sistemas de alimentación ininterrumpida, a las fuentes de alimentación redundante, al control de acceso físico, a los sistemas de videovigilancia, a la ubicación correcta de los sistemas, a los centros de respaldo, a los sistemas de control de temperatura y humedad, a los sistemas contra incendios, etcétera.

El respaldo físico es muy importante, ya que minimiza el impacto ocasionado por las amenazas, pero está muy alejado en importancia si se enfrenta al respaldo de la información. La recuperación de datos, su conservación y su eliminación, según políticas de seguridad, son operaciones fundamentales, y su planificación y desarrollo son de gran importancia para cualquier organización.

En esta unidad se profundiza en diferentes metodologías para el mantenimiento de los datos y la recuperación de los mismos. Se estudian los diferentes soportes de almacenamiento masivo, así como las tecnologías emergentes en el almacenamiento no local, en la nube o en servidores remotos.

Se analiza cómo afecta la planificación de las copias de seguridad en el plan de continuidad de negocio y en el plan de recuperación ante desastres. Se profundiza en las diferentes metodologías para las copias de seguridad y se presentan herramientas que facilitan su gestión tanto en sistemas operativos propietarios como libres. Por último, se estudian los sistemas de almacenamiento remoto (DAS, NAS y SAN) y se usan herramientas para su explotación.

■ 3.1. Almacenamiento de la información

Atendiendo a la función que desempeña la información, esta se puede clasificar en información operativa, aquella relacionada con los sistemas transaccionales, en información táctica, aquella relacionada con los sistemas de gestión y administración, y en información estratégica, la que está relacionada con los sistemas de soporte a la decisión.

Los sistemas de información ayudan a administrar, recolectar, recuperar, procesar, almacenar, distribuir, comparar y analizar información en diferentes procesos de cualquier tipo de organización y, por tanto, los sistemas de información se convierten en ese conjunto de tecnologías, procesos, aplicaciones de negocios y software que permiten transformar los datos en información y, esta, en conocimiento.

A través de programas informáticos, las personas manejan información (*information processing*) que puede ser muy sensible, información crítica que, de verse comprometida, destruida o divulgada, puede acarrear problemas muy graves en el propio funcionamiento de la organización. Por ello, la gestión de la seguridad de la información es una tarea no solo imprescindible, sino obligatoria y por ley. Se hace, pues, necesario establecer procedimientos, planes y políticas de almacenamiento, conservación, recuperación y eliminación de la información. Los pasos fundamentales para llevar estos planes con seguridad son:

- Clasificar la información.
- Garantizar un almacenamiento adecuado.
- Establecer claras técnicas de recuperación y asegurar la continuidad de la información almacenada.
- Instaurar políticas de borrado seguro sobre información no útil para la organización.
- Implementar métodos para la conservación de la información en caso de que por ley se tenga que hacer.



Figura 3.1. Para la ayuda del procesamiento de la información, las tecnologías de la información ofrecen soportes para el almacenamiento, la recuperación, la transmisión y la manipulación de los datos.

■ ■ ■ 3.1.1. Seguridad y almacenamiento de la información

La seguridad de la información se define como la preservación de la confidencialidad, la integridad y la disponibilidad de esta. No debe ser confundida con la seguridad informática, ya que esta se encarga de la seguridad atendiendo al medio, ya que la información puede encontrarse en diferentes formas.

Por tanto, a la hora de garantizar que la información es segura, se deben considerar estas tres dimensiones: el grado de confidencialidad, la integridad y el nivel de disponibilidad.



Figura 3.2. La confidencialidad, la integridad y la disponibilidad son los pilares para garantizar que la información es segura.

- **Confidencialidad (confidentiality):** la información no debe estar a disposición de usuarios, entidades o procesos no autorizados ni debe revelarse a estos.
- **Integridad (integrity):** la información debe conservar su exactitud y completitud.
- **Disponibilidad (availability):** la información debe estar accesible y utilizable siempre que haya autorización para ello.

Se hace necesario contar con sistemas de almacenamiento flexibles que protejan y resguarden la información y se adapten a los rápidos cambios en su manejo, en sus procesos de gestión y en sus modelos de tratamiento. Los principales sistemas de almacenamiento de información son: almacenamiento local, servidores de almacenamiento en red, dispositivos externos, sistemas de copias de seguridad y servicios de almacenamiento en la nube.

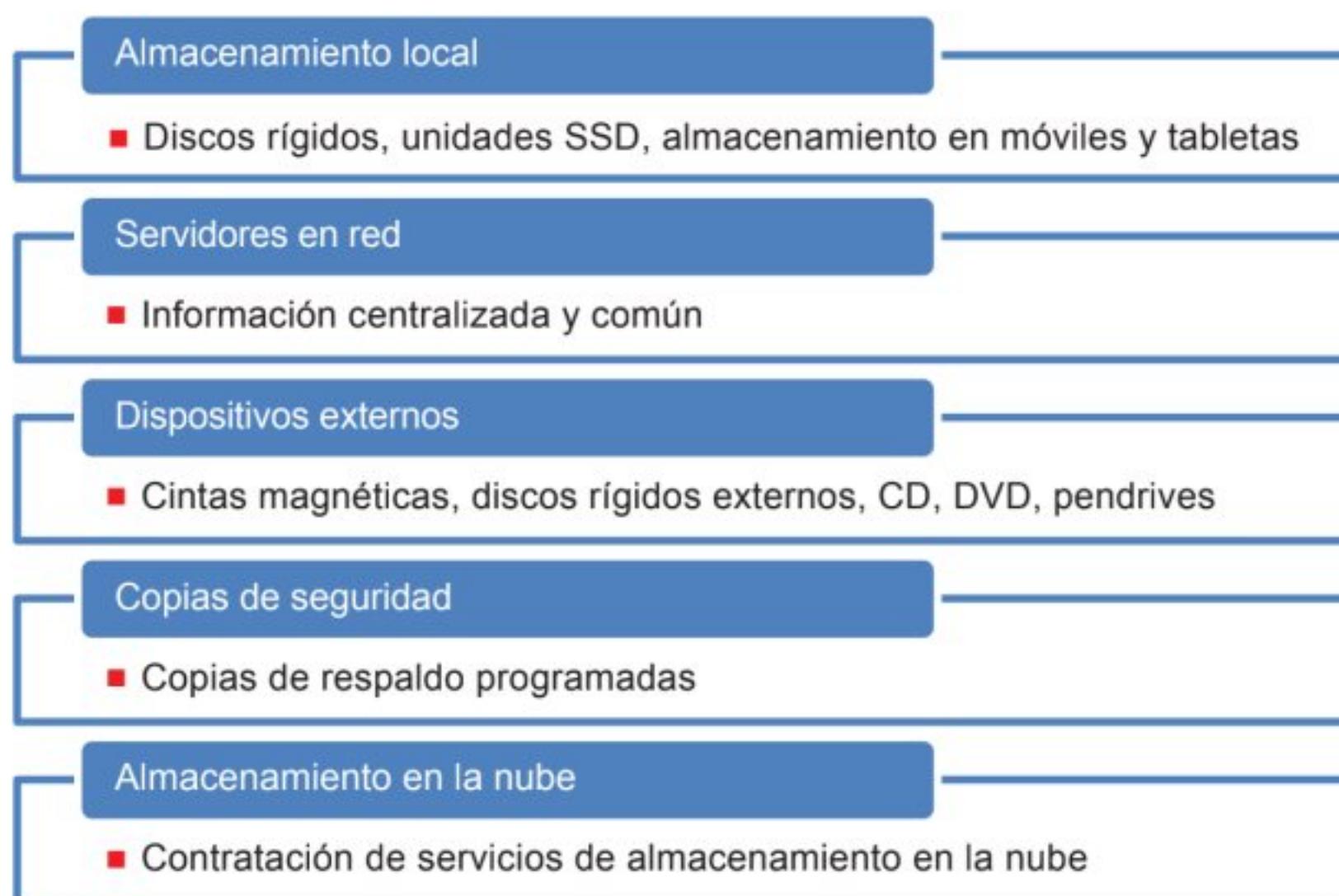


Figura 3.3. Principales sistemas de almacenamiento de la información.

A continuación, se describe cada uno de ellos:

- **Almacenamiento local:** información que generan los equipos locales en las fases de procesamiento de la misma, donde, en la mayoría de los casos, se obtiene información nueva. Esta nueva está pendiente de almacenar, y se graba en la memoria secundaria del equipo que la procesa. El almacenamiento local está en cada uno de estos equipos de procesado, normalmente en discos rígidos o en unidades SSD. El almacenamiento usado en tabletas y dispositivos móviles también constituye almacenamiento local.
- **Servidores de almacenamiento en red:** centralizan la información y proveen de un repositorio común para todos los usuarios de la red con privilegios suficientes para su acceso.
- **Dispositivos externos:** de forma adicional, con conexión directa a los equipos, se pueden añadir sistemas de almacenamiento extra. Pueden ser cintas magnéticas, discos rígidos externos, CD, DVD o pendrives.
- **Sistema de copias de seguridad:** procedimientos para sistematizar la realización de copias de respaldo de la información vital de la organización, ya sea en soportes externos o en otra ubicación.
- **Servicios de almacenamiento en la nube:** la contratación de servicios de almacenamiento en la nube como medio de almacenamiento externo está en expansión, no solo para el copiado de la información, sino para otros servicios añadidos, como las copias de seguridad, alojamiento web, tiendas online, etcétera.

■ ■ ■ 3.1.2. Tipos de soporte de almacenamiento de datos

El **soporte o medio de almacenamiento** es el material físico donde se almacenan los datos, y es diverso en sus componentes de hardware, materiales y sus propiedades magnéticas, ópticas y eléctricas. Se hace referencia al dispositivo de almacenamiento de datos o unidad de almacenamiento al aparato que opera con los datos almacenados en los soportes. Los soportes de almacenamiento más usados son los magnéticos (cinta magnética y disco magnético), los ópticos (disco láser, disco compacto, disco versátil digital y disco Blu-ray), los magneto-ópticos (disco zip, disco jaz, minidisc y superdisk) y los de estado sólido (memoria USB, tarjeta de memoria y disco de estado sólido). En la Figura 3.4, se detallan las características de los dispositivos de almacenamiento de datos usados en la actualidad:



Figura 3.4. Diferentes tipos de soporte que permiten almacenar la información de forma masiva.

- **Discos rígidos:** ya sean discos magnéticos (HDD) o dispositivos de estado sólido (Solid-State Drive-SSD), son los más usados en el almacenamiento local de los equipos. Los primeros, de mayor capacidad y más económicos, son magnéticos y llevan piezas mecánicas, por lo que se requiere de ciertos cuidados: evitar campos magnéticos cercanos, movimientos bruscos cuando están encendidos, etc. Los segundos son electrónicos, más rápidos y silenciosos, de menor capacidad y más caros. También se utilizan como medios externos a través de conectores USB, eSATA, Firewire o Thunderbolt, incluso conexiones inalámbricas.
- **Cintas magnéticas:** se utilizan principalmente en los procesos de copias de seguridad, ya que son más económicos que otros medios y permiten almacenar grandes cantidades de datos. El acceso a los datos es más lento que el de los discos duros. Los formatos más conocidos son Digital Audio Tape (DAT), Digital Data Storage (DDS), Digital Linear Tape (DLT) y Líneas Tape-Open (LTO), cada uno con diferentes ventajas y facilidades de uso.

- **Discos ópticos:** aunque los discos ópticos cada vez están más en desuso por su inferior durabilidad con respecto a otros medios, siguen siendo útiles en diferentes soluciones. Ejemplos de estos discos son los discos compactos, Compact Disc (CD), los discos versátiles digitales, Digital Versatile Disc (DVD) y los discos de láser azul, Blu-ray Disc (BD), en sus diferentes versiones de escritura y lectura. Son económicos y fáciles de transportar, apilar y conservar, y son idóneos en copias de seguridad anti-ransomware (no podrán ser secuestrados por malware que pida rescate para su recuperación).
- **Discos magneto-ópticos:** combinan tecnología magnética y óptica. Entre los más conocidos se encuentran los discos zip, jaz, minidisc y superdisk.
- **Sistemas de almacenamiento en red:** estos sistemas, en auge en la actualidad, permiten mayor volumen de almacenamiento y otorgan una serie de ventajas que hacen que su explotación sea muy adecuada en sistemas que requieren de tasas altas de transferencia de datos y capacidades muy elevadas para el almacenamiento. Existen soluciones DAS (Direct Attached Storage), que son las más fáciles de implantar, NAS (Network Attached Storage), que proveen de innumerables ventajas a pesar de su cómoda implantación, y soluciones SAN (Storage Area Network), que son más costosas y complejas, pero resultan ser las mejores implantaciones en el almacenamiento masivo de información y su respaldo.
- **Memoria flash:** usan memorias de tipo EEPROM (Electrically Erasable Programmable Read Only Memory) que están basadas en transistores FAMOS (Floating Gate Avalanche-Injection Metal Oxide Semiconductor), es decir, unos transmisores con conductores basados en un óxido metálico. Es una tecnología usada en memorias tipo USB, tarjetas de memoria y en unidades de estado sólido (SSD). Ejemplos de tarjetas son Secure Digital (SD), MultiMediaCard (MMC), Memory Stick (MS), CompactFlash (CF), MicroDrive (MD) y SmartMedia (SM). Este tipo de memoria para copias de seguridad resulta muy caro, pero, conforme se vaya abaratando, será una solución muy adecuada, ya que es más veloz y de menor tamaño que el resto de medios de almacenamiento masivo.

■ ■ ■ 3.1.3. Control de acceso a los sistemas de almacenamiento de datos

Se hace necesario establecer políticas para la explotación de los sistemas de almacenamiento. Estas deben estar encaminadas principalmente a la protección máxima de la información que almacena. En general, los objetivos que se persiguen son:

- Evitar la pérdida o robo de la información.
- Controlar la difusión indebida de información confidencial y la destrucción, manipulación o difusión no autorizada.
- Evitar la divulgación o destrucción de información de carácter personal, credenciales de acceso o cualquier otro tipo de información sensible.
- Vigilar la intrusión.
- Fiscalizar los datos compartidos en la nube para evitar su manipulación, destrucción o divulgación malintencionada, etcétera.

En general, se deben establecer reglas de uso que contemplen las siguientes premisas base:

- Implementar un procedimiento que controle la retirada de soportes y equipos que han dejado de usarse, ya que contienen información que se debe borrar o destruir con el fin de evitar su divulgación y lo que ello conlleve, como daños de imagen, consecuencias legales, etcétera.
- Establecer políticas en el control de acceso, que determinen, para cada usuario, qué puede hacer y a qué puede acceder en cuanto a las aplicaciones que se usan y a las propias operaciones de acceso a los datos albergados en los sistemas de almacenamiento.
- Cifrar la información en soportes de almacenamiento masivos, en copias de seguridad, en clonaciones, etcétera.

■ 3.2. Copias de seguridad

Una **copia de seguridad**, **copia de respaldo** o, en inglés, **backup**, se puede definir como aquel proceso mediante el cual la información se duplica desde un lugar de almacenamiento a otro, con el objetivo de recuperarla y restaurarla en caso de no disponer de ella ante fallos. Se hace uso de ella cuando el original está inutilizado o corrupto. Una clasificación general sobre las copias de seguridad se muestra en la Tabla 3.1.

Tabla 3.1. Clasificación general sobre las copias de seguridad

Copias de recuperación	Sirven para disponer de una copia que subsane la potencial pérdida de datos valiosos.
Copias operacionales	Se hacen para disponer de una instantánea de los datos del sistema en un momento determinado, con el fin de regresar a esa situación anterior si se necesita.
Copias reguladas	Se realizan para cumplir con normativas que exigen el almacenado de datos históricos durante un periodo de tiempo.

■ ■ 3.2.1. Planificación de las copias de seguridad

En cualquier organización, la información es un activo importante que cuidar, no solo para garantizar la confiabilidad de aquellos a los que se les provee de algún servicio a través del sistema de información que se tiene en mano, sino también por la propia responsabilidad de la naturaleza de los datos, sensibles para los propietarios y para aquellos que disponen de dichos datos. Para asegurar los sistemas de información, la organización responsable del sistema deberá contar con un plan de dirección de seguridad, así como un plan de contingencia y continuidad de negocio, en los que las copias de seguridad serán parte fundamental.



Figura 3.5. El plan de continuidad de negocio (*Business Continuity Plan*) es un plan logístico para recuperar y restaurar las funciones críticas interrumpidas por un desastre. El plan de restauración de copias de seguridad en caso de fallos sigue el mismo esquema de desarrollo.

El **plan director de seguridad** señala las prioridades y los recursos para aumentar los niveles de seguridad, así como los responsables de los mismos. Contempla la política de copias de seguridad que se debe aplicar en la organización. El **plan de contingencia y continuidad de negocio** indicará las pautas para actuar rápida y eficazmente ante un incidente de seguridad, con el fin de restablecer la actividad del sistema lo antes posible, reduciendo al máximo el impacto ocasionado.

Ante la posibilidad de pérdida de la información, el plan de contingencia establecerá qué tipo de información debe incluirse en las copias de seguridad, el soporte en el que se almacenará, la ubicación en dichos soportes, cada cuánto tiempo se realizará y en qué lugar físico se encontrarán los diferentes sistemas de almacenamiento masivo. Además, y con igual importancia, se hará necesario establecer pruebas para verificar la integridad de los datos y su correcta recuperación.

El contenido que tiene el **plan de continuidad del negocio (*Business Continuity Plan*)** se refiere a las metodologías de la organización ante amenazas internas y externas, y las contramedidas para su prevención y recuperación. Este incluye:

- **El análisis de impacto en el negocio (*Business Impact Analysis, BIA*):** existirán diferentes parámetros que tener en cuenta, y se dividirán en críticos y no críticos. Los tiempos de recuperación ante un desastre son un ejemplo de este ítem.
- **El análisis de amenazas y riesgos (*Threat and Risk Analysis, TRA*):** en esta parte del plan se identifica qué posibles amenazas se puede encontrar la organización.

En el **plan de recuperación ante desastres** (Disaster Recovery Plan) se determinan las diferentes acciones que llevar a cabo para los procesos de recuperación ante un incidente. Incluye las prioridades de las tareas, los canales de comunicación, los simulacros para verificar la integridad de los datos y la agilidad de los procedimientos, así como aspectos asociados al inventario de equipos y pólizas de seguros.

Los plazos de recuperación son valores muy importantes en la política sobre seguridad de la información. Estos plazos son de dos tipos principalmente:

- **Recovery Point Objective (RPO):** es el periodo máximo de tiempo en el que se han podido ver afectados datos antes de un incidente.
- **Recovery Time Objective (RTO):** es el periodo máximo de tiempo que se puede asumir tener los sistemas de información parados después de un incidente.

Actividad propuesta 3.1

Sistemas de gestión de continuidad de negocio

Analiza diferentes paquetes software que faciliten la implantación, la gestión, el mantenimiento y el despliegue de sistemas para la gestión de continuidad de negocio. Estos productos software trabajan conforme a las diferentes normativas actuales. Despliega uno de ellos y especifica cuál es la normativa actual que regula estos procesos.

■ ■ 3.2.2. Métodos para las copias de seguridad

Atendiendo a la metodología llevada a cabo para la realización de las copias de seguridad, se pueden distinguir copias por granularidad y copias por operatividad del sistema, aunque se señalan otros de manera adicional, como se indica en la Figura 3.6:

1. **Por granularidad:** existen tres métodos de copias de seguridad: copias completas, diferenciales e incrementales.
 - a) **Copias de seguridad completa:** se copian integralmente todos los datos seleccionados.
 - b) **Copias de seguridad diferencial:** partiendo de una copia de seguridad completa, se hacen copias solo de los datos modificados desde que se hizo dicha copia completa. Se usa más espacio de almacenamiento y el proceso es más largo, ya que se copian más ficheros, pero las recuperaciones son mucho más rápidas, debido a que solo hay que recuperar la última copia completa y la última copia diferencial.
 - c) **Copias de seguridad incremental:** partiendo de una copia de seguridad completa, se hacen copias solo de los datos modificados desde la última copia, sea una completa o una diferencial. Se hace un número menor de copias, y se precisa una menor capacidad de almacenamiento. Los procesos de copia son más rápidos, pero los tiempos de recuperación son mayores, ya que se necesita deshacer la última copia completa y todas las incrementales hechas de esta copia.

2. Por operatividad del sistema: existen dos tipos en cuanto a la operatividad del sistema mientras se hace la copia: copias en frío u off-line y copias en caliente u on-line.

a) **Copias en frío:** el sistema no accede a los datos a los que se les desea hacer la copia. Para hacerla, se requiere de suficiente tiempo, por lo que debe ser programada y validada, y debido a ello no se efectúan en sistemas en los que la producción es muy alta.

b) **Copias en caliente:** el acceso a los datos que copiar no se detiene por las necesidades del propio sistema de información. Los tiempos en los que los datos están libres de acceso son muy cortos, por lo que la gestión de estos y el copiado deben ser muy precisos. En este tipo de sistemas, las operaciones intermedias u operaciones log determinan las modificaciones de los datos originales que se tienen en un determinado momento. Por tanto, en el momento de las copias se hace necesario hacer las modificaciones e insertarlos en la copia como si fueran los datos originales.

Se usa mucho en bases de datos y en sistemas de ficheros. El sistema se configura en un modo llamado Point-in-time Recovery, y se crea un fichero log de operaciones llamado redo log, donde se almacenan todas las modificaciones que se piden sobre los datos al comenzar la copia. Al finalizar esta, el redo log se ejecuta y se aplican todos los cambios.



Figura 3.6. Diferentes métodos de copias de seguridad: completa, diferencial, incremental, en frío, en caliente, en espejo y sintética completa, incremental inversa, y continua.

Existen otras soluciones que mezclan diferentes técnicas y que permiten aumentar la eficacia del sistema de copiado. Estas son el esquema espejo, el esquema sintético completo, el esquema incremental inverso y el esquema de protección de datos continua.

- **Espejo:** es un reflejo exacto del origen que se está respaldando, es decir, cada archivo modificado o eliminado en la fuente se modificará o eliminará en la copia de seguridad.
- **Sintético completo:** reconstruye la imagen de copia de seguridad completa haciendo uso de las copias incrementales o diferenciales ya realizadas. Se almacena, generalmente, en cintas y en ubicaciones externas a la red. El tiempo de restauración se minimiza, ya que dicha reconstrucción ya está realizada.
- **Incremental inverso:** es una copia incremental de los cambios realizados entre dos copias espejo. Después de la copia completa inicial, cada copia que se hace a continuación aplica solo los cambios de la anterior, creando una nueva copia de seguridad sintética completa.
- **Protección de datos continua:** permite realizar mayor cantidad de puntos de restauración que el resto de tipos de copias de seguridad.

■ ■ ■ 3.2.3. Determinar qué copiar

Decidir qué copiar no es tarea fácil. La capacidad de almacenamiento disponible no es infinita y, por tanto, afecta a la decisión del contenido que copiar. Si se copian datos redundantes, se agotará dicha capacidad sin respaldar toda la información imprescindible. En caso contrario, si se limita, se podría perder información crítica. Para decidir qué es susceptible de ser copiado, se deben hacer inventarios de la propia información y realizar una clasificación de estos teniendo presente su importancia para la organización. Este contenido está compuesto por los ficheros de datos, los programas y aplicaciones que los usan, y los sistemas que soportan los servicios relacionados.

Los criterios para dicha clasificación dependerán de las políticas de seguridad establecidas con anterioridad a los procesos de respaldo de la información. Estos criterios pueden ser desde la accesibilidad o confidencialidad, hasta la funcionalidad, el robo, el borrado o la pérdida.

Atendiendo al nivel de accesibilidad o confidencialidad, la información se clasifica en los tres siguientes tipos:

- 1. Confidencial:** aquella especialmente sensible o de carácter personal. Debe ser de acceso restringido a usuarios bien definidos con responsabilidad directa o que la precisen para desarrollar su actividad en el sistema. En caso de necesidad de su tratamiento externo al sistema, debe estar cifrada. Es imprescindible tener en cuenta la legislación sobre los datos de carácter personal.
- 2. Interna:** información propia de la organización, generalmente, accesible a todos los usuarios. Esta información estará adecuadamente identificada, con los mecanismos suficientes para su acceso por parte de todos los usuarios, y controlada por políticas que restrinjan su difusión fuera de la organización.
- 3. Pública:** cualquier información que no tenga restricción para su difusión.

La información que copiar también depende del tiempo de vida de la misma y el del soporte en el que está almacenada. Si este último es menor que el primero, será necesario realizar un volcado a otro tipo de soporte que permita la **durabilidad** de la información.

Otro factor importante que debe ser analizado es la **frecuencia** con la que se deben hacer las copias de seguridad. Esta dependerá del volumen de información nueva o modificada, el coste de su almacenamiento y la reglamentación existente para los procedimientos de copias de seguridad.

■ 3.3. Medios para las copias de seguridad

La elección del medio físico para salvaguardar los datos de una organización es vital para una buena planificación de las copias de seguridad. Se hace necesario un análisis exhaustivo de las características de cada uno de estos medios, y si son acordes o no a las características de la información que copiar. En gran medida, las características más importantes son la cantidad de información que es capaz de almacenar, la capacidad para ulteriores copias, el tiempo que se invierte para la copia, y la durabilidad de la información almacenada.

Estos son los factores, entre otros también cruciales, que se deben tener en cuenta para la elección de un buen sistema físico para el almacenamiento de copias de seguridad. A continuación, se van a detallar las características más importantes de los medios más usados en la actualidad. Evidentemente, existen soluciones mixtas que aprovechan las características óptimas de cada una de ellas, lo que ofrece una solución más eficaz.

■ ■ 3.3.1. Medios usados para las copias de seguridad masivas

La principal cuestión cuando se realizan copias de seguridad es determinar el volumen de datos que se desea copiar. Si estos volúmenes de datos no son especialmente grandes, cualquier dispositivo de almacenamiento provee soluciones para este copiado. El planteamiento es más complejo cuando este volumen es muy grande y se requieren soluciones más complejas que tengan en cuenta parámetros tan importantes como la velocidad de copiado y la respuesta de recuperación ante desastres. Estas soluciones pueden ser sistemas RAID, NAS, SAN, bibliotecas de cintas físicas o virtuales (VTL), etcétera.

Nota técnica



Las **bibliotecas de cintas** físicas o virtuales son soluciones hardware y software para redirigir los datos que se quieren salvaguardar a matrices de RAID usando cintas magnéticas como soporte. Las configuraciones virtuales (VTL) agrupan datos en una configuración de RAID 0 a RAID 5.

Generalmente, para las copias de seguridad masiva locales, se usan sistemas híbridos compuestos por cintas magnéticas y arrays de discos magnéticos o unidades SSD. Otras son soluciones que explotan las ventajas de disponer de los datos alojados en servidores remotos cuyos propietarios son proveedores de servicios. A continuación, se analizan

las características principales de estos medios físicos en su explotación como medios para copias de seguridad masivas.

- 1. Cintas magnéticas:** a pesar de parecer un sistema de almacenamiento obsoleto, las cintas magnéticas ofrecen prestaciones lo suficientemente convenientes como para no convertirlas en sistemas en desuso. Tienen una durabilidad muy alta, casi de 30 años, y se están desarrollando sistemas que permiten una mayor velocidad de acceso a los datos, así como un aumento considerable en su capacidad. Existen soluciones que mejoran el uso de este tipo de medios, como la lectura de códigos de barras, que permiten agilizar y optimizar la administración de las cintas, así como sistemas robotizados que aceleran los mecanismos de acceso a los almacenes de cintas. Son soluciones muy adecuadas para organizaciones de tamaño pequeño o medio, para soluciones de respaldo y de almacenamiento a bajo costo, y están orientadas al archivado definitivo de datos. Las aplicaciones para su gestión pueden estar incluidas en el propio sistema operativo, pero generalmente se prefiere el uso de aplicaciones de terceros, o del propio fabricante, que ofrecen mayor facilidad de gestión.
- 2. Copias basadas en discos ópticos:** el principal uso de los discos ópticos es el almacenamiento de copias de respaldo de las propias copias de seguridad efectuadas en otros dispositivos. Los discos Blu-ray de solo escritura son usados para soluciones baratas que no requieren de un volumen muy alto de capacidad ni una tasa de frecuencia de volcado alta. Tienen una durabilidad corta con respecto a otros medios físicos y no son una solución para copias de seguridad masivas.
- 3. Copias basadas en discos:** el mayor uso de los discos duros para las copias de seguridad masivas, ya sean discos duros magnéticos o unidades de estado sólido (SSD), es en los sistemas que apilan un conjunto de unidades de discos. Por ejemplo, se usan en soluciones NAS para sistemas que no requieran de volúmenes de copiado muy elevados. También las usan los fabricantes que proveen de soluciones a grandes organizaciones que requieren de velocidades de acceso y escritura muy elevadas, pero, generalmente, se combinan con otros medios para aprovechar la ventaja que ofrece cada uno.
- 4. Copias basadas en memoria flash:** generalmente, este tipo de memoria para copias de seguridad se usa como elemento caché o de niveles para administrar el volcado de datos cuando se usan arrays basados en disco. Son memorias más rápidas que los discos, pero no se alcanzan las capacidades de las copias de seguridad masivas. Los datos se copian primero en la caché con almacenamiento flash y, luego, se escriben en el disco.

Actividad propuesta 3.2

Copias de seguridad de un directorio

Usando tu máquina Windows, configura copias de seguridad de un directorio para que estas se hagan automáticamente. Haz lo mismo para una máquina Linux.

■ ■ ■ 3.3.2. Copias de seguridad en la nube

Esta opción cuenta con la ventaja de no disponer de ninguna infraestructura local para el volcado de la información, lo que disminuye considerablemente costes de hardware y de software, así como los procesos de administración de la información y de los componentes de almacenamiento. Para que resulte una buena solución, se debe disponer de un ancho de banda muy alto para la conexión al exterior (internet) y poseer la máxima confianza con el proveedor del servicio. La mayor desventaja de esta solución es la propia seguridad de la información, su vulnerabilidad y los procesos de restauración e integración.

Obviamente, es un sistema que garantiza la supervivencia de la información en caso de desastre, ya que se encuentra externa al sistema, en soportes a los que es imposible que les afecte lo ocurrido.

Una premisa importante para optar por esta solución es tener garantizado el uso de un canal de comunicación con el exterior totalmente cifrado, por ejemplo, usando SSL y algún algoritmo de cifrado, como puede ser AES de 256 bits.



Figura 3.7. Los nuevos modelos As a Service hacen uso de la nube para ofrecer sus servicios. Por ejemplo, Software As a Service es un modelo que distribuye software en el que tanto el soporte lógico como los datos se ofrecen a sus clientes a través de internet. Las copias de seguridad también se ofrecen bajo este modelo.

■ ■ ■ 3.3.3. Soluciones mixtas

Basadas en la unión de algunos de los medios descritos anteriormente, estas soluciones ofrecen arquitecturas mucho más óptimas y una mayor adaptación a las necesidades de la organización. Las más conocidas son D2D2T (Disk to Disk to Tape) y D2D2C (Disk to Disk to Cloud).

- **D2D2T (Disk to Disk to Tape):** solución disco a disco a cinta. Este esquema realiza una primera copia de seguridad sobre un conjunto de discos tipo NAS, SAN, etc. Al utilizar discos duros, este copiado se hace de forma rápida y eficaz, incluso se pueden

programar varios volcados diarios para evitar una posible pérdida de la información. Una vez realizada la operación completa de copiado en disco, se guarda en el sistema de cintas magnéticas. Este copiado es más lento, pero la gestión se lleva a cabo para que se realice sin que afecte al almacenamiento de los datos en los discos duros. Una vez volcada en las cintas toda la información que se desea copiar, los discos duros vuelven a ser utilizados para nuevos volcados a disco. Esta solución minimiza el coste de los discos, ya que las cintas son más económicas y, además, de mayor durabilidad. Generalmente, las cintas son almacenadas en lugares físicos diferentes al sistema de almacenamiento en disco, lo que conlleva una mayor seguridad.

- **D2D2C (Disk to Disk to Cloud):** con la aparición de copias de seguridad en la nube, esta estrategia aporta un alojamiento externo de la información, ya que las cintas no tienen que ser transportadas. De igual modo que en D2D2T, las copias se guardan primero en discos, pero, a diferencia de este, la réplica de la información copiada en disco se lleva a un sistema de almacenamiento en la nube.
- **C2C (Cloud to Cloud):** existe una tendencia en la contratación de software donde la aplicación y los datos se alojan en servidores remotos cuyos proveedores usan para la distribución el software que producen. Este tipo de tecnología, llamada **Software as a Service** (SaaS), provee de configuraciones para las copias de seguridad basadas en aquellas en el que tanto el sistema origen donde se alojan los datos como el destino donde se desea copiar los mismos están alojados en la nube.

■ ■ ■ 3.3.4. Copias de seguridad en Windows Server

La edición AOMEI Backupper Server de Microsoft es un producto que viene usándose desde Windows 2003 y que se sigue utilizando en los actuales sistemas operativos Server. Aporta características que aumentan la seguridad del sistema y de los datos. Permite copias de seguridad incrementales y diferenciales, diarias, semanales y mensuales, así como activación de eventos, conexiones con unidades USB, estrategias de backup 3-2-1, etc. Permite clonar sistema, disco o particiones.

Actividad propuesta 3.3

Copias de seguridad en Windows Server

Investiga sobre la utilidad del producto AOMEI Backupper Server, y si ha sido reemplazado por algún otro más avanzado. Procede a la descarga, instalación y ejecución.

Realiza una copia de seguridad completa y varias incrementales sobre una partición pequeña de sus discos duros (de forma predeterminada, la unidad y sus particiones están seleccionadas).

Responde esta pregunta y analiza su alcance: ¿qué tipo de destinos se pueden elegir?

Luego, programa el modo de copia de seguridad. Elige una semanal.

Responde y analiza estas preguntas: ¿cuántos tipos se puede elegir? ¿En qué consiste cada uno de ellos?

Más tarde, configura la estrategia sobre la copia de seguridad: esquema de copia de seguridad completa, incremental, diferencial, esquema de gestión de espacio u otros esquemas de copia de seguridad.

■ 3.4. Protección, imágenes del sistema y puntos de restauración

Una vez que el sistema de copias de seguridad garantiza la disponibilidad constante de los datos desde el punto de vista lógico, es necesario reflexionar acerca de ciertas consideraciones técnicas desde el punto de vista físico. No sirve de nada que el sistema de copias de seguridad sea eficiente si no está protegido contra cualquier tipo de desastre y de sabotaje.

Para las copias de seguridad en las que se usa la nube como medio de almacenamiento, los proveedores de estos servicios son los encargados de respaldar las aplicaciones locales en nubes privadas dedicadas, y proveer de sistemas de recuperación de desastres como un servicio más, conocido como **DRaaS (Disaster Recovery as a Service)**. Por tanto, se contratan los servicios para la copia de seguridad centralizada y la gestión de su línea de vida.

Para sistemas locales, se hace necesario buscar el mejor lugar para guardar las copias. Como buena política, se recomienda realizar tres copias de cada fichero y contar con un lugar fuera de la organización para almacenar y custodiar una de las copias. En este proceso, desde el punto de vista físico, también es posible plantearse la necesidad de contratar servicios de guarda y custodia.

Se hace necesario llevar un control exhaustivo de la vida útil de los soportes físicos, teniendo en cuenta el posible deterioro natural del propio soporte, errores humanos en su manipulación, fallos mecánicos, etc. Por tanto, se recomienda copiar la información, como mínimo, en dos tipos de soporte distintos. Además, se llevará a cabo un mantenimiento tanto del hardware como del software de gestión del sistema de copias de seguridad, analizando los criterios establecidos para la detección y prevención de fallos mecánicos, vulnerabilidades, infecciones o cualquier otro tipo de intrusión. Las condiciones físicas, como las climáticas, logísticas, acústicas, lumínicas, etc., deben ser las adecuadas para la conservación en los soportes usados.



Figura 3.8. Las condiciones para la conservación de los dispositivos de almacenamiento deben ser las más adecuadas. Se debe considerar la ubicación (por su peso), la climatología, las condiciones ambientales, la accesibilidad y los accesos (deben permitir labores de restitución y mantenimiento).

La conservación de la información almacenada como copia de seguridad está sujeta, principalmente, a los requerimientos legales y a su utilidad. Los datos que no son útiles y que deben ser eliminados están sujetos a la normativa sobre su conservación. Dependiendo del tamaño de la organización, la frecuencia con la que se deben hacer las copias varía. En general, una buena política sobre dicha frecuencia es realizar copias incrementales todos los días y copias totales todas las semanas.

Otra cuestión muy importante es el **cifrado de las copias de seguridad**. Se hace necesario garantizar la confidencialidad e integridad de la información. Para ello, se usarán herramientas de cifrado que protejan los datos en caso de robo o acceso no autorizados y que cumplan con lo que exige la reglamentación sobre la protección de datos sensibles.

Las **imágenes del sistema** son en realidad una copia de seguridad, pero del propio sistema. No son copias de seguridad como tales, ya que no almacenan información irre recuperable o confidencial, sino que, más bien, almacenan una copia exacta del sistema. Se usan para hacer de las reinstalaciones procesos más cómodos, sencillos y rápidos. Restaurando una imagen del sistema, se vuelve a una situación de la misma en la que se cuenta con todas las aplicaciones y servicios instalados y configurados sin tener que volver a desplegarlos.

Actividad propuesta 3.4

Creación de imágenes del sistema

Usando una máquina Windows, realiza una imagen del sistema.

Un **punto de restauración** es una copia de la información contenida en un sistema informático en cuanto a los archivos del sistema, programas y archivos ejecutables, y no a los archivos propios del usuario. Cuando se crea un punto de restauración, el sistema operativo o la aplicación usada para tal efecto guarda la información actual del sistema, de su estado, del registro y de las aplicaciones y controladores instalados, a través de información que se llama *metadatos*.

Estos metadatos describen la situación exacta en la que se encontraría el sistema si se hiciera una lectura de los mismos. Volver a un punto de restauración deja el sistema en la situación almacenada en ese momento en el que se creó el punto de restauración. Generalmente, se usa antes de instalar algún paquete, controlador o aplicación que se advierte que puede dejar inestable el sistema.

Estos puntos pueden ser creados automáticamente o gestionados por la persona responsable de sistemas. Se pueden usar herramientas de terceros para gestionar la restauración de sistemas o funciones propias incluidas en versiones del sistema operativo instalado. Estos puntos de restauración ocupan espacio en disco y, por tanto, el tamaño que ocupa ese conjunto de metadatos que almacena la situación actual del sistema debe preverse. Por ello, la gestión de puntos de restauración debe llevarse a cabo con eficacia. Un historial abusivo de puntos de restauración dejaría sin espacio de almacenamiento al sistema. Por esta cuestión, existen operaciones asociadas al mantenimiento de los puntos de restauración, como puede ser la eliminación de puntos antiguos.

Actividades propuestas

3.5. Puntos de restauración en Windows

Usando una máquina Windows, genera un punto de restauración automático y otro programado. A continuación, restaura el punto anterior.

3.6. Copia de seguridad del registro Windows

El registro de Windows es una base de datos que almacena información del sistema y metadatos, y que el sistema operativo usa cuando requiere información sobre el hardware, las aplicaciones instaladas y configuradas, las cuentas de usuarios, etc. Son las aplicaciones las que hacen los cambios en él, pero, en caso de que sea necesario realizar cambios en el registro para administración avanzada, sería recomendable realizar una copia de seguridad de este.

Realiza una copia de seguridad del registro en una máquina Windows.

3.5. Copias de seguridad en Linux

Generalmente, para las copias de seguridad en Linux es recomendable la instalación de aplicaciones propietarias. También se pueden usar las aplicaciones estándar disponibles en todas las distribuciones, pero estas no incluyen ninguna interfaz gráfica y tampoco cuentan con propiedades avanzadas en el uso de diferentes esquemas de copias de seguridad. Estas herramientas están cada vez más en desuso, pero que pueden resolver algunas situaciones urgentes son `dump`, `restore`, `tar`, `cpio`, `dd` y `duplicity`.

3.5.1. Respaldos en cintas magnéticas

El medio físico más común para los respaldos son las cintas, según se ha comentado ya, por una mejor relación costo/capacidad. Todos los dispositivos en Linux tienen un nombre lógico usado para hacerles referencia cuando se usa la línea de comandos. El nombre lógico para las cintas SCSI es `/dev/st` y, para cintas IDE, es `/dev/ht`. Para conocer a qué dispositivo está asociado una cinta SCSI, se puede ejecutar el comando

```
dmesg | grep scsi
```

Con el comando `mt` (magnetic tape control) se pueden enviar instrucciones al dispositivo de cinta. La sintaxis de este comando es

```
mt [opciones] [-f dispositivo] [comando] [cantidad] [argumentos]
```

Por ejemplo, con `-f /dev/tape` se especifica la unidad de cinta con la que se va a trabajar.

Los posibles comandos que se puede usar son:

- **Rewind:** rebobina la cinta hasta el inicio.
- **Fsf:** mueve una cantidad de volúmenes hacia delante. La cinta se posiciona en el primer bloque del volumen siguiente.

- **Fsfm:** igual que en el caso anterior, pero la cinta se posiciona en el último bloque del volumen anterior.
- **Bsf:** se mueve una cantidad de volúmenes hacia atrás, posicionándose en el primer bloque del volumen siguiente.
- **Bsfm:** igual que en caso anterior, pero la cinta se posiciona en el último bloque del volumen anterior.
- **Asf:** se posiciona en el comienzo del archivo correspondiente al parámetro ‘cantidad’ a partir del inicio de la cinta.
- **Eod:** se posiciona al final de los datos válidos.
- **Offline:** rebobina la cinta y se descarga de la torre.
- **Erase:** borra la cinta.
- **Status:** muestra el estado actual de la cinta: posición de la cinta, número de bloque actual, archivo o volumen, etcétera.
- **Eof:** escribe en la cinta tantas marcas de tipo EOF (End of File) como ‘cantidad’.

Actividad propuesta 3.7

Copia de seguridad en cintas magnéticas

Si dispones de un sistema de almacenamiento de cintas magnéticas, usa una máquina Linux y, con el comando `mp`, genera varias copias de seguridad usando las diferentes opciones que ofrece el programa.

3.5.2. Comandos para realizar copias de seguridad

En este apartado se van a analizar brevemente el comando `tar`, por su uso en compresión de datos, y el comando `duplicity`, para copias de seguridad en versiones Linux más actuales.

Comando tar

El comando `tar` (tape archiver) toma como entrada los archivos y directorios y los almacena en un único fichero. La sintaxis de este comando es

```
tar [x|c]vf [nombre-destino] [archivos-o-directorios]
```

Con la opción `c` se indica el modo de creación, con `x`, el modo de extracción, y con `t`, el modo listado.

Para crear un archivo simple con `tar`, se usaría `tar -cvf backup01.tar /home`,

donde `-c` creará el archivo `backup01.tar`, `-v` habilitará el modo detallado y mostrará el progreso, y `-f` permitirá nombrar el archivo. El destino puede ser tanto un directorio (`/home`) como un fichero o conjunto de ficheros que cumplan una expresión regular.

Para crear un archivo comprimido gzip con `tar`, se usará la sintaxis

```
tar -cvzf backup02.tar.gz /home,
```

donde la opción `-z` permite crear un archivo comprimido basado en compresión gzip.

Para usar bzip2 como método de compresión, se usa la siguiente sintaxis:

```
tar -cvjf backup03.tgz2 /home
```

donde la opción `-j` permite crear un archivo tar basado en bzip2. La extensión que usar puede ser `tgz2` o `tar.bz2`.

En caso de que se deseen comprimir varios directorios con el comando `tar`, se usa la siguiente sintaxis:

```
tar -cvf backup04.tar /ruta1 /ruta2 /ruta3
```

Cuando se quiere crear un archivo `.tar` pero se hace necesario excluir algunos archivos o directorios contenidos en la ruta, se usa la opción `--exclude`, por ejemplo,

```
tar -cvf bk05.tar /home --exclude=/home/datosnoimp01.txt  
--exclude=/home/datosnoimp02.txt
```

```
tar -cvf bk06.tar /home --exclude=/home/*.txt
```

Para listar el contenido de un archivo sin necesidad de extraerlo, se usaría el comando

```
tar -tvf bk06.tar
```

Si se trata de un archivo comprimido gzip, se usaría

```
tar -ztvf backup02.tar.gz
```

Si es un archivo bzip2, el comando es

```
tar -jtvf backup03.tar.gz2
```

Y, para descomprimir los archivos, se usa `tar -xvf` para ficheros `".tar"`, `-zxvf` para ficheros `".tar.gz"` y `-jxvf` para ficheros con el formato `".tar.gz2"`.

Comando `duplicity`

Duplicity es una herramienta de copias de seguridad disponible para la línea de comandos. Usa otras herramientas como Librsync, que implementa el protocolo rsync para almacenamiento remoto, y GnuPG para el cifrado y firma de la información y de las comunicaciones.

Algo que se debe tener en cuenta a la hora de usar Duplicity es que el usuario debe tener permisos de escritura en el directorio destino donde se va a volcar la copia de seguridad. Para ello, se usa el comando `chmod` como ya se ha visto en otras ocasiones.

Cuando se hace una copia de seguridad con Duplicity, este almacena los archivos en el destino en formato `.tar` y usa GnuPG para cifrarlos.

Para instalar Duplicity, se ejecuta el siguiente comando para añadir repositorios al sistema propios de Duplicity:

```
apt-add-repository ppa:duplicitiy-team/ppa
```

Y se actualiza la base de datos de paquetes almacenados por el sistema operativo ejecutando

```
apt update  
apt upgrade
```

A continuación, se instalan los paquetes necesarios:

```
apt-get install duplicity haveged Python-boto
```

Para averiguar si se tienen instalados GnuPG o GPG, se ejecuta `gpg --version`.

En caso de que se quisieran hacer copias en un servidor externo, se indicaría el protocolo que se quiere usar en el mismo lugar donde se ha escrito *file*.

Para programar una copia diaria incremental, se colocaría el comando correspondiente en un fichero dentro del directorio `/etc/cron.daily`. Para una copia semanal completa, se usaría el directorio `/etc/cron.weekly`.

Actividad resuelta 3.1

Copias de seguridad con Duplicity

Para realizar este ejercicio, se deben tener instalados Duplicity y Gpg en el equipo Linux. Para ejecutar diferentes situaciones con Duplicity, se va a simular una situación real. Se supone que en el directorio `/var/local/origen` se dispone de un conjunto de ficheros a los que se les requiere hacer copias de seguridad.

Para simular esto, se pueden crear una serie de ficheros que, aunque estarán vacíos, servirán para la actividad.

Se ejecutaría el comando

```
touch /var/local/datos/file{1..40}.conf
```

Este comando crea 40 ficheros vacíos en `/var/local/origen` con los nombres `file1.conf`, `file2.conf`, etcétera.

Se supone que el destino en el que se quieren almacenar las sucesivas copias es `/var/local/copia`, y el directorio de restauración es `/var/local/restauracion`.

El usuario debe disponer de suficientes privilegios para escribir en ambos directorios. Para ello, se ejecuta la orden

```
Chmod 777 /var/local/copia /var/local/restauracion
```

Solución

Para realizar la primera copia, se escribiría

```
duplicity full /var/local/origen/ file:///var/local/copia
```

La primera vez que se ejecuta este comando, se crea una copia completa. Las siguientes serían copias incrementales de la primera. Si se quisiera forzar una nueva copia como completa, se escribiría

```
duplicity full /var/local/origen/ file:///var/local/copia
```

Para ver el contenido de este backup, se escribiría

```
duplicity list-current-files file:///var/local/copia
```

Para mostrar todos los backups realizados en esta copia, se habría que usar la opción collection-status en

```
duplicity collection-status file:///var/local/copia
```

Para recuperar todos los ficheros, se usa la opción restore

```
duplicity restore file:///var/local/copia/ /var/local/restauracion/
```

Si se quisiera recuperar solo un grupo de ficheros dando una fecha, se usaría la opción time del modo

```
duplicity --time 28/09/2025 --file-to-restore *.conf restore  
file:///var/local/copia/ /var/local/restauracion/
```

Con el siguiente comando, se copia el directorio /var/local/origen a un servidor remoto en el directorio copia usando el protocolo ftp.

```
duplicity /var/local/origen  
ftp://antonio:5p7o9s1t9i0g8o2@paraninfo.es/copia
```

En este ejemplo, la contraseña se muestra en la URL de la conexión. Para evitar esto, se podría haber escrito

```
duplicity /var/local/origen ftp://antonio@paraninfo.es/copia
```

pero, en esta ocasión el servidor ftp remoto habría pedido la contraseña del usuario.

El siguiente ejemplo permite restaurar, usando el protocolo ssh, todo el directorio del servidor remoto en el que se hizo la copia de seguridad hace tres días en el directorio /var/local/restauracion

```
duplicity -t 3D ssh://usuario@paraninfo.es/copia  
/var/local/restauracion
```

El siguiente ejemplo permite hacer un borrado de backups. Este comando eliminaría del directorio copia en el servidor remoto la copia de seguridad de tipo full y todas las incrementales que dependan de ella usando el protocolo rsync.

```
duplicity --no-encryption remove-all-but-n-full 1 --force  
rsync://antonio@paraninfo.es/copia
```

■ 3.6. Seguridad en el almacenamiento conectado en red

En los apartados anteriores, se han analizado diferentes configuraciones para proveer de una alta disponibilidad de los datos al sistema de información. En cualquier sistema de información, lo más importante no es el hardware ni el software, ya que estos pueden ser restituidos en cualquier momento, al contrario que los datos. El volumen de la información cada vez es mayor y se necesita acceder los datos en el menor tiempo posible. Por tanto, los procesos para su adecuada y eficaz gestión, atendiendo a los costes que conllevan, son uno de los objetivos primordiales en cualquier sistema de información.

Las tecnologías de almacenamiento remoto ofrecen grandes mejoras en estos procesos de gestión que merecen su implantación. Ejemplos de ellas son las arquitecturas DAS (Direct Attached Service), NAS (Network Attached Storage) y SAN (Storage Area Network).

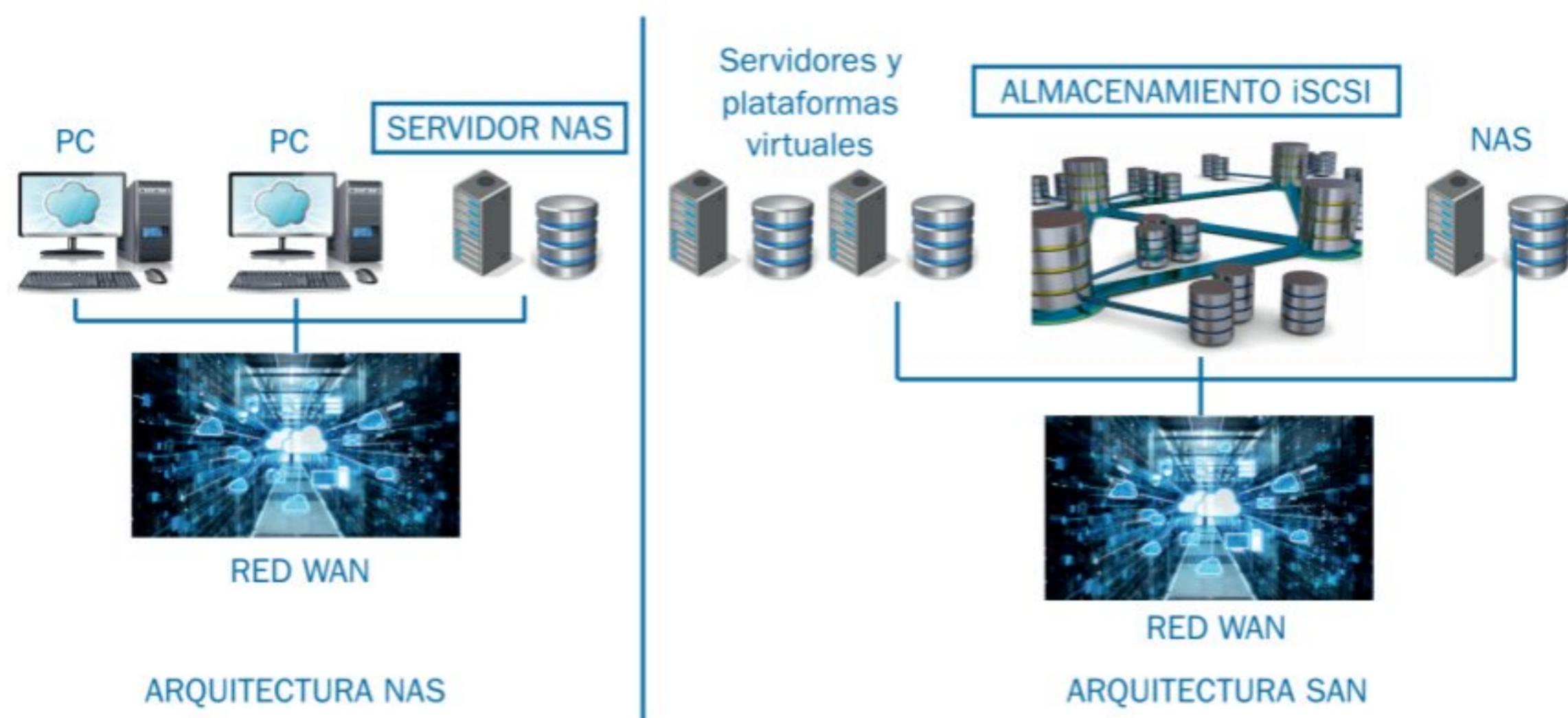


Figura 3.9. Diferencia entre las arquitecturas NAS y SAN.

■ ■ 3.6.1. Arquitectura Direct Attached Service (DAS)

En esta arquitectura, los medios de almacenamiento, generalmente discos rígidos, se conectan directamente al servidor que gestiona el control de acceso al sistema de información centralizado. El sistema de disco se conecta al equipo servidor a través de conexiones SATA, SAS, USB y SCSI. Se pueden utilizar sistemas RAID para mejorar la seguridad de los datos, que se almacenan como ficheros, que son, a su vez, la unidad mínima de acceso a disco.

Cualquier cliente que requiera acceso a la información centralizada accederá a través del servidor mediante sus aplicaciones instaladas. Es el servidor el que gestionará el acceso a los datos alojados en sus medios de almacenamiento. Es una solución económica y fácil de gestionar, ya que todo está centralizado en un punto, pero, si este servidor deja de trabajar por alguna razón, los datos compartidos no estarán accesibles para ningún cliente.

■ ■ 3.6.2. Arquitectura Network Attached Storage (NAS)

En esta solución, el sistema de almacenamiento compartido y centralizado se encuentra conectado a toda la red local, por lo que cualquier cliente con los permisos suficientes y software de gestión oportuno pueden acceder a la información dispuesta en los discos que comportan el servidor NAS. Esta tecnología requiere del uso de sistemas operativos para la gestión de protocolos SMB/CIFS, Samba, NFS, HFTP, FTP y TFTP. La comunicación se hace a través de un medio físico compartido, generalmente guiado, a través de una red, normalmente TCP/IP.

También se considera un sistema NAS al propio servidor que comparte sus unidades de red. La unidad mínima de acceso en estos sistemas es, igual que en arquitecturas DAS, el fichero. Por tanto, los accesos a discos desde los clientes se hacen a través del fichero que contiene la información a la que se quiere acceder. Generalmente, estas arquitecturas se basan en la explotación de discos rígidos dispuestos en tecnología RAID o gestionados con contenedores de almacenamiento redundante.

La interfaz hardware entre el NAS y los clientes se denomina *NAS box* o *NAS head*, que son los propios controladores que gestionan la comunicación con los diferentes discos y poseen una dirección IP para toda la red local. Las aplicaciones de usuario se comunican con los sistemas de archivos de manera remota mediante protocolos destinados para ello como pueden ser CIFS y NFS, pero el almacenamiento es local al sistema de archivos.

La gestión de este tipo de tecnología no es compleja y resulta muy ventajosa por sus bajos costes y sus altas prestaciones, pero tiene un menor rendimiento y confiabilidad debido al uso compartido de las comunicaciones. Son soluciones adecuadas en sistemas con grandes cantidades de datos, que requieren tolerancia a fallos y balance de carga a bajo costo.

■ ■ ■ 3.6.3. Arquitectura Storage Area Network (SAN)

Una red de área de almacenamiento SAN (Storage Area Network) constituye una red paralela a la red local por donde circulan los datos críticos con una calidad de transporte asegurada, es decir, comporta una red especializada que permite acceso rápido y confiable entre los servidores y los recursos de almacenamiento. Esta red va a permitir la conexión de servidores, sistemas de discos apilados y librerías de soporte. Se basa en tecnología fibre channel e iSCSI, con el fin de asegurar una conexión rápida sin perder seguridad y fiabilidad.

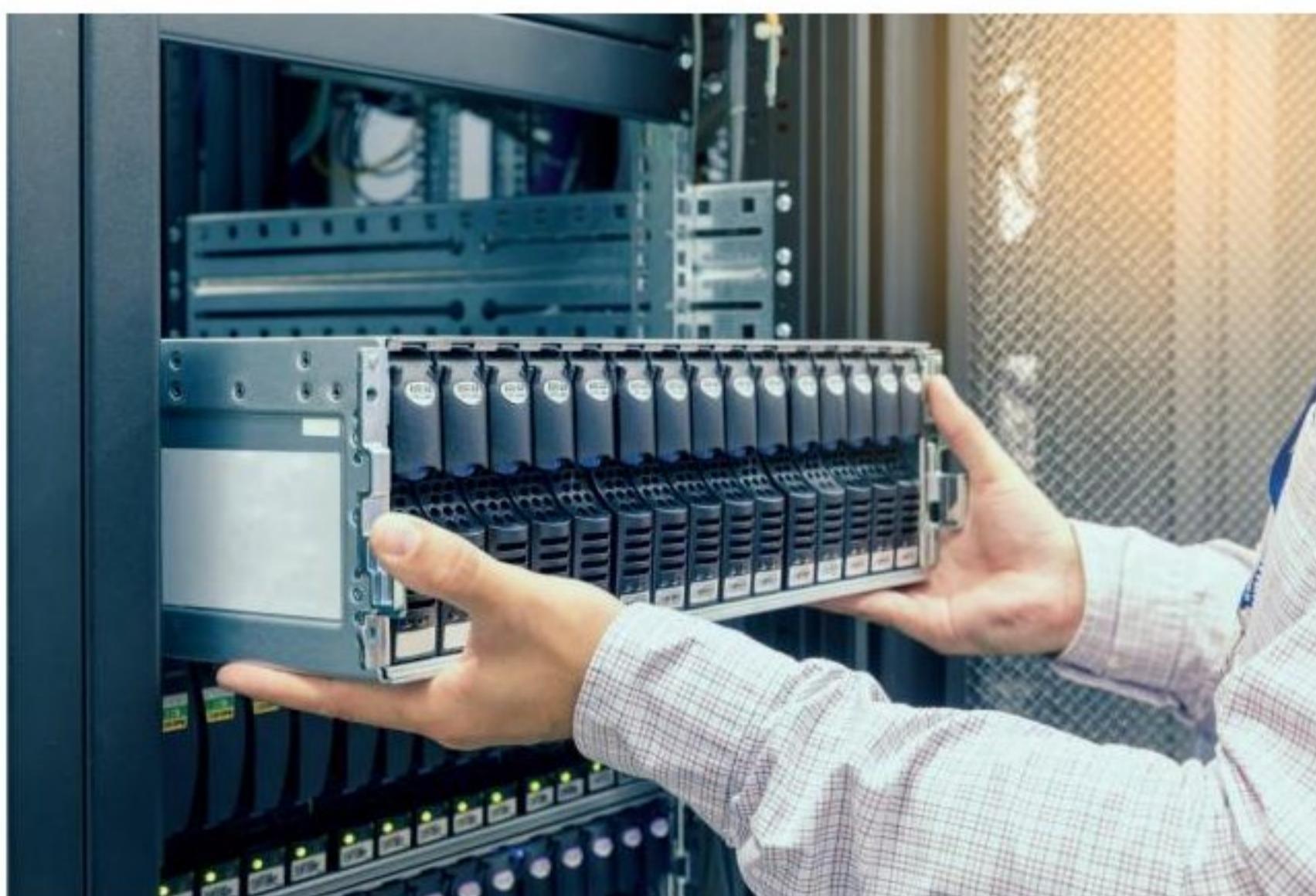


Figura 3.10. El acceso a los discos en SAN es a través de una red de alta velocidad (iSCSI, red de fibra óptica, etc.). Optimiza el espacio en la cabina de discos. En la arquitectura iSCSI, la capacidad se reparte entre usuarios y almacenamiento.

En las arquitecturas SAN se encuentran los siguientes elementos:

- Una red de alta velocidad (fibra o iSCSI).
- Dispositivos de interconexión dedicados, como conmutadores, puentes, etcétera.
- Elementos de almacenamiento en red (generalmente, discos rígidos, unidades SSD, etcétera).

Y se pueden diferenciar las siguientes tres capas:

- **La capa host:** compuesta por los servidores, dispositivos o componentes, llamados HBA, GBIC, GLM, y los sistemas operativos.
- **La capa fibra:** generalmente compuesta por el cableado de fibra óptica, o ethernet de alta velocidad, y los elementos que comportan los puntos centrales de conexión, como son los concentradores y los conmutadores SAN.
- **La capa de almacenamiento:** compuesta por el sistema de almacenamiento, generalmente formado por arrays de discos con tecnología RAID o sistemas de accesos a cintas.

La red de almacenamiento puede ser una red de canal de fibra que usa conmutadores especiales de fibra óptica y protocolos FCP (Fibre Channel Protocol) para el transporte. Una opción más económica es el uso de una infraestructura LAN, con el uso de concentradores y conmutadores ethernet interconectados llamados SAN IP. Estos usan iSCSI como protocolo de transporte.

Actividad propuesta 3.8

Despliegue de un servidor SAN en Windows Server

Usando un sistema operativo Windows Server, ofrece un servicio de almacenamiento por red usando iSCSI en red ethernet.

En Windows Server, la consola de administrador del servidor y los cmdlets de Windows Powershell para el administrador del servidor permiten la instalación de roles y características en servidores remotos o locales, o en discos duros virtuales (VHD) sin conexión. Despliega un servidor SAN en tu servidor haciendo uso de estas herramientas.

3.6.4. Arquitectura híbrida SAN-NAS y alta disponibilidad

Cuando el sistema requiere acceder a volúmenes de datos excesivamente grandes y la velocidad de acceso debe ser lo mayor posible, la mejor solución son las tecnologías SAN. Estas son mucho más caras que las NAS. Cuando no sea posible una arquitectura SAN completa, se pueden minimizar costes mezclando soluciones NAS en una arquitectura base SAN. Existen soluciones que implican el uso de las tres tecnologías (DAS, NAS y SAN) en un mismo contexto.

La alta disponibilidad en el almacenamiento de datos es un factor muy importante para garantizar la disponibilidad de la información y, por tanto, la seguridad de la misma. Confi-

guraciones no complejas que permiten alta disponibilidad en el almacenamiento de datos son la arquitectura redundante NAS y los clústeres de alta disponibilidad:

- **Arquitectura redundante NAS:** agrega un segundo servidor de almacenamiento usando un dispositivo llamado *comutación por error*, que incluye una copia en caliente de todos los datos. Ambos equipos están configurados en la misma red local y comparten una misma dirección IP. Si alguna vez uno de los dos servidores de almacenamiento redundante no está disponible, los datos serán accesibles a través de la comutación por error hacia el otro servidor.
- **Clúster de alta disponibilidad:** consiste en dos o más servicios replicados mediante el uso de un equilibrador de carga. Este garantiza que el tráfico se envíe al servidor en funcionamiento de comutación por error en caso de fallos en el hardware o en la aplicación.

■ ■ ■ 3.6.5. Despliegue de un servidor NAS usando NAS Synology

En esta solución, se plantea el despliegue de un sistema de almacenamiento conectado en red en el cual una máquina actúa como gestor para la conexión a los discos duros que se comparten dentro de la red local a través de la gestión de permisos de acceso. Las principales ventajas de este tipo de servidores NAS son:

- Consume poca electricidad.
- No son precisos grandes conocimientos técnicos para su configuración y mantenimiento, ya que cuenta con una interfaz sencilla para su gestión.
- Se centraliza toda la información digital en un solo lugar, lo que posibilita los respaldos centralizados direccionalmente las copias de seguridad automáticamente.
- Permite la sincronización de archivos con la nube y de forma on-line.
- Se pueden crear accesos remotos, lo que permite acceso desde el exterior.

■ ■ ■ Instalación y configuración de red

Una vez descargada la aplicación de Synology Assistant desde la página web de Synology.com, se procede a la instalación. Este instalador buscará el sistema operativo de Synology, el DiskStation. Una vez localizado, mostrará el nombre del servidor, la dirección IP, la dirección MAC de la interfaz de red, la versión, el modelo y el número de serie.

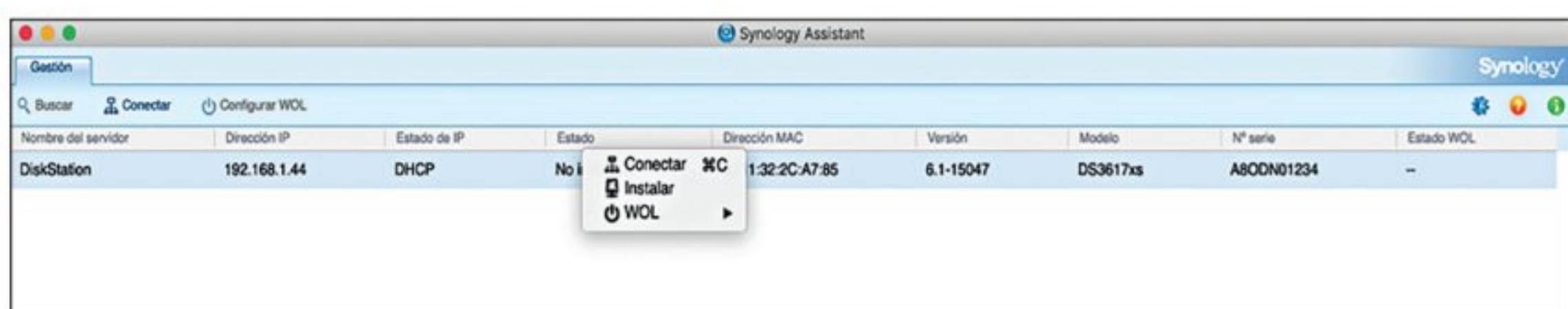


Figura 3.11. Una vez localizado el sistema operativo de Synology (por ejemplo, DiskStation con IP 192.168.1.44), en su menú contextual se puede proceder a la instalación del producto.

En el menú contextual de DiskStation se encuentra la opción Instalar. Tras pulsar Instalar, se completará la información del servidor NAS cumplimentando la cuenta del administrador, su contraseña y el nombre del servidor.

Una vez instalado, se procede a la configuración de red del servidor NAS. Por defecto, la opción preseleccionada es ‘Obtener la configuración de la red automáticamente (DHCP)’, pero se puede configurar un direccionamiento estático, indicando la dirección IP, la máscara de red, la dirección IP de la pasarela predeterminada, y la dirección IP del servidor DNS primario.

Una vez configurados los parámetros de red, se puede acceder a la sesión de inicio a través del navegador e indicar la dirección IP del servidor NAS Synology. La primera pantalla que se obtiene es la de autenticación del usuario. Se insertarán los datos ofrecidos en el proceso de instalación.

■■■ Creación y configuración de grupos RAID

Para crear los grupos RAID, se accede a Administrador de Almacenamiento y se selecciona RAID group. Una vez creado, se configura el tipo de RAID que se va a usar. Se procede a elegir el sistema RAID 1. Este tipo de RAID se compone, como mínimo, de dos discos en espejo con igual capacidad de almacenamiento, de tal forma que, si uno falla, está a disposición el otro con toda la información.



Figura 3.12. Este es el asistente de creación de un grupo RAID. En la parte izquierda de esta pantalla, se muestra cada uno de los discos que pueden participar en el grupo RAID (pueden ser discos reales, discos virtuales o particiones). Arrastrando hacia la derecha, los discos quedan seleccionados para participar en el grupo RAID.

A continuación, se debe elegir los discos que componen dicho RAID 1. Aunque no es imprescindible que tengan el mismo tamaño, sí es recomendable, ya que solo se amortiza el tamaño del disco menor. Una vez configurado, se podrá obtener una pantalla con toda la información del sistema de información recién creado.

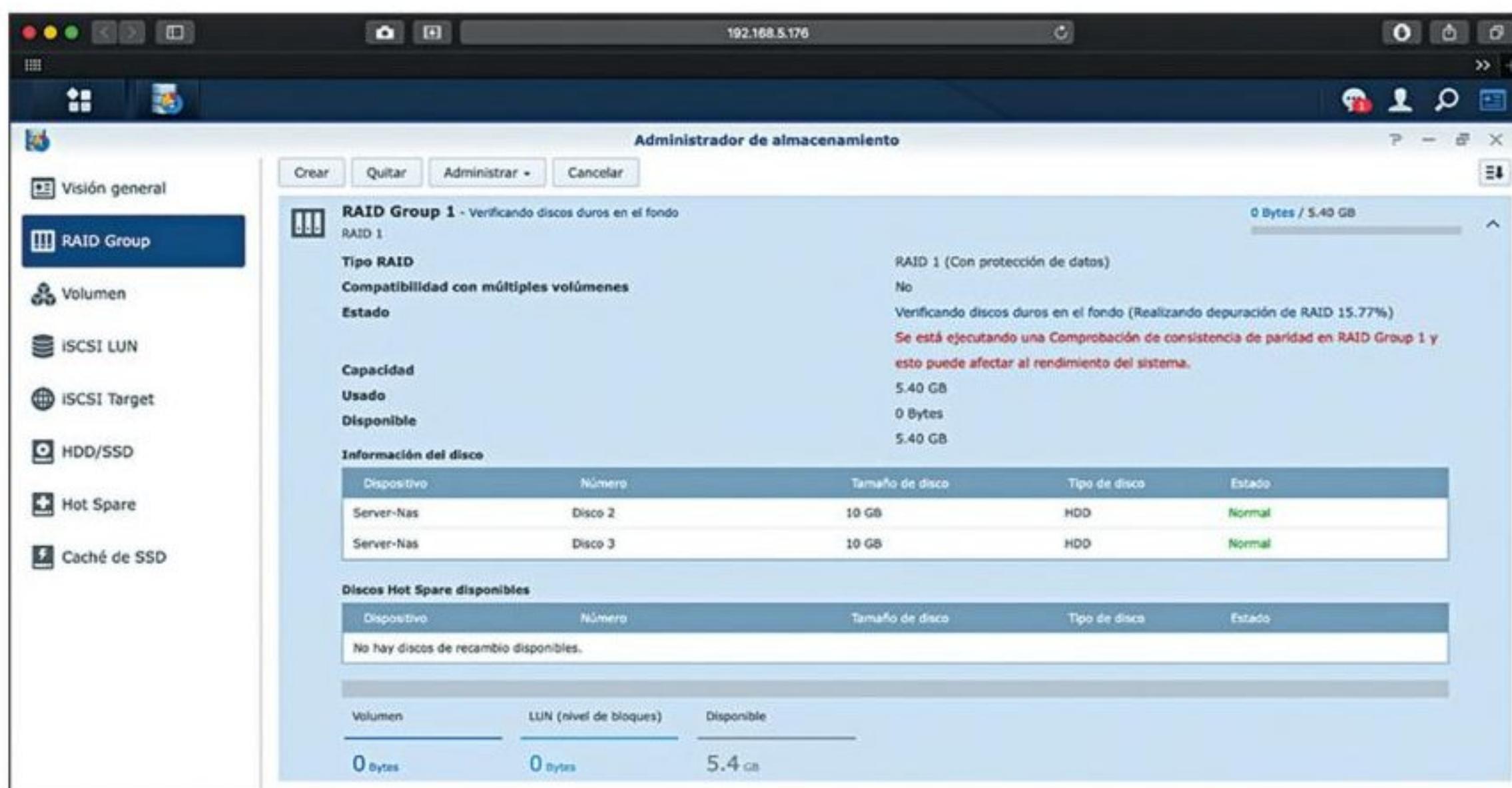


Figura 3.13. Este es el panel que muestra toda la información sobre el grupo RAID creado. Se ve el nombre del dispositivo, el número de disco, el tamaño de cada disco, el tipo de partición y el estado en el que están.

A continuación, se procede exactamente igual para un segundo RAID Group. Este alojará los directorios compartidos para todo el sistema. El tipo que RAID que se debe elegir es RAID Basic. Se compone de un solo disco, que se usará para almacenar la información de todos los directorios compartidos a los que tienen acceso los clientes de la red.

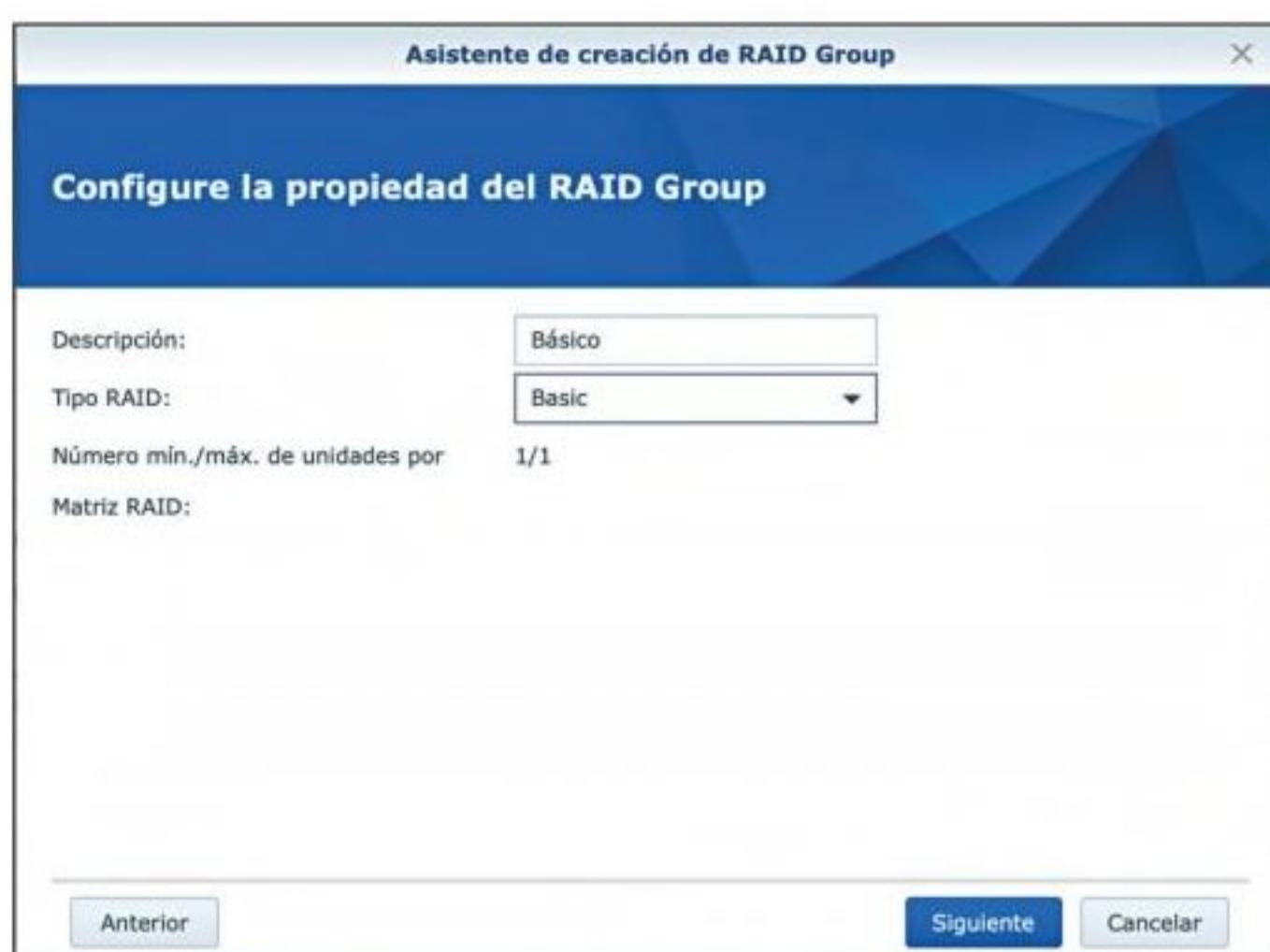


Figura 3.14. Creación del segundo sistema RAID de tipo básico, con un número mínimo y máximo de unidades por array de uno.

Igual que en el caso del grupo anterior, se elige el disco que compone este grupo.

■■■ Creación de los volúmenes

A continuación, se procede a crear el primer volumen eligiendo el RAID Group 1. Este volumen se usará para almacenar las aplicaciones que se instalarán en el servidor NAS. Luego, se procede a crear el segundo volumen, eligiendo en esta ocasión el RAID Group 2. Este segundo volumen se usará para almacenar todos los ficheros y directorios que se pretenden compartir por la red.

Seleccionando la pestaña volumen de la izquierda, se obtiene toda la información de los volúmenes creados.

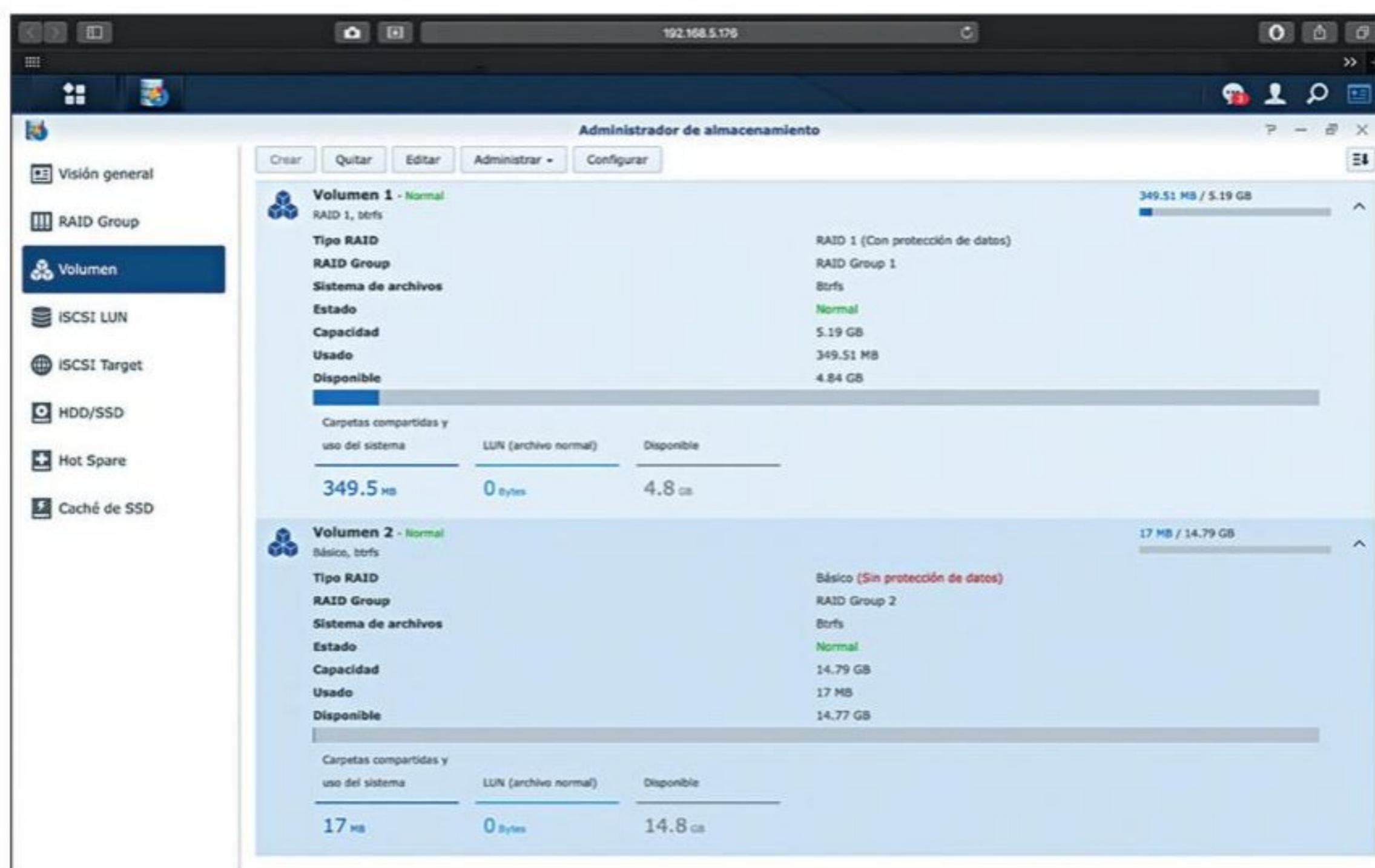


Figura 3.15. Esta es la pantalla de información de los volúmenes creados en el sistema. Se puede observar que se han creado dos volúmenes, uno con el grupo RAID 1 (con protección de datos) y otro con el grupo RAID 2 (sin protección de datos, ya que solo tiene un disco), ambos con el sistema de archivo BTRFS.

■■■ Gestión de usuarios

En el panel de control se pueden crear los grupos, los usuarios y otras opciones avanzadas de configuración. La opción grupo del panel de control permite arrancar el asistente que posibilitará gestionar grupos de usuarios, indicando el nombre del grupo y una descripción. Tras esto, se debe elegir una cuota para todos los usuarios de dicho grupo. Si está deshabilitado, la cuota será ilimitada. Luego, se indicarán los permisos de acceso a las aplicaciones nativas del servidor NAS, por ejemplo, escritorio, FTP y File Station.

Una vez creado el grupo, en editar se pueden reajustar dichos parámetros de configuración.

Con usuario del panel de control se ejecutará el asistente para crear un nuevo usuario. Se indicarán su nombre, descripción, correo electrónico y contraseña. Luego, se elige en

qué grupo se añadirá el usuario recién creado. Existe un grupo llamado *System default group* que contiene todos los usuarios creados en el servidor NAS. Más tarde, se escoge una cuota de usuario si es diferente a la cuota de usuario asignada al grupo. También se selecciona el volumen donde se almacenarán todos los usuarios, por ejemplo, volumen 1. Por último, se eligen los permisos que dicho usuario posee para acceder a las aplicaciones nativas del servidor NAS.

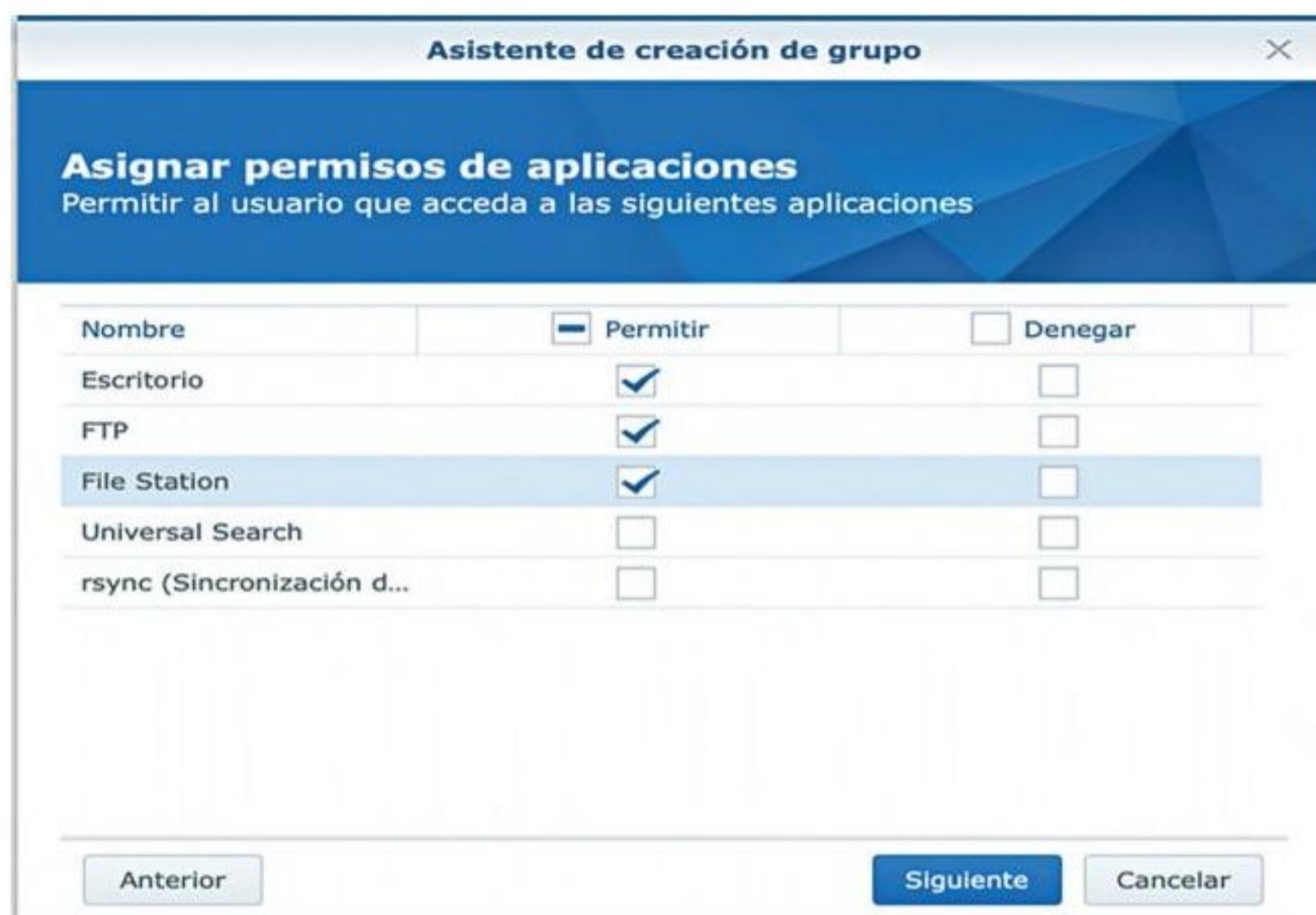


Figura 3.16. Esta pantalla muestra la asignación de permisos de los usuarios hacia las aplicaciones nativas del NAS.

■ ■ ■ Conexión desde el exterior

Para la conexión al servidor NAS desde el exterior es necesario activar QuickConnect. QuickConnect facilita la conexión a DiskStation desde cualquier lugar, tan solo se necesita habilitarlo y crear una cuenta Synology. Tras el registro de una cuenta Synology, se obtendrá una dirección web de acceso que permita la conexión remota desde el exterior. Lo único que se necesita hacer desde el cliente es introducir dicha dirección en el navegador, lo que redireccionará al servidor NAS remoto y hará posible iniciar sesión en dicho servidor NAS como si estuviera en la propia red local.

■ ■ ■ 3.6.6. Despliegue de un servidor NAS usando FreeNAS

FreeNAS es un sistema operativo basado en FreeBSD que proporciona servicios de almacenamiento en red y que permite convertir un equipo en un soporte de almacenamiento accesible desde la red.

La administración se hace desde páginas web accesibles desde cualquier equipo de la red usando simplemente el navegador. Se puede instalar en discos rígidos o SSD, USB key o tarjeta compactFlash.

Entre los servicios que proporciona, destacan los de controlador de dominio, DNS dinámico, CIFS, NFS, SSH, rSync, protocolos iSCSI, autenticación de usuarios y RAID por software.

Los protocolos de red incorporados proporcionan acceso de almacenamiento a múltiples sistemas operativos y proporcionan un sistema de complementos para ampliar las funciones integradas.

Las funciones principales de FreeNAS son:

- **Réplica:** se usa el sistema de ficheros ZFS que permite el uso de instantáneas y replicación en otros sistemas. Estas instantáneas del mismo sistema de ficheros se pueden enviar de forma incremental, lo que reduce el tamaño de cada copia. Las instantáneas permitirán recuperar los datos en caso de catástrofe.
- **Protección de datos:** con ZFS, la integridad de los datos está asegurada. RAID-Z ofrece protección única de paridad en RAID 5.
- **Cifrado:** permite cifrar los diferentes volúmenes creados, usando cifrado AEZ-XTS.
- **Instantáneas o snapshots:** el sistema permite crear instantáneas de todo el sistema completo en cualquier momento, posibilitando la vuelta a cualquier estado anterior, ya sean programadas o gestionadas manualmente.
- **Ficheros compartidos:** es compatible con muchos de los sistemas de archivo habituales, como SMB/CIFS, NFS, AFP, FTP, SCSI o WebDAV.

Actividad resuelta 3.2

Despliegue de NAS con FreeNAS

Despliega un servidor NAS en un equipo con las siguientes características:

El servidor NAS FreeNAS contará con 8 GByte de RAM (recomendado).

Se usará VirtualBox como aplicación para la virtualización.

El servidor NAS contará con adaptador puente con la NIC del equipo servidor.

El servidor NAS contará con la disponibilidad de tres discos duros, uno para la instalación y, los otros dos, para el almacenamiento.

Solución

Primero se inicia la máquina virtual (el arranque desde el CD debe configurarse de manera predeterminada) y se procede con la instalación de FreeNAS. En el menú que se obtiene en 'Console setup' se elige la opción 1 Install/Upgrade. A continuación, se escoge el disco duro en el que se instalará el sistema operativo, pudiéndose elegir más de un disco. Una vez finalizado el proceso, la máquina se reiniciará y el sistema FreeNAS estará instalado en el disco seleccionado.

A continuación, se obtiene un menú modo consola con las siguientes opciones: 1) Configure Network Interface para configurar parámetros de la interfaz de red; 2) Configure Link Aggregation para configurar datos de enlace; 3) Configure VLAN Interface para configurar parámetros de la LAN virtual; 4) Configure Default Route para configurar rutas por defecto; 5) Configure Static Routes para configurar rutas estáticas; 6) Configure DNS para configurar parámetros relacionados con el servidor DNS; 7) Reset Root Password para

reconfigurar el password de root; 8) Reset Configuration to Defaults para reiniciar con los parámetros por defecto; 9) Shell, 10) Reboot para reiniciar; 11) Shut Down para apagar.

Por tanto, se pulsa 1 y se selecciona direccionamiento estático o dinámico. En caso de direccionamiento estático, se introduce la dirección IP y la máscara de subred.

Para cambiar la contraseña del root, se pulsa 7.

Una vez configurados todos los parámetros necesarios, se accede a cualquier máquina de la red y, usando el navegador, se introduce la dirección IP de la tarjeta de red recién configurada.

En el Dashboard, se muestra un resumen del sistema, discos, estado de la red, etcétera.

A continuación, se explican algunos contenidos de especial interés que se muestran en la barra vertical de la izquierda:

- **Account:** aquí se configura todo lo referente a usuarios, grupos y su configuración. Se pueden configurar nombre, contraseñas y permisos. Con el botón add, se podrán añadir nuevos usuarios.
- **System:** aquí se puede configurar todo lo relativo a correos, alertas, credenciales, certificados, horas, idiomas, etcétera.
- **Services:** aquí se puede configurar todo lo relativo a los diferentes servicios de los que dispone el servidor NAS desplegado. Por ejemplo, se puede dejar activado smb para compartir ficheros, Smart para el test de rendimiento de los discos duros y rsync para la sincronización y copias de seguridad.
- **Plug-in:** aquí se muestran los plug-in disponibles y los instalados.
- **Storage:** aquí se crean los diferentes RAID y se parametrizan los diferentes discos duros.

A continuación, se procede a crear los diferentes RAID. En Storage, se añade dos POOL principales, uno para cada disco. Uno será copia del otro gracias a la función rSync. En el POOL principal se creará un POOL para cada directorio que se desea compartir, y en el apartado configuración se añadirán los permisos de grupos y usuarios que dicho pool directorio necesite.

Actividad propuesta 3.9

Copiando ficheros de configuración

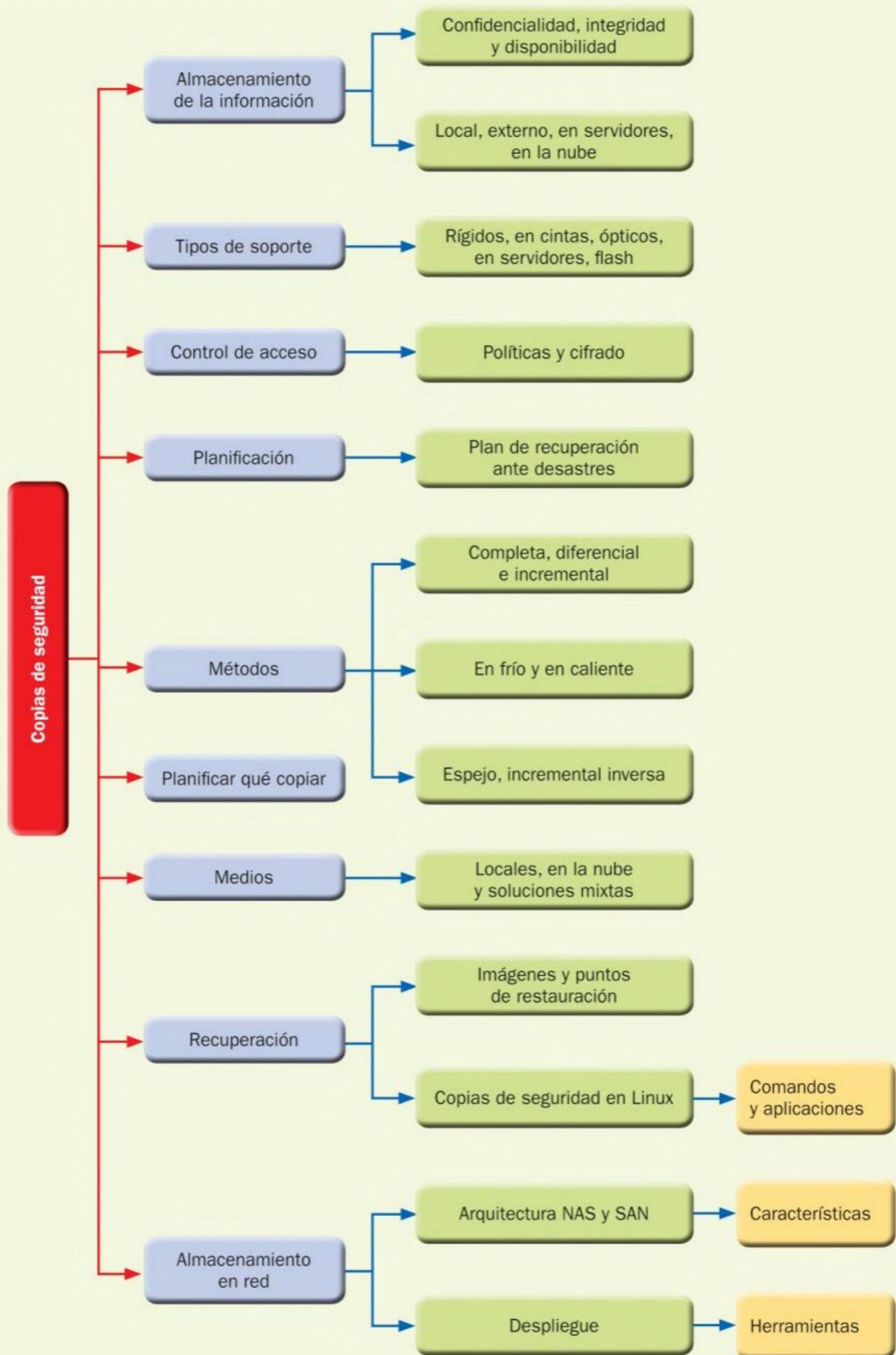
Analiza los servicios instalados en tu máquina Linux: servicio DHCP, servicio DNS, servicios web, servicio ftp, servicio SMB y servicio correo electrónico.

Para cada uno de estos servicios, detecta cuáles son los ficheros de configuración que sería necesario copiar para una posible reconfiguración en caso de reinstalación de los mismos.

Completa para ello la siguiente tabla:

Servicio	Fichero	Ubicación	Acepta otra ubicación	Descripción

En la columna 'Acepta otra ubicación' se indicará Sí, si el fichero de configuración puede ubicarse en cualquier directorio sin que afecte al servicio.



Actividades de comprobación

- 3.1. ¿Cuál de las siguientes opciones no es un objetivo que persiguen las políticas de explotación de sistemas de almacenamiento?**
- a) Evitar la divulgación.
 - b) Controlar la intrusión.
 - c) Vigilar la difusión indebida.
 - d) Permitir la destrucción de información de carácter personal.
- 3.2. Las copias reguladas:**
- a) Se hacen para disponer de instantáneas de los datos en un momento determinado.
 - b) Se hacen para cumplir con normativas.
 - c) Se hacen para usarlas cuando se necesite subsanar la pérdida de datos valiosos.
 - d) Ninguna de las opciones anteriores es correcta.
- 3.3. Las copias operacionales:**
- a) Se hacen para usarlas cuando se necesite subsanar la pérdida de datos valiosos.
 - b) Se hacen para disponer de instantáneas de los datos en un momento determinado.
 - c) Se hacen para cumplir con normativas.
 - d) Ninguna de las opciones anteriores es correcta.
- 3.4. ¿Cómo se denomina la copia de seguridad que reconstruye la imagen completa haciendo uso de las copias incrementales o diferenciales ya realizadas?**
- a) Copia en frío.
 - b) Copia en caliente.
 - c) Copia sintética completa.
 - d) Copia incremental inversa.
- 3.5. El contenido que tiene el plan de continuidad del negocio incluye metodologías ante amenazas:**
- a) Internas para la organización.
 - b) Externas a la organización.
 - c) Internas y externas.
 - d) Ninguna de las anteriores es correcta.
- 3.6. En las copias de seguridad completa:**
- a) Se copian integralmente todos los datos seleccionados.
 - b) Se hacen copias de los datos modificados desde la última copia completa.
 - c) Se hacen copias de los datos modificados desde la última copia diferencial.
 - d) Se hacen copias de los datos modificados desde la última copia completa o diferencial.
- 3.7. En las copias de seguridad incremental:**
- a) Se hacen copias de los datos modificados desde la última copia completa o diferencial.
 - b) Se hacen copias de los datos modificados desde la última copia diferencial.
 - c) Se hacen copias de los datos modificados desde la última copia completa.
 - d) Se copian integralmente todos los datos seleccionados.
- 3.8. La solución de copia de seguridad D2D2T:**
- a) Supone la contratación de software y alojamiento en servidores remotos.
 - b) Aporta un alojamiento externo de la información usando internet.
 - c) Hace una copia sobre un conjunto de discos tipo NAS, SAN o DAS.
 - d) Ninguna de las anteriores es correcta.

3.9. ¿En qué consiste un clúster de alta disponibilidad?

- a) En agregar un segundo servidor de almacenamiento.
- b) En replicar dos o más servicios mediante el uso de un dispositivo llamado *comutación por error*.
- c) En replicar dos o más servicios mediante el uso de un dispositivo llamado *equilibrador de carga*.
- d) Ninguna de las opciones anteriores es correcta.

3.10. En cuanto a la arquitectura DAS:

- a) Los discos rígidos se conectan directamente al servidor.
- b) El almacenamiento es compartido y centralizado a través de toda la red local.
- c) Comporta una red especializada de acceso rápido y fiable entre servidores y recursos de almacenamiento.
- d) Ninguna de las opciones anteriores es correcta.

Actividades de aplicación

3.11. Enumera brevemente los principales sistemas de almacenamiento de la información.

3.12. De los soportes de almacenamiento de datos existentes en el mercado, ¿cuál es el más usado para las copias de seguridad? Justifica tu respuesta.

3.13. Enumera y describe brevemente diferentes políticas de acceso a los datos.

3.14. Desarrolla un pequeño informe en el que se especifiquen las acciones de un plan de recuperación ante desastres.

3.15. En una máquina Windows, restaura una copia de seguridad realizada en otro equipo.

3.16. En tu máquina Windows, usa el historial de archivos para hacer una copia de seguridad y procede luego a su restauración.

3.17. ¿Cuáles son las diferencias principales entre D2D2T, D2D2C y C2C?

3.18. Elige un sistema operativo de Microsoft en el que se pueda desplegar un servidor de archivos. Procede a la configuración del mismo y pon un ejemplo de uso compartiendo un directorio y una partición a diferentes usuarios de la red corporativa.

Actividades de ampliación

3.19. Busca en internet información sobre las copias de seguridad en OwnCloud. Usa esta plataforma para hacer una copia de seguridad de una partición en particular de una máquina Linux.

- 3.20.** Con la herramienta Cron de Linux, programa una tarea que ejecute una aplicación de backup para hacer una copia de seguridad de una partición. Ten en cuenta que la aplicación de backup está ubicada en el directorio /usr/bin y se quiere ejecutar todos los sábados a las 12:00 de la noche. Programa otro backup total una vez al mes.
- 3.21.** Investiga sobre herramientas para Windows que permitan realizar recuperaciones de datos. Evalúa las más conocidas.
- 3.22.** Investiga sobre herramientas para Linux que permitan realizar recuperaciones de datos. Evalúa las más conocidas.
- 3.23.** Desarrolla los conceptos que se pueden identificar en la siguiente figura:



Enlaces web de interés

■ **OwnCloud** - <https://Owncloud.org>

Plataforma para la gestión de almacenamiento y aplicaciones en línea.

■ **Soporte técnico de Microsoft** - <https://support.microsoft.com/es-es>

Portal que permite consultar multitud de documentos de ayuda sobre cualquier tema de los sistemas operativos de Microsoft. Se puede escribir «Copias de seguridad» para obtener una lista de documentos muy útiles.