TEMA 3: SEGURIDAD PASIVA: RECUPERACIÓN DE DATOS

1. COPIA DE SEGURIDAD....2
1.1 COPIA COMPLETA....2
1.2 COPIA DIFERENCIAL....2
1.3 COPIA INCREMENTAL....3
1.4 OTRAS CLASIFICACIONES....3
2. COPIA DE SEGURIDAD DE LOS DATOS....4
2.1 POLÍTICA DE COPIA DE SEGURIDAD....5
3. MODOS DE RECUPERACIÓN FRENTE A PERDIDAS DEL SISTEMA OPERATIVO....7
4. CREACIÓN DE IMÁGENES DEL SISTEMA....9
5. COPIA DE CONFIGURACIONES ESPECIALES....10
5.1 COPIA DE SEGURIDAD DE UN SERVICIO WEB....10
5.2 COPIA DE SEGURIDAD DE UNA BASE DE DATOS....10
5.3 COPIA DE SEGURIDAD DE MAQUINAS VIRTUALES....10
6. VERSIONES DE DOCUMENTOS, RECUPERACIÓN DE DATOS ELIMINADOS Y BORRADO SEGURO....11
ENLACES INTERESANTES - BIBLIOGRAFÍA....13
EJERCICIOS....14

1. COPIA DE SEGURIDAD

Las copias de seguridad garantizan la disponibilidad y la integridad de la información.

Son útiles para restaurar el sistema operativo, las aplicaciones y los datos en caso de ocurrir algún desastre.

TIPOS DE COPIA:

Dependiendo de la cantidad de ficheros que se almacenan en el momento de realizar la copia:

1.1 COPIA COMPLETA

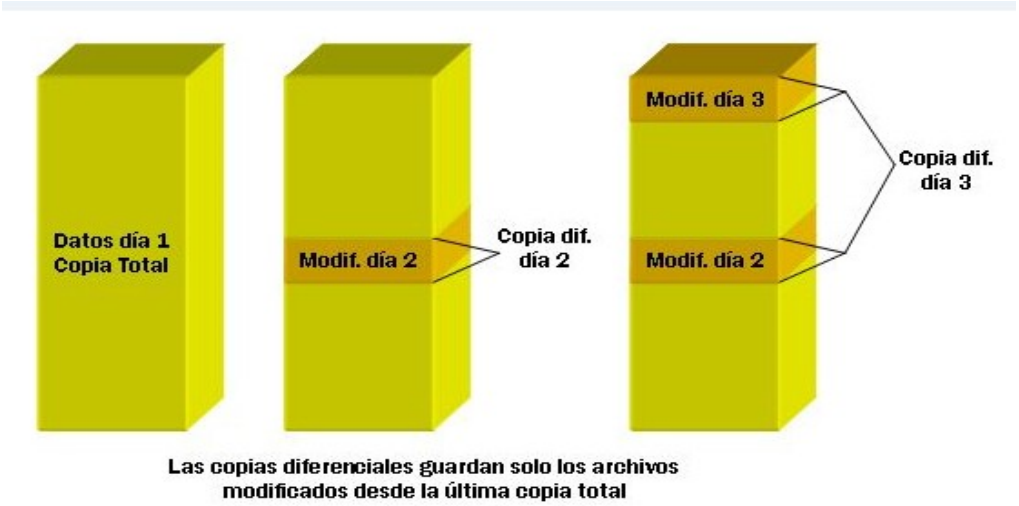
Completa: realiza una copia de todos los archivos y directorios seleccionados.

1.2 COPIA DIFERENCIAL

Diferencial: se copian todos los archivos que se han creado o actualizado desde la última copia de seguridad completa realizada.

Ventaja: Requiere menos espacio y tiempo que la copia completa para hacer la copia.

Inconveniente: para recuperar la copia de un objeto es necesario cargar la última copia completa y después la última copia diferencial.

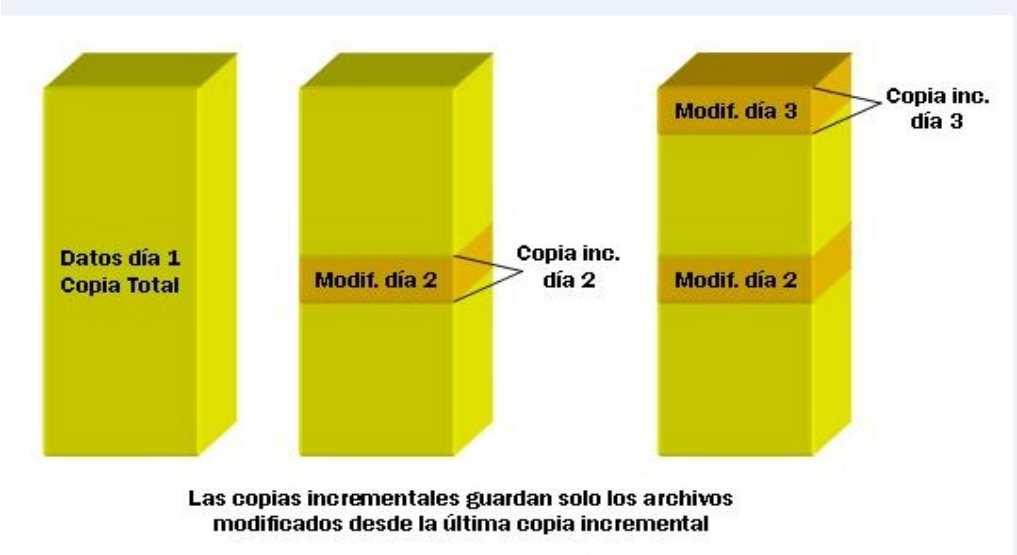


1.3 COPIA INCREMENTAL

Incremental: se copian todos los archivos que se han creado o actualizado desde la última copia de seguridad completa o incremental realizada.

Ventaja: Requiere menos espacio y tiempo que la copia diferencial para hacer la copia.

Inconveniente: para recuperar la copia de un objeto es necesario cargar la última copia completa y todas las copias incrementales posteriores.



1.4 OTRAS CLASIFICACIONES.

Dependiendo del lugar geográfico donde guardamos la copia realizada: **local** o **remota**.

Dependiendo del sistema de almacenamiento, soporte utilizado: **disco duro, disco USB, memoria**, **cinta**, **DVD**,...

Dependiendo de la tecnología de conexión del sistema de almacenamiento: **IDE**, **SATA**, **NAS**, **SAN**, **USB**, **WEB**...

Dependiendo de quien la hace: **automática** (**desatendida**), **manual**.

Dependiendo de si es necesario parar el servicio o no, **copia en caliente**.

Copia **comprimida** o no.

Copia **cifrada** o no.

2. COPIA DE SEGURIDAD DE LOS DATOS

Los datos (la información) generada en cualquier empresa es muy difícil de reconstruir en caso de perdida, imposible en algunos casos

Las copias de seguridad deben almacenarse en un lugar diferente al original.

Es muy común cometer el error de guardar la copia en el mismo soporte que el original o muy cerca del mismo; aunque resulte más cómodo puede causarnos muchos problemas.

¿De qué archivos debemos hacer la copia?

Las copias de seguridad deben realizarse de todos los archivos que sean difíciles o imposibles de reemplazar en caso de pérdida.

¿Dónde debemos hacer las copias de seguridad?

Alejados del soporte donde se encuentran los originales.

La finalidad de la copia de seguridad es poder recuperar los datos en caso de desastre, por tanto, debemos procurar que el desastre no afecte a la copia también.

Cumpliendo las normas de protección de datos de carácter personal y las propias de la seguridad de la empresa igual que los datos originales.

Copia de seguridad de los datos en Windows:

Utilizando el propio sistema operativo o utilizando una herramienta software.

Utilizando herramientas software sobre el sistema operativo: **Cobian Backup**

Nota: Herramientas recomendadas por Incibe

Copia de seguridad de los datos en Linux:

12 formas de hacer copias de seguridad en Linux

Copia de seguridad de los datos en la nube:

Servidores dedicados en Internet para almacenar copias de seguridad o sincronizar con carpetas de nuestro sistema. Servidores de alojamiento de archivos.

Dropbox **SkyDrive** **GoogleDrive** **Box** **Mega** **OneDrive**

2.1 POLÍTICA DE COPIA DE SEGURIDAD

La política de copia debe explicar como deben de hacerse las copias, cuando, que datos se incluyen, donde se guardan, cifrado, responsable de hacerlas, procedimiento de recuperación total o parcial de una copia, responsable de recuperarlas, donde se deja la información recuperada,...

Ejemplo: en una empresa mediana podría ser suficiente con el siguiente esquema de 10 cintas

Una para el backup completo (los viernes)
Cuatro para un backup parcial diario (diferencial o incremental) de lunes a jueves
Cinco para backup completos anteriores: quincenal, mensual, trimestral, semestral, anual.

Las políticas de copia de seguridad deben definir el tipo de copias y la periodicidad de las mismas, así como los soportes en las que se deben realizar y las ubicaciones de los centros de respaldo.

Los **centros de respaldo** son las ubicaciones donde se guardan las copias de seguridad.
Los centros de respaldo deben estar protegidos de la misma forma que los centros de procesos de datos.
Los datos almacenados en los dispositivos de copia deben ser protegidos de la misma forma que los datos originales.

Los errores clásicos en la realización de copias de seguridad son guardarlas en la misma ubicación del original y no etiquetarlas correctamente; ambos errores nos llevan a no poder utilizar la copia en el momento en el que la necesitamos.

Etiquetado correcto de la copia:

Identificador de la copia
Tipo de copia
Fecha
Contenido
Responsable

(Registro) Base de datos que recoge información sobre las copias de seguridad y sus soportes:

Identificador de la etiqueta
Tipo de soporte
Ubicación

(Registro) Base Base de datos que recoge información sobre las restauraciones de copia realizadas:

Fecha de restauración
Incidencia que ha motivado la restauración
Ubicación
Técnico

Política de copia de seguridad:
Toda política de copia de seguridad debe contemplar los siguientes aspectos:

Determinar la persona o **personas responsables** encargados de realizar y mantener las copias de seguridad.
Analizar los **datos susceptibles de ser salvaguardados** en copias de seguridad teniendo en cuenta la frecuencia con la que se modifica o actualiza la información.
Determinar el **tipo de copia a realizar: completa, diferencial o incremental**; en función de los datos a salvaguardar y la periodicidad con la que se modifican.
Determinar la **frecuencia** con la que se realizarán las copias de seguridad. Análisis de la cantidad de información que estamos dispuestos a perder.
Determinar la **ventana de backup** (franja horaria en la que deben realizarse las copias), teniendo en cuenta la duración que cada tipo de copia consumirá.
Determinar el **tipo de soporte** en el que se realizan las copias de seguridad.
Determinar la **ubicación de las copias de seguridad**.
Determinar el **número de copias que se mantienen**, almacenamiento histórico.

Plan de contingencias para la recuperación frente a un fallo:

Análisis de riesgos del sistema.
Estudio de las protecciones actuales
Plan de recuperación antes, durante y después del desastre

Plan de respaldo	**antes**
Plan de emergencia	**durante**
Plan de recuperación	**después**

3. MODOS DE RECUPERACIÓN FRENTE A PERDIDAS DEL SISTEMA OPERATIVO.

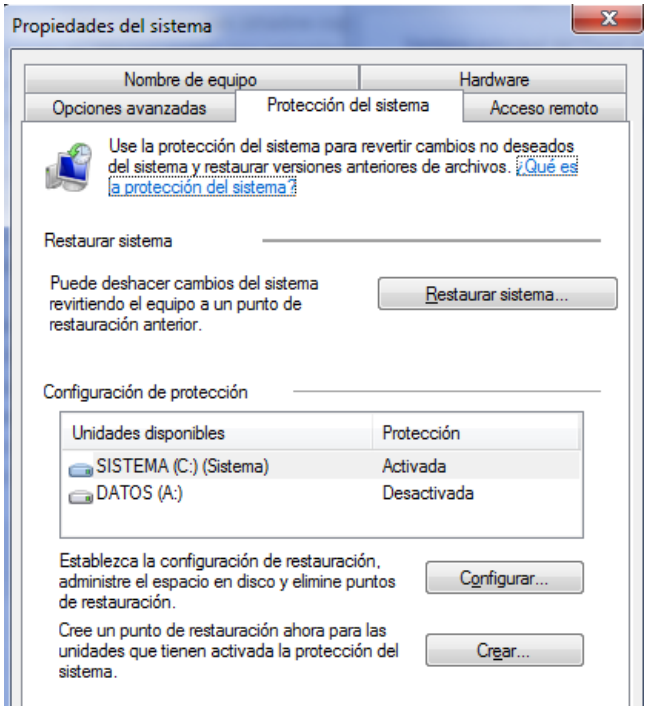
El sistema operativo y los programas instalados en un ordenador son mucho más fáciles de sustituir en caso de perdida que los datos (la información) que generamos con estos programas.

Una imagen del sistema operativo y los programas instalados en un ordenador queda desfasada (desactualizada) muy rápidamente debido a la frecuencia de la actualización del software.

Al igual que realizamos copias de seguridad de los datos, debemos realizar otras del sistema operativo, para así restablecer su correcto funcionamiento lo más rápidamente posible y evitar la instalación del mismo desde cero.

Para ello debemos crear y guardar **puntos de restauración**.

Señalar que los puntos de restauración pueden ocupar mucho espacio.
Restaurar el sistema a un punto de restauración anterior. La restauración a un punto anterior solo afecta a la configuración de los archivos del sistema, programas, archivos ejecutables y el registro; no afecta a los documentos personales, por lo que con dicha operación no podemos recuperar un archivo que hayamos eliminado.
Eliminar los puntos de restauración más antiguos y dejar los más recientes.



Arrancar el equipo con la última configuración válida

Presionando la tecla F8 en el arranque de Windows y seleccionando la opción “Reparar el equipo”.

Recuperación automática del sistema: Utilizando la herramienta del sistema “Copia de Seguridad” y el “Asistente para recuperación automática del sistema” crearemos un disco DVD que utilizaremos para arrancar el sistema en caso de problemas y recuperar la configuración del sistema que teníamos en el momento de realizar la copia.

4. CREACIÓN DE IMÁGENES DEL SISTEMA

La imagen de una partición o de un disco nos permite recuperar tanto el sistema operativo como los datos existentes en el ordenador en el momento de realizar la imagen

Hacer una copia de seguridad del sistema no es tan importante o imprescindible como la copia de los datos, pero nos ahorrará mucho tiempo en caso de tener que reinstalarlo.

Las imágenes del sistema son muy útiles para el caso de tener que preparar muchos equipos con las mismas características hardware y software.

Para hacer copias de seguridad del sistema (que permite su reinstalación de forma más cómoda, sencilla y en menos tiempo) existen aplicaciones especializadas:

Symantec Norton Ghost

clonezilla.org **clonecilla.es** **clonecilla(wikipedia)**

Acronis True Image

FOG project

¿Dónde guardamos la imagen del sistema?

En el mismo disco en una partición diferente (en la partición de datos o en una partición oculta para guardar las imágenes (de uso exclusivo))
En un soporte DVD, USB que nos permita utilizarla cuando la necesitemos
En un servidor de imágenes (FTP)

Procedimiento de **recuperación de imágenes**: desde un soporte conectado al equipo - desde un servidor de imágenes.

Procedimiento de **distribución de una imagen multicast o broadcast**.

Sysprep de Microsoft.

Clonación de discos

5. COPIA DE CONFIGURACIONES ESPECIALES

La copia de seguridad solo será útil si disponemos de un procedimiento de restauración probado.

Algunos de los servicios que corren sobre el sistema operativo utilizan una base de datos para guardar su configuración. Es conveniente, por tanto, realizar una copia de seguridad de dicha base de datos antes de proceder a realizar modificaciones que puedan poner en peligro el correcto funcionamiento del servicio.

La copia de seguridad de la configuración de un servicio solo nos resulta útil si conocemos el ***procedimiento de restauración*** de la misma.

Copia de seguridad del registro:

> **regedit**: para ejecutar la consola de administración del registro
> (botón derecho) exportar: para exportar la configuración que deseamos copiar
> (botón derecho) importar: para recuperar la configuración copiada

Copia de seguridad de la configuración de un servidor: DNS, DHCP, AD, ...

5.1 COPIA DE SEGURIDAD DE UN SERVICIO WEB

Copiar toda la estructura de un servidor web, incluidos los contenidos, que nos permita recuperarnos en caso de desastre (perdida del servidor que está dando el servicio, ataque al servidor que está dando el servicio).

5.2 COPIA DE SEGURIDAD DE UNA BASE DE DATOS

Copiar toda la estructura de un sistema gestor de base de datos y sus datos, que nos permita recuperarnos en caso de desastre (perdida del servidor que está dando el servicio, ataque al servidor que está dando el servicio).

5.3 COPIA DE SEGURIDAD DE MAQUINAS VIRTUALES

Comentar la forma de realizar la copia de máquinas o servicios virtualizados.

Copia de seguridad en caliente de máquinas virtuales.

6. VERSIONES DE DOCUMENTOS, RECUPERACIÓN DE DATOS ELIMINADOS Y BORRADO SEGURO

Podemos configurar el sistema para que almacene versiones anteriores de los documentos con los que trabajamos.

Existen herramientas software que nos permiten recuperar ficheros que hemos borrado en el sistema.

Existen herramientas software que nos permiten borrar documentos en el sistema de tal forma que no puedan ser recuperados.

Cuando borramos un archivo en Windows, normalmente lo que se hace es mandarlo a la papelera de reciclaje. Únicamente cuando se vacía la papelera, el archivo ya no estará visible para nosotros en nuestro sistema operativo.
Pero que no esté visible no significa que no se pueda recuperar.

Estudiar las opciones de configuración de la **Papelera de Reciclaje.**

Estudiar las opciones de configuración del **Volumen de Shadow Copy Service**

Instantáneas de carpetas compartidas que nos permiten:

Recuperar archivos que se eliminaron accidentalmente. Si elimina accidentalmente un archivo, puede abrir una versión anterior y copiarla en una ubicación segura.

Recuperar un archivo que se ha sobrescrito accidentalmente. Si sobrescribe accidentalmente un archivo, puede recuperar una versión anterior del archivo. (El número de versiones depende de la cantidad de instantáneas que haya creado).

Comparar versiones de un archivo mientras trabaja. Puede usar versiones anteriores cuando desee comprobar qué es lo que cambió entre las versiones de un archivo.

Ejercicio:

Crear un fichero para realizar el ejercicio.
Borrar el fichero.
Recuperar el fichero de la papelera de reciclaje, configuración de la papelera de reciclaje.
Borrar el fichero de la **papelera de reciclaje**.
Recuperación de un fichero borrado que no está en la papelera de reciclaje.

Localizar programas para la **recuperación de datos** en discos duros o pinchos defectuosos o dispositivos sobre los que hemos hecho un borrado de ficheros “accidental” y no disponemos de una papelera de reciclaje correctamente configurada.

Borrado seguro: Eliminar permanentemente ficheros o datos temporales.
Los métodos de borrado seguro son distintas forma de sobrescribir la información almacenada en el dispositivo.

eraser	Eliminar permanentemente archivos
ccleaner	Eliminar permanentemente datos temporales

Instalar y probar un programa de borrado seguro, comentar las posibilidades de configuración de dicho programa.

ENLACES INTERESANTES - BIBLIOGRAFÍA

Copia de seguridad (Wikipedia)

Centro de respaldo (Wikipedia)

Imagen de disco (Wikipedia)

Clonación de discos (Wikipedia)

Cobian Backup (Wikipedia)

Clonezilla

Almacenamiento distribuido (Wikipedia)

RAID (Wikipedia)

Cluster de servidores (Wikipedia)

NAS Network Attached Storage (Wikipedia)

SAN Storage Area Network (Wikipedia)

NFS Network File Sistem (Wikipedia)

Samba (Wikipedia) SMB Server Message Block CIFS Comon Internet File SMB (Wikipedia)

DFS Distributed File Sistem (Wikipedia)

Virtualización (Wikipedia)

ProxMox

FOG Project

“Fundamentos de seguridad de redes” – Eric Maiwald – Editorial Mc Graw Hill – ISBN 970-10-4624-2

“El Tao de la monitorización de seguridad en redes – Richard Bejtlich – Editorial Pearson Educación – ISBN 84-205-4600-3

“Seguridad informática – Jose Fabián Roa Buendía – Editorial Mc Graw Hill – ISBN 978-84-481-8396-7

EJERCICIOS

1. Explica las diferencias, similitudes y relación entre los siguientes conceptos:
   Copia de seguridad
   Punto de restauración
   Imagen de una partición
   Imagen de un disco
   Imagen del sistema
   Clonación de un disco
   Congelación de un sistema, partición o disco
   Centro de respaldo
   Servidor de imágenes

2. Explica las **características** que debe tener una buena **copia de seguridad** (Incluidas en la **política de copia de seguridad** de tu empresa).

3. Explica los **tipos de copia de seguridad de datos** que conozcas.

4. Explica la diferencia entre una **política de copia diferencial** y una **política de copia incremental**.

5. Explica la **política de almacenamiento y organización de la información** (datos de la empresa) que recomendarías a una pequeña empresa (5 empleados / 5 PC (iguales), un servidor w2012, una impresora de red y conexión a Internet a través de un router ADSL en todos los puestos).

6. Describe una **política de copia de seguridad** que recomendarías a una pequeña empresa (5 empleados / 5 PC (iguales), un servidor w2012, una impresora de red y conexión a Internet a través de un router ADSL en todos los puestos).

7. Explica el concepto y utilidad de **imagen del sistema** y un ejemplo de herramienta para poder hacerla.

8. Explica la diferencia entre una imagen de disco y una imagen de partición.

9. Si un equipo tiene una **partición de sistema** (donde está instalado el sistema operativo y los programas que utiliza) y una **partición de datos** (donde guardamos el trabajo que realizamos). ¿Cuál es la partición de la que debemos hacer la imagen para recuperar el equipo cuando se estropee? ¿Qué debemos hacer con la otra partición?

10. Explica la utilidad de un **punto de restauración en Windows**.

11. Describe las alternativas que conozcas para la **ubicación de las copias de seguridad.**

12. Explica los mecanismos de **protección y alta disponibilidad** de los equipos de tu empresa.

13. Explica el **protocolo de recuperación total o parcial de una copia de datos**.

14. Explica el **protocolo de recuperación de una imagen del sistema**.

15. Localiza **software** (programas) adecuados para realizar **copias de seguridad** de datos. ¿Cuál recomendarías?

16. Localiza **software** (programas) adecuados para realizar **imágenes del sistema**. ¿Cuál recomendarías?

17. Localiza webs que podamos utilizar para almacenar **copias de seguridad (en la nube)**.

18. Explica los mecanismos de **copia de seguridad de configuraciones especiales** que recomendarías en tu empresa. Ejemplos:
    - **Copia de la configuración de un servicio**: DHCP, AD, DNS…
    - Copia trimestral de datos después de cerrar la contabilidad…
    - Copia de la **base de datos**…
    - Copia en la nube de…

Avanzado

1. **Estudio de contratación de una copia remota**

   Realiza un estudio para la contratación de un ***servicio de copia remota en Internet*** para una pequeña empresa con un volumen de datos susceptibles de copia menor de 50 GB.
   Valoración de las opciones estudiadas y motivación de la propuesta definitiva.

2. **Recuperación de datos y borrado seguro**

   Crear un fichero para realizar el ejercicio.
   Borrar el fichero.
   Recuperar el fichero de la ***papelera de reciclaje***, configuración de la papelera de reciclaje.
   Borrar el fichero de la papelera de reciclaje.
   Recuperación de un fichero borrado que no está en la papelera de reciclaje.
   Instalar y probar un programa de ***borrado seguro***, comentar las posibilidades de configuración de dicho programa.
   Localizar programas para la recuperación de datos en discos duros o pinchos defectuosos.

3. **Gestor de arranque múltiple: GAG**

   Crear una máquina virtual con ***GAG*** como gestor de arranque y con las siguientes características:
   Disco físico 1 (sistemas.vdi):
   XP1 (10GB)

XP2 (10GB)
LD3 (10GB)
Disco físico 2 (datos.vdi) (10GB)
Disco físico 3 (backup.vdi) (10GB)

Situación inicial: el disco backup.vdi contiene una imagen del sistema para una partición XP de 10 GB.
GAG: gestor de arranque para tres posibles sistemas:
XP1: imagen recuperada con clonezilla live desde el disco backup.
XP2: imagen recuperada con clonezilla live desde el disco backup.
LD3: Linux instalado desde la disquetera.
Todos los sistemas deben poder acceder a los discos de datos y backup.

4. TrueNAS

Configurar una máquina virtual con un servidor TrueNAS:

para dar un ***servicio de alojamiento*** a los compañeros de la clase disponible desde equipos Windows y Linux.

para soportar ***PLEX Media Server*** que ofrece servicio en el aula.

Control de acceso a los servicios TrueNAS utilizando cuentas de usuario.

Estudiar otras posibilidades del software TrueNAS.