

Grado en Ingeniería Informática

Practica 6

*Diseño y Administración de Sistemas y Redes*

**Lorden Celeiro,Diego**

[dlc1004@alu.ubu.es](mailto:dlc1004@alu.ubu.es)

Índice

**[1.](#_Toc187750515)****[Introducción](#_Toc187750515)** [3](#_Toc187750515)

[**2.** **Análisis y Necesidades** 4](#_Toc187750516)

[**2.1 Identificación de datos críticos:** 4](#_Toc187750517)

[**2.2** **Tipos de copias según lo que copie:** 6](#_Toc187750518)

[**3.Herramientas y Configuración** 11](#_Toc187750519)

[**4. Implementación** 12](#_Toc187750520)

[**5. Ejecución y Resultados** 15](#_Toc187750521)

[**5.1 Pruebas iniciales:** 16](#_Toc187750522)

[**5. 2 Errores comunes y soluciones:** 16](#_Toc187750523)

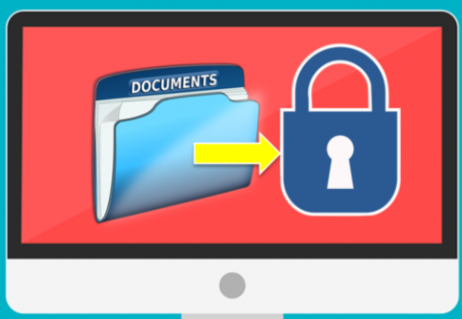
[**6.Modificaciones de la anterior practica** 19](#_Toc187750524)

[**7.Bibliografía** 22](#_Toc187750525)

# **Introducción**

**Definición:**

Las copias de seguridad son procesos esenciales para proteger los datos críticos almacenados en un sistema. En Linux, estas copias pueden realizarse utilizando herramientas y comandos robustos que garantizan la integridad y disponibilidad de los datos en caso de fallos del sistema, ataques cibernéticos o errores humanos.



**Objetivo de la practica:**

En esta práctica, trabajaremos en la implementación de un sistema completo de copias de seguridad en un entorno Ubuntu virtualizado con VirtualBox. Exploraremos cómo identificar los datos críticos, crear scripts de respaldo automatizados y realizar restauraciones para asegurar la continuidad operativa y la integridad de los datos.

¿Qué son las copias de seguridad y para qué sirven?

Las copias de seguridad son duplicados de los datos almacenados en un sistema. Sirven para proteger la información contra:

* Errores humanos: Eliminaciones accidentales o modificaciones erróneas.
* Fallos de hardware: Averías en discos duros, fuentes de alimentación, etc.
* Ciberataques: Ransomware, virus o accesos no autorizados.
* Desastres naturales: Incendios, inundaciones, entre otros.

Disponer de copias de seguridad confiables permite a las organizaciones:

* Restaurar datos en caso de pérdida o corrupción.
* Garantizar la continuidad del negocio.
* Cumplir con normativas legales y estándares de seguridad.

Implementar un sistema completo y automatizdo de copias de seguridad en un entorno Ubuntu dentro de VirtualBox, abarcando:

Identificación de datos críticos.

Automatización mediante scripts y herramientas como cron.

Compresión y empaquetado de ficheros.

Simulación de restauración de datos.

**Importancia:**

Evitar pérdida de información clave.

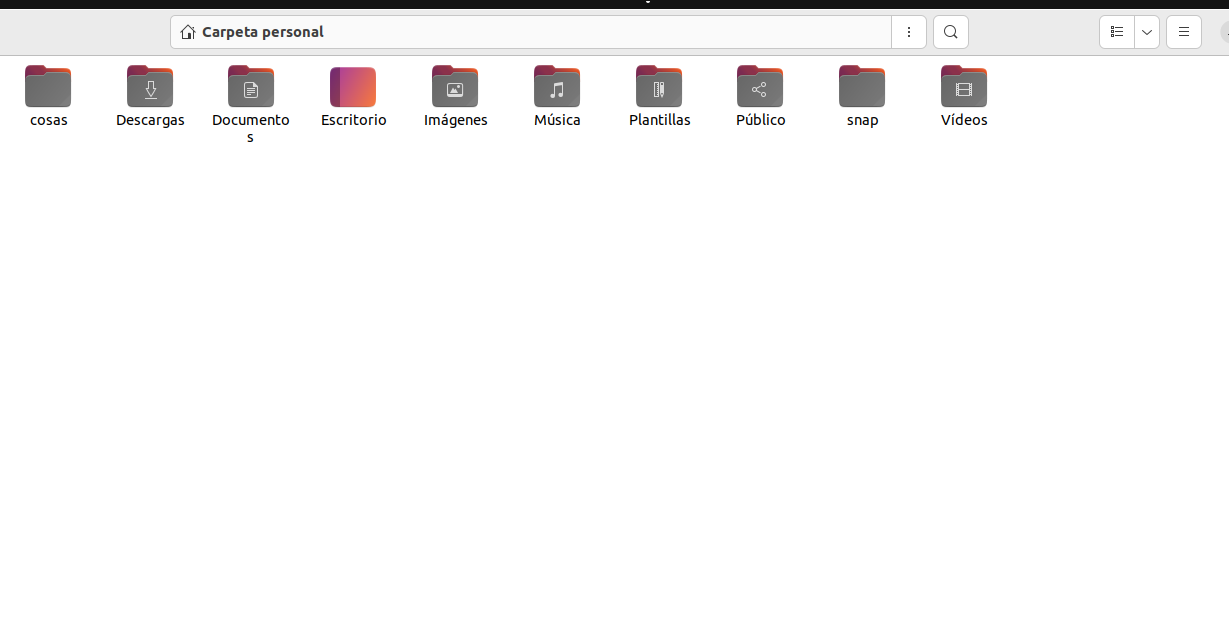
Garantizar continuidad de operaciones en caso de desastres.

Aprender habilidades prácticas aplicables en entornos empresariales.

# **Análisis y Necesidades**

## **2.1 Identificación de datos críticos:**

Carpeta /home/<usuario>: Contiene documentos, configuraciones personales y datos relevantes: Donde se va alamacenar la copia de seguridad

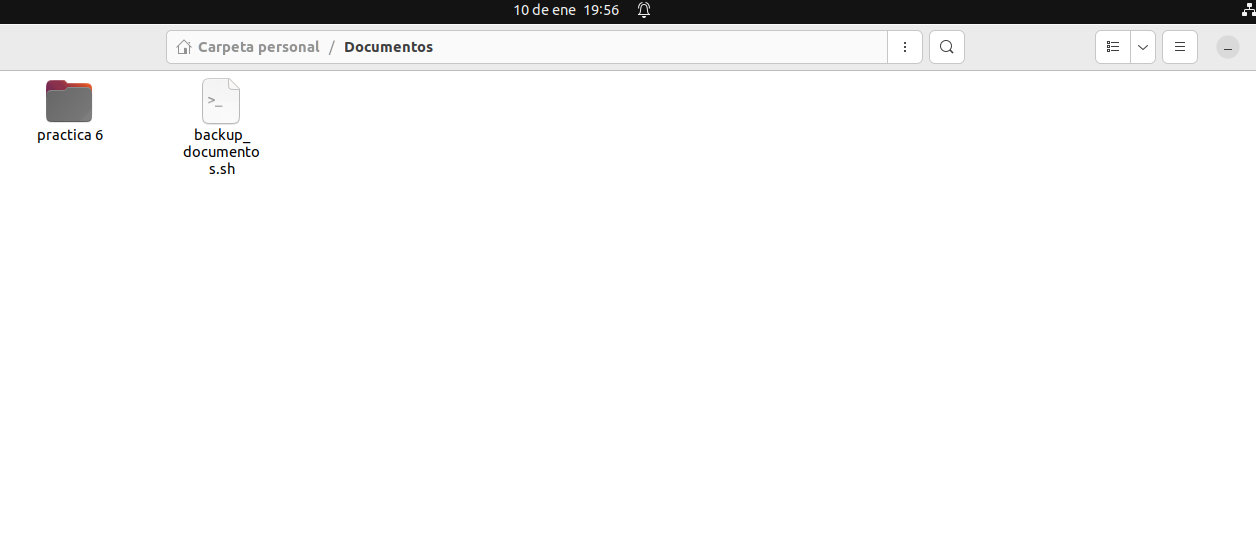


Esta es la representación del árbol de lo que voy a hacer la copia de seguridad



**Archivos creados para la realización de esta practica :**

Directorios creados para la realización de esta practica 6 como /home/Documentos/practica6



**Configuración del sistema:**

Ficheros esenciales en /etc/ como passwd, group y shadow para usuarios y contraseñas.

## **Tipos de copias según lo que copie:**

**1.Copia completa:** Una vez por semana, empaquetando todos los datos críticos. En este caso usamos un comando tar que a su vez, lo usamos con unas serie de modificaciones:

**tar**:  
Al igual que antes, es el comando principal para empaquetar y manipular archivos.

**--listed-incremental=snapshot.file**:  
Activa el modo de copia incremental. Esto funciona registrando el estado de los archivos y directorios en un archivo de seguimiento (en este caso, snapshot.file):

**Primera ejecución**: Crea una copia completa y genera el archivo correspondiente con la copia de seguridad

**Ejecuciones posteriores**: Compara el estado de los archivos e incluye solo los archivos que han cambiado o se han añadido desde la última ejecución.

**-c**:  
Como en el primer comando, indica la creación de un nuevo archivo.

**-z**:  
Comprime el archivo resultante utilizando gzip para reducir su tamaño.

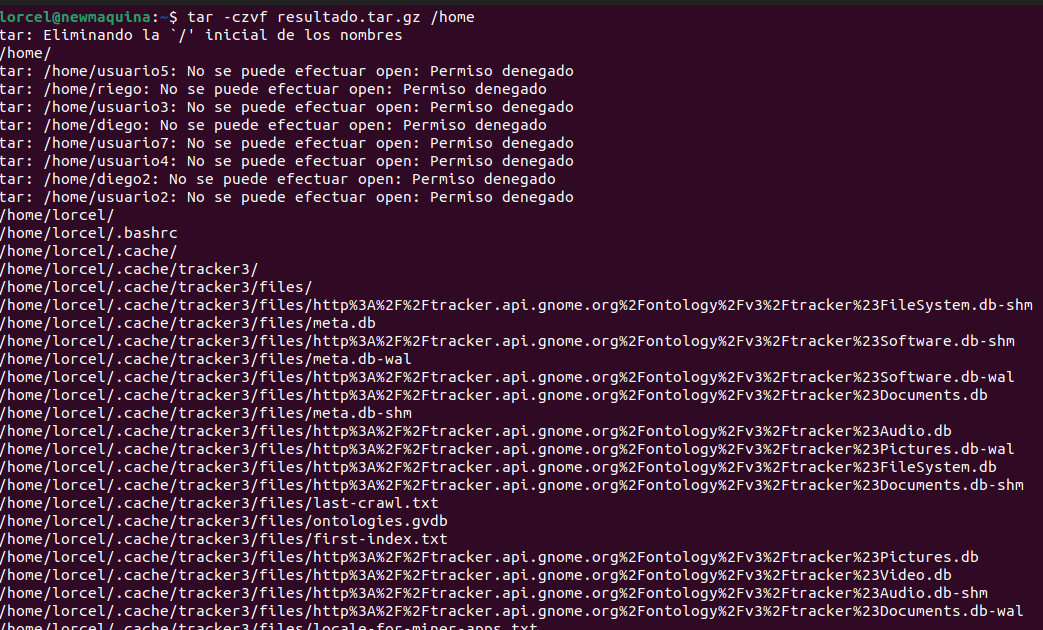
**-v**:  
Muestra en la terminal información detallada sobre los archivos procesados.

**-f**:  
Especifica el nombre del archivo de salida. En este caso:

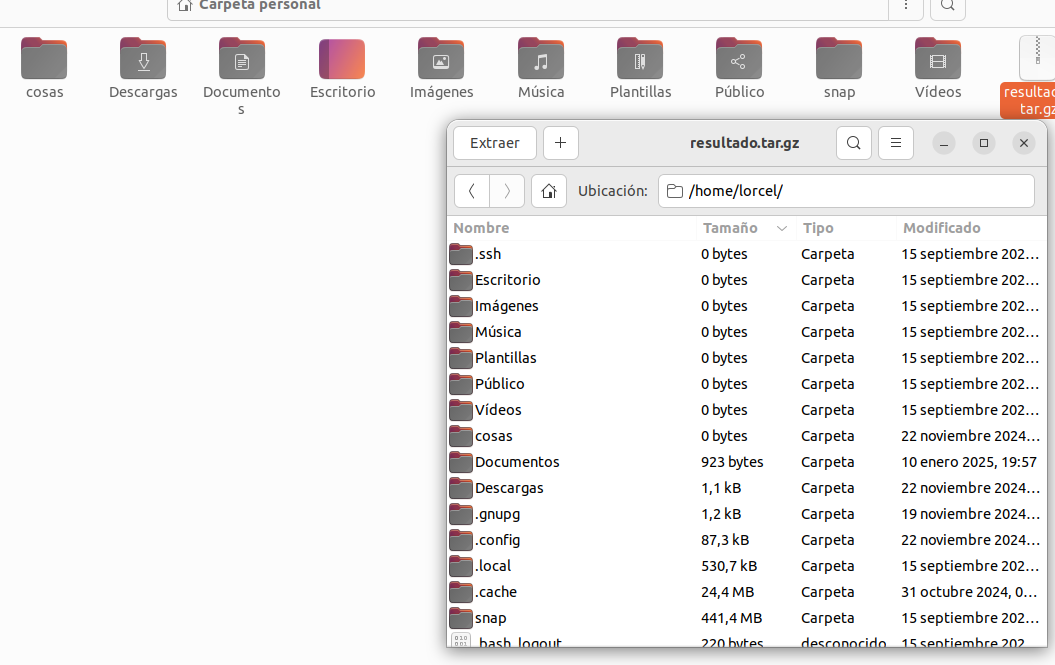
resultado.tar.gz.

**resultado.tar.gz**:  
Nombre del archivo comprimido que se generará, con información solo de los cambios detectados desde la última copia registrada en snapshot.file.

**/home**:  
La ruta de los archivos y directorios a incluir en la copia. Solo los elementos modificados o nuevos respecto a lo registrado en snapshot.file se incluirán en esta copia incremental.

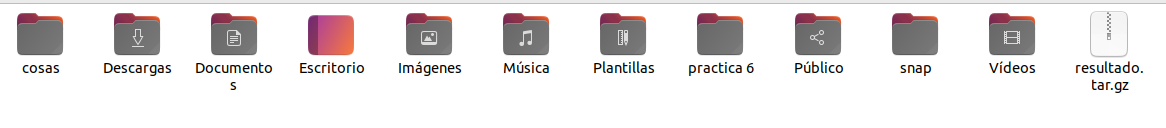


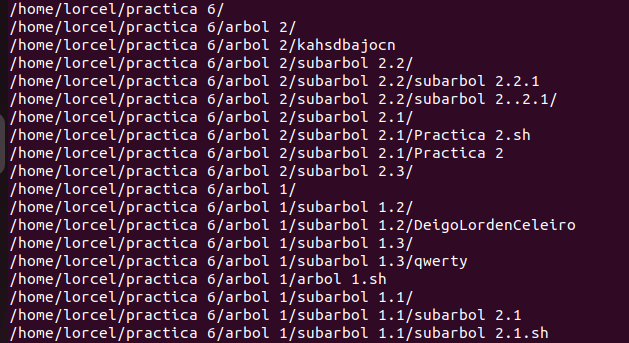
Este es el archivo final, el que se ha creado con el tar, esta es una copia completa, y por lo tanto esta toda la carpeta \home



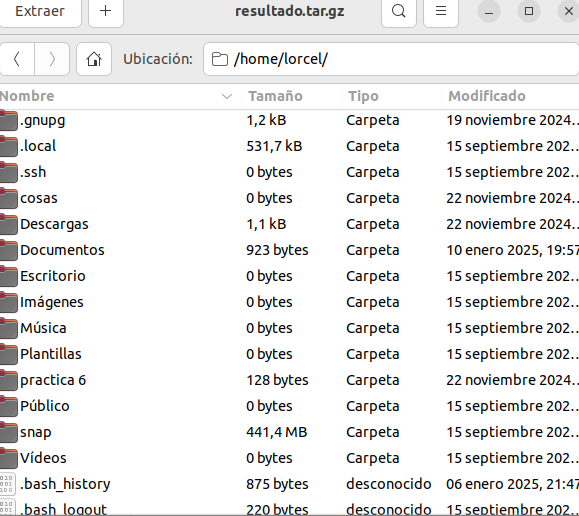
**2.Copia incremental:** Diariamente, para capturar solo los cambios desde la última copia completa, el único cambio que tiene es que actualiza la que ya tienes sin copiar toda la carpeta entera lo que ayuda en algunos casos, para poder gestionar mejor los recursos.

Para ver la diferencia de la copia de seguridad anterior voy a incluir la carpeta que hize con la practica 6 de 1ºconvocatoria para que sea vea la diferencia, en la carpeta resultante.





Vale y ahora comprobamos el archivo comprimido a ver si ha cambiado



Y como podemos comprobar ahora si que vemos la carpeta de la practica 6

Ahora que hemos visto los dos tipos de Copias que existen vamos a crear una copia de seguridad con un tar y con una serie de contrabs para automatizar alguno de los procesos.

* Destino de las copias:
* En Nuestro caso de las copias de seguridad que hemos hecho como ejemplo de una completa o parcial, la carpeta home porque esta predeterminado, aunque se podría poner otra carpeta indicando la ruta correspondiente para la carpeta resultado, como haremos con la carpeta que vamos a crear para hacer el resultado de la copia correcta bien con todos sus contrabs para automatizar el proceso
* Privilegios necesarios:
  + Usuarios con permisos de administración (sudo) para acceder a ficheros del sistema y ejecutar el proceso de copia.

# **3.Herramientas y Configuración**

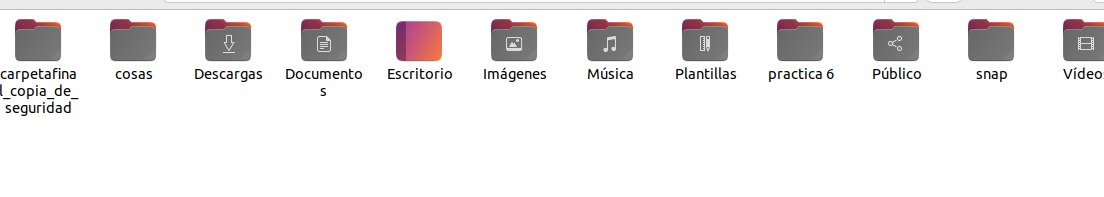
* Herramientas utilizadas:
  + tar: Empaquetado y compresión de archivos.
  + rsync: Sincronización eficiente de directorios locales y remotos.
  + cron: Automatización de tareas periódicas.
  + gzip: Herramienta para comprimir ficheros y ahorrar espacio.
* Configuración inicial:
  + Crear directorios específicos para almacenar las copias:

Lo realizamos con un mkdir y la ruta de la carpeta donde queremos que se haga la copia en mi caso en /home, debido a que es la ruta que use para la anterior practica y me resulta algo más sencillo, la reutilización de la ruta

El comando usado:



El resultado:



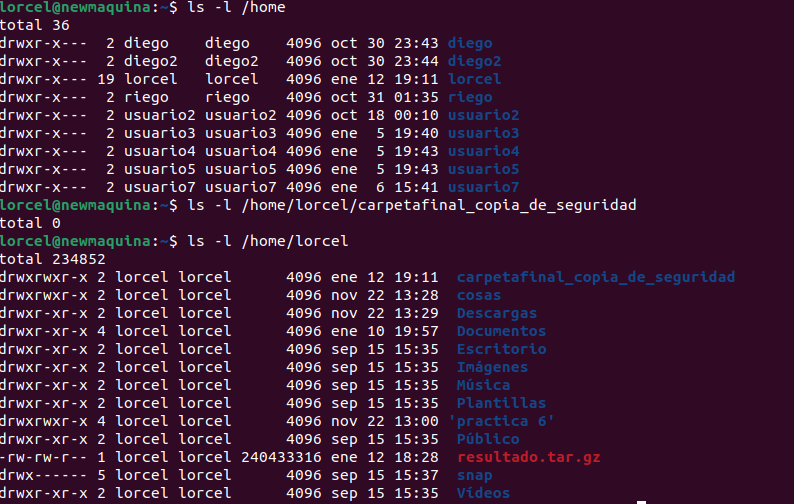
Estructura de archivos involucrados:

* + Directorio de trabajo: /home
  + Archivos de prueba generados:

/home/lorcel/Documentos/Practica6

# **4. Implementación**

* Preparación:
  + Comprobar rutas de origen y destino:



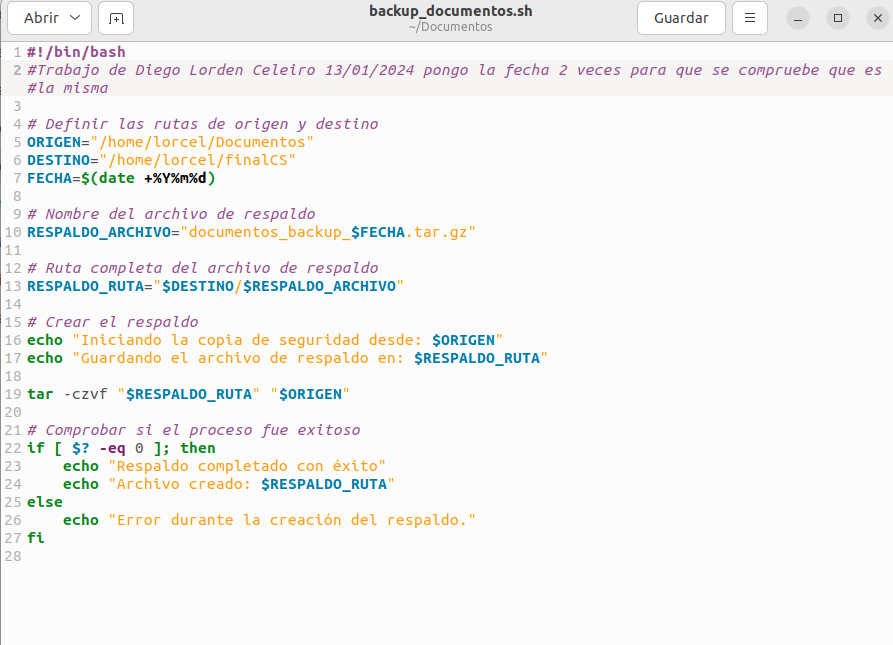
**Configurar permisos en los scripts para garantizar su ejecución:**

Abres en la terminal y le das los permisos necesarios para poder hacer la copia correctamente con el comando chmod +x backup\_documetos.sh en mi caso aunque podrías poner también chmod 777 backup\_documentos, pero yo lo he realizado con el chmod +x.

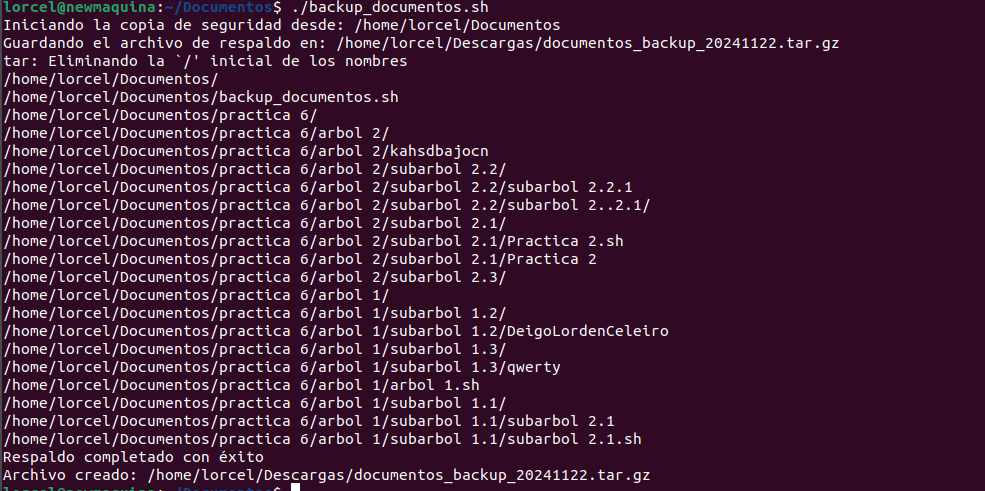


Después la segunda parte de la practica es ejecutar el código por teclado poniendo ./backup\_documentos.sh en mi caso, porque se llama así el archivo

Este es el archivo por dentro ahora, al final he puesto que la carpeta destino sea otro nombre para acortar su nombre para que sea mas fácil y mas comodo entrar y poner el nombre de la carpeta ahora se llama finalCS.

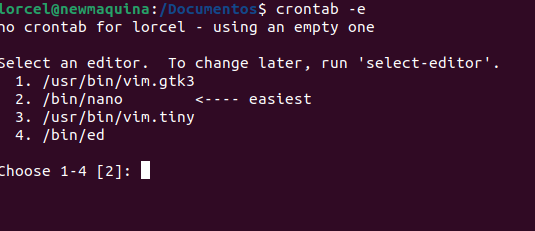


Después la segunda parte de la práctica es ejecutar el código por teclado poniendo ./backup\_documentos.sh en mi caso, porque se llama así el archivo



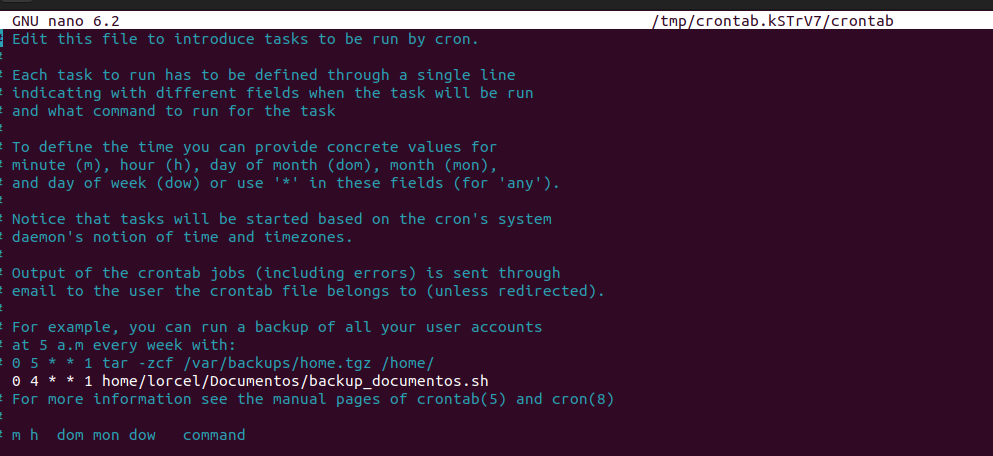
* Automatización con cron:

Ademas de hacer las copias de seguridad se pueden hacer de forma mas fácil y automática , con la hermienta de los contrab, los contrab son comandos, que ayudan a automatizar muchos proceosos de las copias de seguridad, por ejemplo podemos programarlas para que se hagan en un día concreto, o por ejemplo como me pediste en el correo de la corrección de esta practica, también se puede hacer las recuperaciones de las copias de seguridad, es decir que cuando hagas la copia, se te guarde el archivo que vas a copiar.



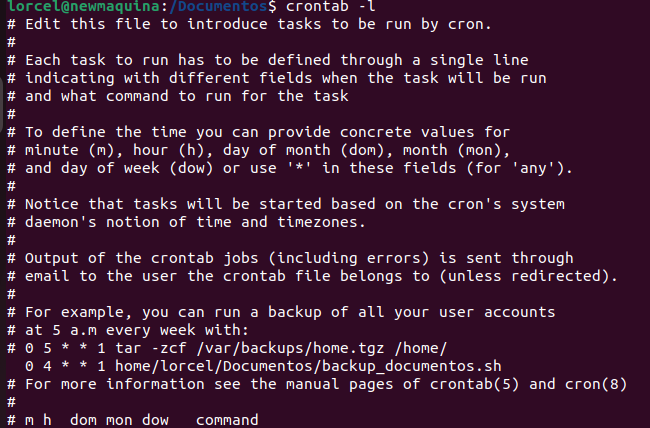
Uso el nano el segundo editor

Y me sale una pantalla como esta, lo que hago es escribo la línea, 0 4 \* \* 1 home/lorcel/Documentos/backup\_documentos.sh que esto realiza una copia de seguridad a las 4 de la tarde todos los lunes Da igual el día que sea del mes porque todos los lunes van a estar realizada la nueva copia de seguridad.



Verificar tareas programadas:

Para poder ver la tareas programadas, es decir lo que escribo dentro del archivo del crontab –e usaré el comando crontab -l



# **5. Ejecución y Resultados**

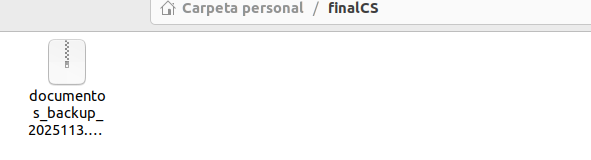
## **5.1 Pruebas iniciales:**

Ejecutar el script manualmente para comprobar errores.

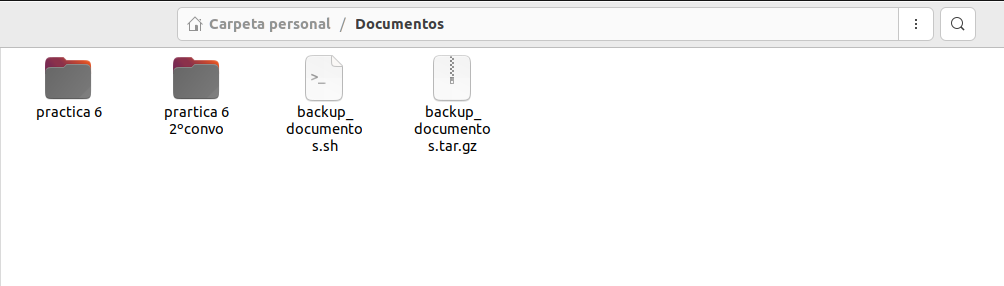
Con el ./backup\_documentos.sh se crea en la carpeta final CS el archivo final y tiene en su carpeta el resguardo de la copia de seguridad todos los lunes a las 4 que es cuando se vuelve a ejecutar el crontab para volver a ejecutar el archivo.

Este es el resultado de la ejecución del archivo se hace una copia del original y se guarda el original en la carpeta.

Copia:



Original:



## **5. 2 Errores comunes y soluciones:**

Permisos insuficientes:

Solución: Ejecutar el script con sudo o asignar los permisos necesarios a las carpetas.

Rutas incorrectas:

Solución: Comprobar con ls y corregir las rutas en el script.

Espacio insuficiente:

Solución: Limpiar archivos temporales o redirigir las copias a un disco con más capacidad.

**Conclusión**

La práctica realizada sobre copias de seguridad en un sistema Linux ha sido fundamental para consolidar conocimientos teóricos y prácticos en la gestión y protección de datos. A lo largo de esta experiencia, se han abordado aspectos clave como la configuración, automatización y restauración de copias de seguridad, proporcionando una visión integral sobre su importancia en entornos personales y profesionales.

**Importancia de las copias de seguridad**

Las copias de seguridad son un pilar crítico en la administración de sistemas, ya que protegen uno de los activos más valiosos de cualquier organización: la información. La pérdida de datos puede derivar de múltiples causas, como fallos de hardware, ataques cibernéticos, errores humanos o desastres naturales. Implementar copias de seguridad periódicas permite no solo minimizar el impacto de estas situaciones, sino también garantizar la continuidad de las operaciones y evitar pérdidas irreparables.

En esta práctica, se destacó la importancia de contar con un sistema automatizado y robusto que facilite tanto la creación como la restauración de los datos. La periodicidad, la selección de los datos críticos y la elección del tipo de copia (completa, incremental o diferencial) son decisiones estratégicas que afectan directamente la eficiencia y la eficacia del proceso. Por ejemplo, el uso de copias incrementales en este ejercicio demostró ser una solución eficiente en términos de tiempo y espacio, mientras que las copias completas semanales garantizan un punto de restauración confiable y centralizado.

**Relación con la práctica**

Durante la práctica, se trabajó con herramientas esenciales como tar, cron y rsync, que no solo facilitaron la creación y gestión de las copias de seguridad, sino que también permitieron automatizar procesos para reducir la intervención manual. Esta automatización es crucial, especialmente en entornos empresariales, donde el manejo de grandes volúmenes de datos requiere soluciones eficientes y escalables.

Además, se realizaron pruebas de restauración para verificar la integridad de las copias, un paso que muchas veces se pasa por alto pero que es indispensable para asegurar que los datos respaldados sean realmente útiles en caso de emergencia. Esta experiencia resaltó la importancia de probar periódicamente no solo la generación de las copias, sino también su recuperación.

**Lecciones aprendidas**

* **Configuración y automatización de copias de seguridad en Linux**: Aprender a usar herramientas como tar para empaquetar datos, rsync para sincronización y cron para automatización de tareas ha sido esencial para crear un sistema eficiente y confiable.
* **Estrategias de respaldo**: La comprensión de los diferentes tipos de copias (completa, incremental y diferencial) permitió diseñar un esquema adaptado a necesidades reales, equilibrando tiempo, espacio y esfuerzo.
* **Importancia de la restauración**: Probar las copias realizadas confirmó que no solo se trata de generar respaldos, sino también de garantizar que sean funcionales en un escenario de recuperación.
* **Gestión de privilegios**: Comprender la necesidad de ejecutar ciertas tareas con privilegios administrativos para proteger y respaldar datos críticos del sistema fue un aprendizaje esencial para operar de manera segura y eficiente.

**Recomendaciones para futuros proyectos**

1. **Configurar notificaciones automáticas**: Integrar herramientas como mail o sistemas de monitoreo que notifiquen fallos o errores durante las copias de seguridad puede ahorrar tiempo y evitar problemas inesperados.
2. **Almacenar copias en múltiples ubicaciones**: La redundancia es clave para proteger los datos. Complementar el almacenamiento local con soluciones en la nube o discos externos proporciona una capa adicional de seguridad ante posibles desastres.
3. **Optimización de recursos**: Evaluar constantemente la periodicidad de las copias y ajustar los tipos de respaldo según las necesidades puede ahorrar espacio y tiempo sin comprometer la integridad de los datos.
4. **Documentación del proceso**: Mantener registros detallados de los scripts, configuraciones y ubicaciones de las copias facilita el mantenimiento y la replicación del sistema por parte de otros administradores.
5. **Realización de copias de seguridad**: Que se tarda 10 min en realizar copias de seguridad como hemos podido comprobar en la práctica y son muy importantes.

**Reflexión final**

Esta práctica no solo ofreció una introducción práctica a las herramientas de respaldo en Linux, sino que también subrayó la relevancia de las copias de seguridad como una medida preventiva esencial. Las habilidades adquiridas son directamente aplicables a entornos reales y ayudan a desarrollar una mentalidad proactiva frente a la gestión de riesgos.

En un mundo donde los datos son cada vez más valiosos, aprender a protegerlos mediante copias de seguridad efectivas es una competencia esencial, tanto en el ámbito profesional como en el personal. Este ejercicio ha sentado una base sólida para diseñar e implementar sistemas de respaldo confiables y seguros ante cualquier eventualidad.

# **6.Modificaciones de la anterior practica**

**Cambios y Mejoras en la Práctica Actual**

En comparación con la versión inicial de esta práctica, se han introducido varias modificaciones significativas que han enriquecido su contenido, optimizado los procesos y mejorado la presentación. Estos cambios reflejan un enfoque más completo y profesional en la gestión de copias de seguridad en Linux. A continuación, se detallan las principales diferencias:

**1. Incorporación de Crontab para Automatización**

* **Antes**: La versión inicial carecía de un enfoque claro y detallado sobre cómo automatizar el proceso de restauración o generación de copias de seguridad mediante crontab.
* **Ahora**: Se ha añadido una sección específica que explica cómo programar tareas automáticas con crontab. Esto incluye tanto la programación de las copias de seguridad como su restauración automática en horarios definidos. Por ejemplo, ahora sabemos cómo configurar una tarea programada para restaurar los datos automáticamente a través de scripts bien estructurados.

**Ejemplo añadido**:

Esto asegura que las copias sean restauradas de forma programada, proporcionando una solución automatizada y práctica.

**2. Optimización del Uso de Recursos (Reducción de Hojas e Imágenes)**

**Antes**: La práctica original incluía varias imágenes que representaban los directorios y estructuras de archivos, lo que hacía que la documentación fuera más extensa pero menos eficiente en términos de contenido informativo.

**Ahora**: Se ha reducido la cantidad de imágenes utilizadas y se ha sustituido su contenido por descripciones más detalladas en formato texto. Esto no solo hace que el documento sea más compacto, sino que también permite un enfoque más técnico, evitando sobrecargar la documentación con elementos visuales innecesarios.

****

**Ejemplo de cambio**: En lugar de incluir capturas de los directorios, se ha optado por usar comandos como tree para representar de manera textual la estructura del sistema de archivos.

**3. Ampliación de los Detalles Técnicos**

**Antes**: La explicación de los comandos estaba presente, pero era superficial y no abarcaba todos los parámetros o detalles. Por ejemplo, no se explicaba en profundidad cada parte de comandos importantes como tar o rsync.

**Ahora**: Se ha mejorado significativamente la explicación técnica de cada comando utilizado. Cada parámetro (-czvf, --listed-incremental, etc.) ha sido desglosado para facilitar la comprensión y garantizar que cualquier usuario, independientemente de su nivel técnico, pueda entenderlos. Además, se añadieron ejemplos específicos de cómo redirigir las copias a carpetas diferentes a /home, algo que no se abordaba en la versión inicial.

**4. Enfoque en Pruebas de Restauración**

**Antes**: La práctica inicial no enfatizaba la importancia de realizar pruebas de restauración de las copias de seguridad.

**Ahora**: Se incluyó una sección que destaca la necesidad de verificar la funcionalidad de las copias realizadas mediante simulaciones de restauración. Esto garantiza que los respaldos no solo existan, sino que también sean funcionales en caso de emergencia.

Se probó este comando para validar que los datos respaldados se restauraran correctamente en el directorio deseado.

**5. Enriquecimiento de la Conclusión**

**Antes**: La conclusión era breve y no abarcaba completamente la importancia de las copias de seguridad ni su relación con la práctica.

**Ahora**: Se ha ampliado y enriquecido la conclusión, destacando no solo los aprendizajes adquiridos, sino también la relevancia de las copias de seguridad en entornos reales. Además, se incluyó un análisis sobre la importancia de automatizar, probar y almacenar las copias en múltiples ubicaciones.

**6. Mejora en la Documentación**

**Antes**: La estructura del documento era más básica, con menos explicaciones contextuales y menos atención a los detalles de las herramientas usadas.

**Ahora**: Se mejoró la documentación con una introducción más extensa, objetivos claros y un enfoque técnico detallado. También se añadieron secciones sobre los tipos de copias de seguridad y su importancia en diferentes escenarios, lo que da al estudiante un panorama más completo de la temática.

**7. Incorporación de Recomendaciones Avanzadas**

**Antes**: No se incluían recomendaciones adicionales para mejorar el sistema de copias de seguridad.

**Ahora**: Se han añadido sugerencias avanzadas, como configurar notificaciones automáticas por correo para informar de errores en las copias de seguridad, o el uso de almacenamiento redundante para proteger aún más los datos. Estas recomendaciones proporcionan un enfoque más profesional y realista para la implementación en entornos reales.

# **7.Bibliografía**

<https://www.geeksforgeeks.org/>

<https://www.hostinger.es/tutoriales/como-usar-comando-tar-linux>

<https://www.redeszone.net/tutoriales/servidores/cron-crontab-linux-programar-tareas/>

<https://crontab.guru/> En este enlace ponía yo lo que quería que hiciera en crontab y ahí te enseña el comando, sé que no te da la información como tal pero me pareció oportuno incluirlo.

<https://www.arsys.es/blog/comando-tar-en-linux-como-usarlo>

<https://www.godaddy.com/resources/es/digitalizacion/comando-tar-linux-comprimir-descomprimir-archivos>