

Seguridad Informática
Almacenamiento de la información

Backup



Autor
Javier Mercillo Marín

1 Introducción

Las copias de seguridad son réplicas (copias) de datos que nos permiten recuperar la información original en caso de haberse perdido. A diferencia del RAID, no hace que la información no se pierda, sino que hace que podamos rescatar la última información guardada.

Hay dos máximas que deberían ser cumplidas a la hora de hacer backups, que son:

- Las copias de seguridad **jamás** debería ser **guardada cerca** del dispositivo original que contiene la información.
- Cada copia de seguridad, **jamás** debería ser **borrada** (aunque esto, ..., es más bien imposible).

Alguna de las posibles causas que hacen que podamos perder información pueden ser, entre otras, las siguientes razones:

Causa	¿Lo arregla el RAID?	¿Lo arregla el Backup?
Por avería del dispositivo de almacenamiento	Sí	Sí
Por error humano	No	Sí
Se modificó un documento por algún programa sin ser conscientes	No	Sí
Virus informático	No	Sí
Degradación de un sistema operativo o de una base de datos	No	Sí
Intrusismo que comprometa la integridad de los datos	No	Sí
Una catástrofe natural (como incendio) o robo	No	Sí

Hay ciertos aspectos que hacen plantearnos necesidades para tener un plan de copias de seguridad.

- **Empresa o particular:** el coste económico que puede suponer para una empresa la pérdida de información le puede llevar a la quiebra.
- **¿Datos propios o de clientes?:** no es lo mismo responsabilizarse de nuestra propia información, que de los datos de los clientes, que nos están pagando por su custodia o gestión.
- **Datos de carácter personal:** sujetos a planes específicos en función del nivel que marque la LOPD.

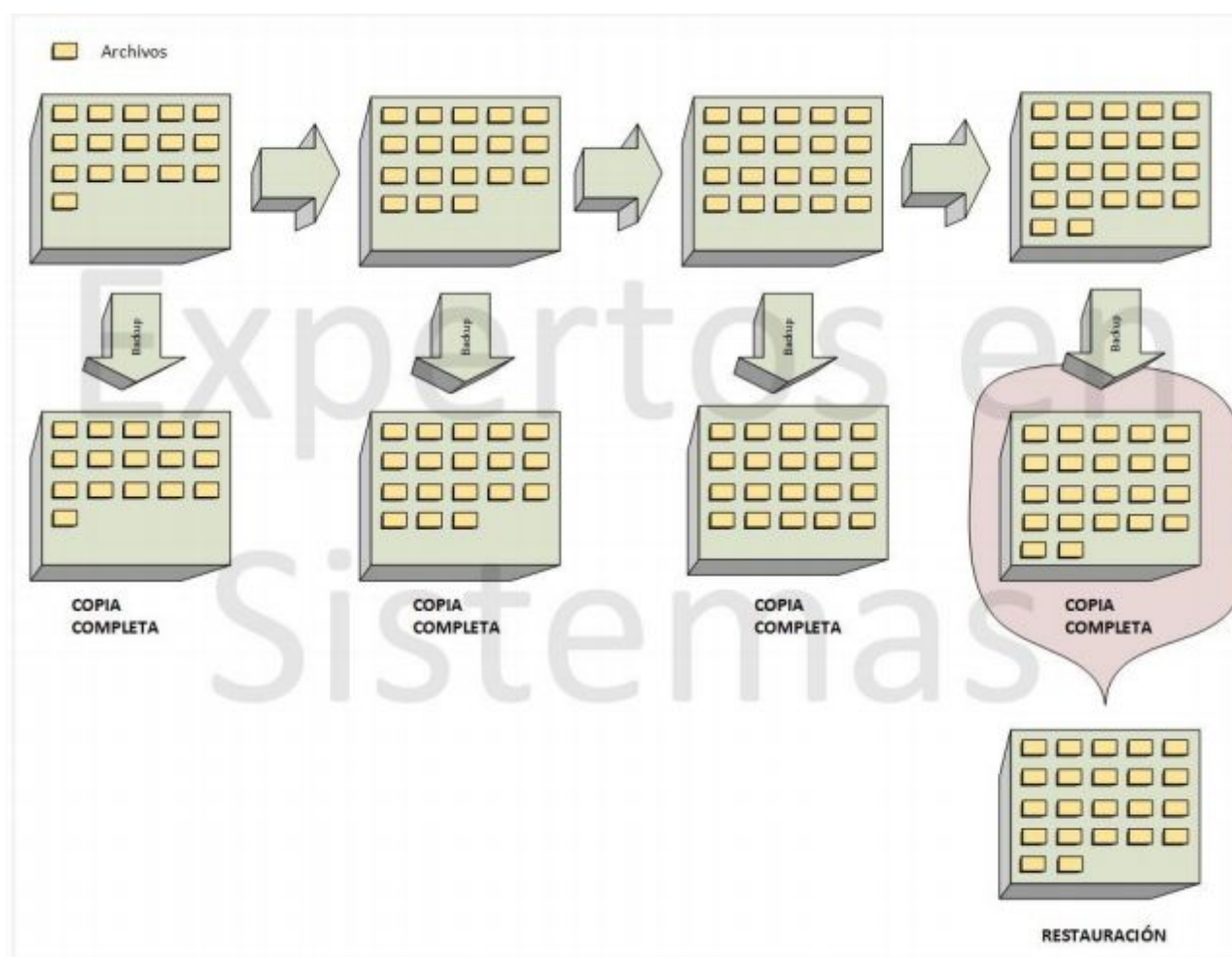
- **Presencia de sistemas preventivos complementarios:** discos RAID, sistemas de alta disponibilidad...
- **Ámbito necesario de restauración:** ¿Hasta qué margen de tiempo hacia atrás podría ser necesario llegar?
- **Tecnologías y plataformas:** dependiendo de la plataforma y/o tecnología se necesita un software o hardware específico, lo cual conlleva un coste económico asociado.
- **Horario:** en el que se realiza los backups, normalmente durante la noche, en el que los usuarios y aplicaciones requieren una menor disponibilidad.
- **Un plan de pruebas de restauración:** nos permitirá asegurar que el plan de copias de seguridad está funcionando correctamente, además de planificar la ejecución periódica del mismo.
- **Custodia de soportes externos y permisos de acceso:** persona responsable y técnicos encargados del proceso, y asignar los permisos adecuados para las diferentes tareas.
- **Garantizar la integridad, confidencialidad y disponibilidad:** tienen que tener las mismas garantías que antes de ser respaldadas.
- **¿Cada cuánto tiempo cambia el contenido?** No es lo mismo realizar backups de un contenido que evolucione constantemente, que de un repositorio cuyas modificaciones se realicen a muy largo plazo.
- **Ubicación de las copias:** no se deben almacenar en el cajón del informático. Caja fuerte, cámara ignífuga o una ubicación fuera del edificio.
- **Presupuesto:** conocer el presupuesto con el que se cuenta es muy importante, ya que de él dependen todos los puntos anteriores.

1.1 Tipos de copias de seguridad.

Existen varios tipos de copias de seguridad. Las tres más comunes se recogen en este apartado.

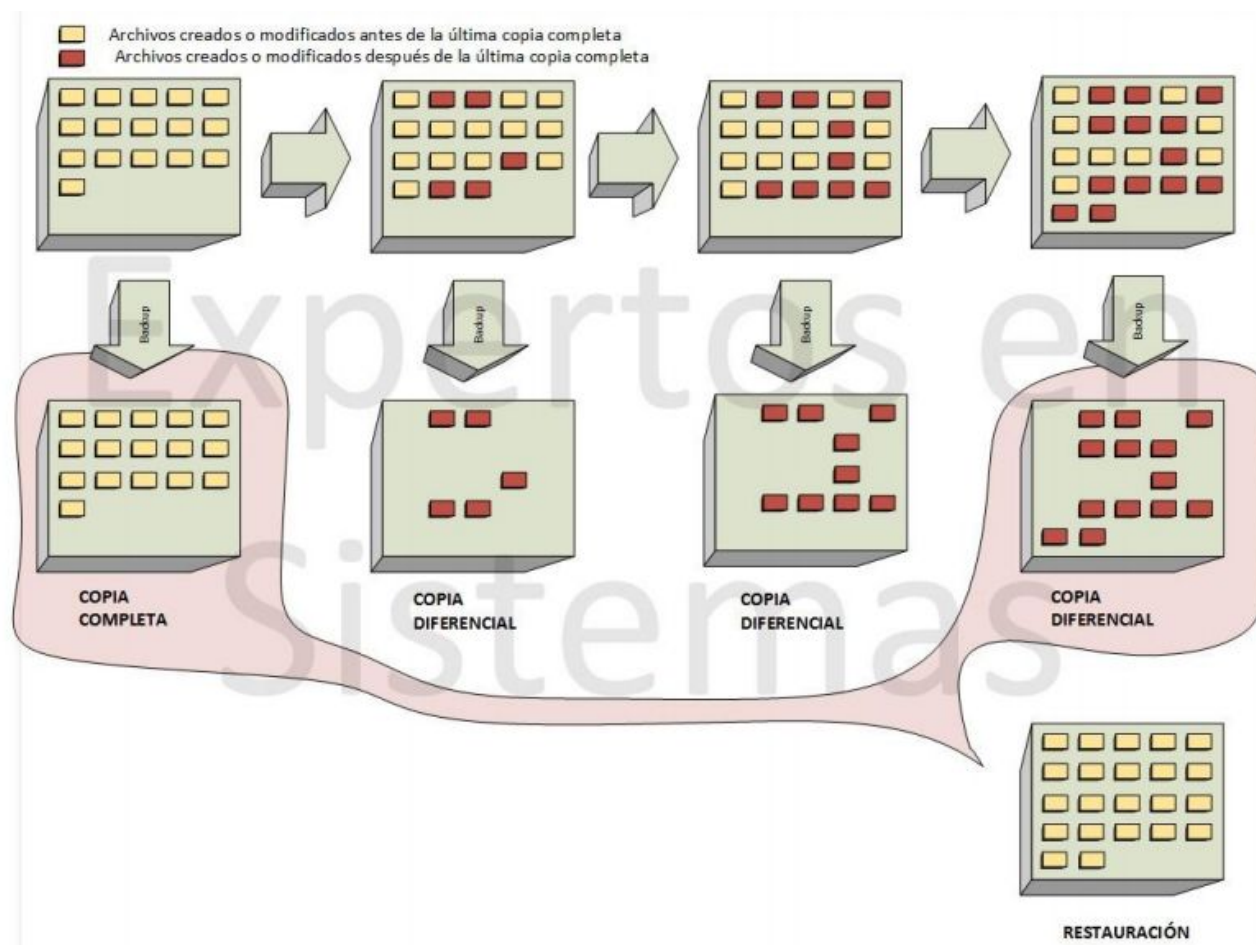
1.1.1 Copia completa

La copia completa, total o íntegra es un backup completo de todos los archivos seleccionados en el plan de copias. Cada vez que se realiza una copia, el sistema operativo pone el bit de copia a 0, para identificar que se le ha realizado un respaldo.



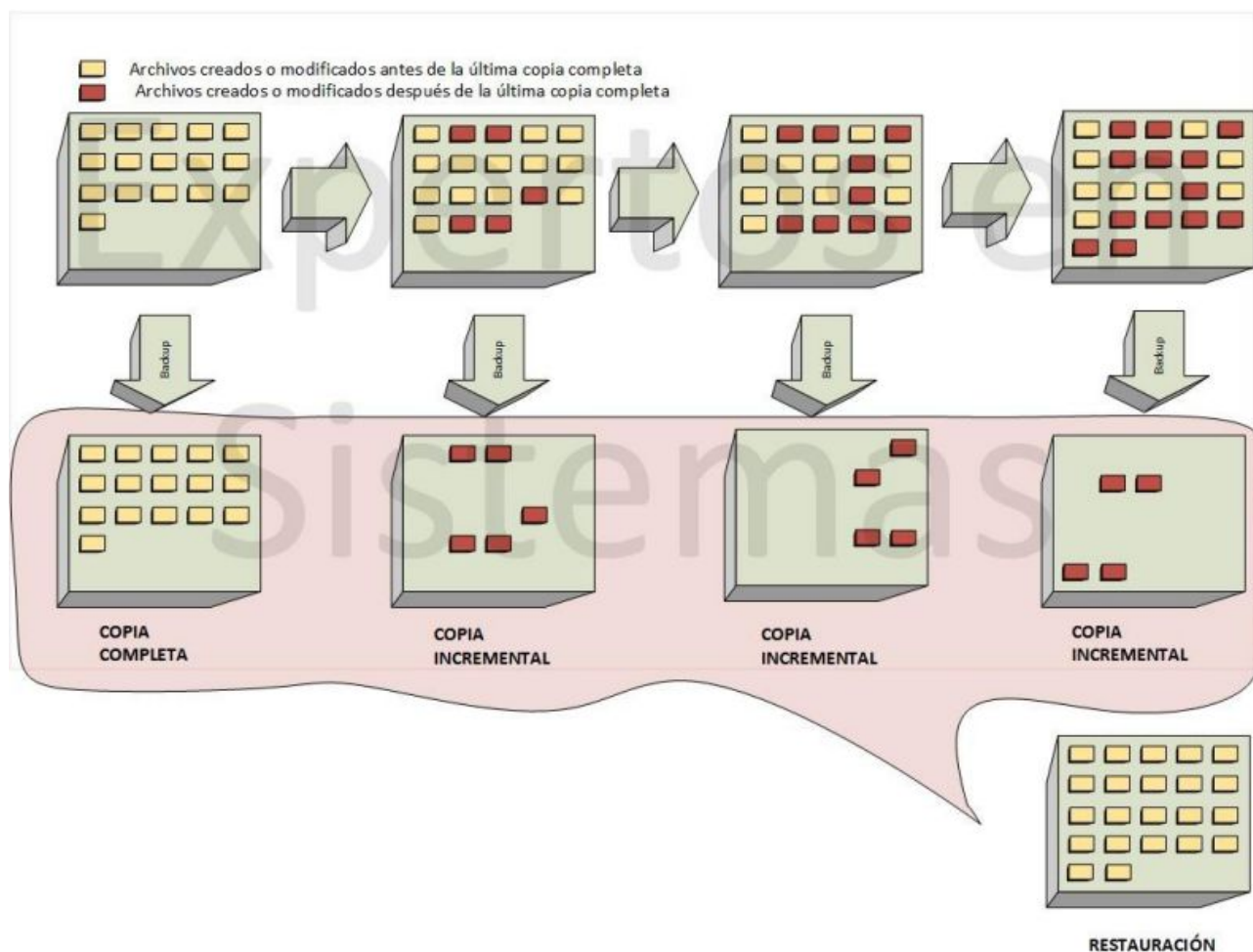
1.1.2 Copia diferencial

Se copian solamente los datos que han sido modificados desde la última copia de seguridad completa. El proceso se fija en el bit de modificación, y sólo copia el archivo en caso que éste se encuentre a 1.



1.1.3 Copia incremental

Se trata del tipo de copia que menos capacidad necesita, ya que sólo almacenará la información que haya sido modificada desde la última copia de seguridad realizada, ya sea completa, diferencial o incremental.



1.2 Recomendaciones sobre el tipo de copia a realizar

Con estas tres técnicas a mano, se nos plantea la pregunta ¿Qué sistema es mejor? Eso depende de los datos que queramos mantener. Se pueden ofrecer los siguientes consejos:

- Volumen de datos no muy elevado (menos de 10GB) → completa
- Volumen de datos muy elevado pero pocas modificaciones → completa + diferenciales
- Volumen de datos muy elevado y muchas modificaciones → completa + incrementales
- Sistemas de copia mixtos (ejemplo):
 - Planificación
 - Todos los días 1 de cada mes, a las 23:00h → copia de seguridad total.
 - Todos los viernes a las 23:00h → copia de seguridad diferencial desde la copia de día 1.
 - Todos los días (excepto los viernes y el día 1) a las 23:00h → copia de seguridad incremental desde la copia del día anterior.
 - Con esta planificación nos aseguramos disponer de copia de seguridad diaria. En caso de desastre deberíamos recuperar la copia total, la última diferencial y todas las incrementales desde la última diferencial.

1.2.1 Utilizar compresión?

Otro factor importante, es si utilizamos o no compresión en las copias que hagamos. Usar la compresión tiene las siguientes características:

- Ventajas
 - El envío de la copia se realiza más rápidamente.
 - El tamaño de la copia es menor.
 - La propia compresión garantiza la integridad de los datos.
- Inconvenientes
 - El empaquetamiento de la información tarda más.
 - La restauración puede tardar más.

1.3 Políticas de copias de seguridad

Las políticas de copias de seguridad deben definir:

- Determinar las personas responsables de las copias y restauraciones.
- Los datos que se copiarán, analizando cuales son lo más importantes y difíciles de recuperar.
- El tipo de copia, que dependerá del volumen de datos que se manejan.
- Periodicidad de la misma, teniendo en cuenta cuanta información estamos dispuestos a perder.
- Soporte para su realización.
- Ubicación de los centros de respaldo.
- La ventana de backup: franja horaria donde se realizarán las copias.

1.3.1 ¿Qué datos hay que guardar?

Otra pregunta que nos puede venir es, ¿Que cosas debo guardar en un backup? Las recomendaciones a esta pregunta son las siguientes

- Información que hace que el equipo funcione correctamente
 - Archivos del sistema operativo.
 - Archivos de configuración del sistema.
 - Logs del sistema.
- Los datos que son únicos o privados.
 - Carpetas personales de los usuarios.
 - Otros de interés

1.3.2 ¿Cómo etiquetar las copias?

Para realizar las copias hay que seguir cierto orden, si no, el caos se apoderará de nuestro sistema y podría inducirnos a errores. Esto nos lleva necesariamente a que llevemos un protocolo de etiquetado y registro de acciones realizadas.

Una etiqueta correcta debería incluir:

- **Identificador de la copia:** Cadena alfanumérica que identifique de forma unívoca la copia
- **Tipo de copia:** Completa, diferencial o incremental.
- **Fecha de realización de la copia:** 22 de Septiembre 2012.
- **Contenido:** Siempre en clave tanto en la etiqueta como dentro de la copia.
- **Responsable:** Técnico que realizó la copia, para posibles consultas posteriores.

Aunque lo que se acaba de enumerar es importante para una empresa, para nuestro hogar es normal que nos relajemos un poco. Aun así, debería haber alguna nomenclatura significativa para nosotros, como por ejemplo:

- CopiaTotal_etc-home_13feb15.tar.bz2
- CopiaDiferencial_etc-home_13feb15-20feb15.tar.bz2

1.3.3 ¿Cómo registrar las copias?

Igualmente se debe llevar un registro exhaustivo de las copias de seguridad y restauraciones realizadas. Este registro debe incluir al menos:

- **Identificador** de la etiqueta de la copia.
- **Soporte** donde se ha realizado la copia.
- **Ubicación** de la copia.

Y por otro lado se debe llevar un registro de las restauraciones realizadas:

- **Fecha** de restauración.
- **Incidencia** que motivó la restauración.
- **Ubicación** del equipo donde se restaura la copia.
- **Técnico** que realiza la restauración

1.4 Soportes para las copias de seguridad

Existen varios tipos de soportes para poder guardar las copias de seguridad, cada uno con sus propias características que lo hacen más idóneo que otro. Podemos encontrar:

- **DVD** (Digital Versatile Disk)
 - Copias de seguridad de usuario particulares.
 - Se trataba del elemento más económico, en la actualidad, casi se puede comparar con el de los discos duros.
 - Sus capacidades no son muy elevadas: DVD 4,7 o 8,5GB
 - Poca durabilidad. En pocos meses o años terminan siendo posavasos.
- **Unidades de cinta magnética**
 - El más utilizado en empresas de tamaño medio y pequeño.
 - Método proporcionalmente más económico.
 - Altamente fiable, usado alrededor de 30 años.
 - Aconsejable para grandes volúmenes de datos.
 - Velocidad de transferencia de hasta 400MB/s y capacidades de 2,5TB, permitiendo hasta 6TB con comprensión hw.
 - Posibilidad de librerías robóticas con cambio automático de cintas.
 - Algunos cuentan con la posibilidad de lectura de códigos de barras, que agiliza y optimiza la catalogación de medios.
- **Copias de seguridad basadas en discos duros**
 - Gracias al abaratamiento de estos dispositivos, ahora cabe la posibilidad de realizar los backups en unidades de discos duros.
 - Su coste puede variar dependiendo del tipo. Desde los más baratos SATA, pasando por los SCSI, hasta los rápidos discos en fibra óptica.
 - Para uso doméstico o pequeñas empresas es común realizar copias en discos USB externos incluso en memorias flash.
- **Backups en la nube**
 - Ventajas:
 - Reducción en la necesidad de disponer de una infraestructura local.
 - Disminución de los costes (hw, sw, recursos técnicos)
 - Coste basado en el almacenamiento utilizado.
 - Externalización de la información → garantiza su supervivencia en caso de un desastre.
 - Inconvenientes:
 - Necesidad de ancho de banda.
 - Problemas de seguridad.
 - La restauración y la integración con los sistemas de información.
 - Solución adecuada para copias de seguridad de dispositivos móviles y oficinas remotas.
- **Soluciones mixtas de backup**
 - Debido a las ventajas e inconvenientes de las distintas opciones, una buena forma de obtener una solución adoptada a nuestras necesidades es utilizar una solución mixta.
 - **D2D2T** – disk to disk to tape. Se realiza un primer backup sobre discos de tipo NAS, SAN... A su vez este contenido es salvaguardado en cinta.
 - El tiempo en realizar el backup es inferior, ya que la copia en discos se realiza a mayor velocidad. Incluso se pueden realizar varias veces al día.

- Se minimiza el coste de los discos, ya que posteriormente se pasan los datos a la cinta, por lo que podrán ser sobrescritos.
- El archivo en cinta es económico y permite poder almacenarlo en sitios físicos diferentes a la oficina.
- **D2D2C** – disk to disk to cloud.
 - Frente a la solución D2D2T, añade la ventaja principal en el alojamiento de la información, eliminando el transporte de las cintas, previo cifrado de las mismas, controles de seguridad...
 - Evidentemente, el coste económico de este servicio en la nube deberá someterse a análisis y contrastarse con el resto de las posibilidades.
- **Almacenamiento NAS, SAN.**
 - En las empresas se suele trabajar en equipo, compartiendo ficheros entre varios ordenadores.
 - Aunque los puestos de trabajo pueden compartir carpetas con el resto de los equipos de la red, no es la solución más recomendable:
 - Hacer de servidor de ficheros afectará al rendimiento de sus aplicaciones.
 - Si el usuario del servidor apaga el equipo deja sin conexión a datos al resto de usuarios.
 - Al ser un puesto de trabajo, lo más probable es que no disponga de RAID ni de copia de seguridad.
 - Lo mejor es un servidor dedicado y especializado en almacenamiento:
 - Trabaja con un software especializado y por tanto con menor riesgo de infecciones.
 - Formará parte de las políticas de copias de seguridad y por tanto se garantiza que esté encendido todo el tiempo.
 - Posibilidad de desplegar RAID, memoria cache de alto rendimiento...
 - NAS (Network Attached Storage)
 - Dispositivos de almacenamiento dedicada a compartir su capacidad con otros equipos haciendo uso de protocolos de red.
 - No suelen tener teclado y se gestión via web.
 - Cada NAS es un nodo independiente de la red al que se accede por su propia IP.
 - Suelen incluir capacidad RAID
 - SAN (Storage Area Network) En un entorno empresarial se necesita más capacidad de procesamiento, amplia memoria caché, tarjetas de red de alta capacidad y configuraciones RAID.
 - Suelen estar en armarios que facilitan la escalabilidad.
 - Existe una red de alta velocidad que interconecta el SAN con los servidores de la red, lo que permite que cada servidor acceda a los ficheros como si fuera a un disco duro ligado directamente a él.

2 Ejercicios

1. Realizar una tabla comparativa de los distintos soportes con su capacidad máxima actual y su precio medio por GB. Después elegir tanto el soporte más adecuado como la política de copias (cuantas, cuándo y de qué tipo de copias) para los siguientes casos
 - a. Casa particular con 3 ordenadores
 - b. Empresa pequeña con un servidor con pocos datos y pocos cambios diarios.
 - c. Empresa mediana con un servidor con pocos datos y muchos cambios diarios.
 - d. Empresa grande con varios servidores con muchos datos y muchos cambio diarios,

Prácticas



3 Backup y restore en Windows

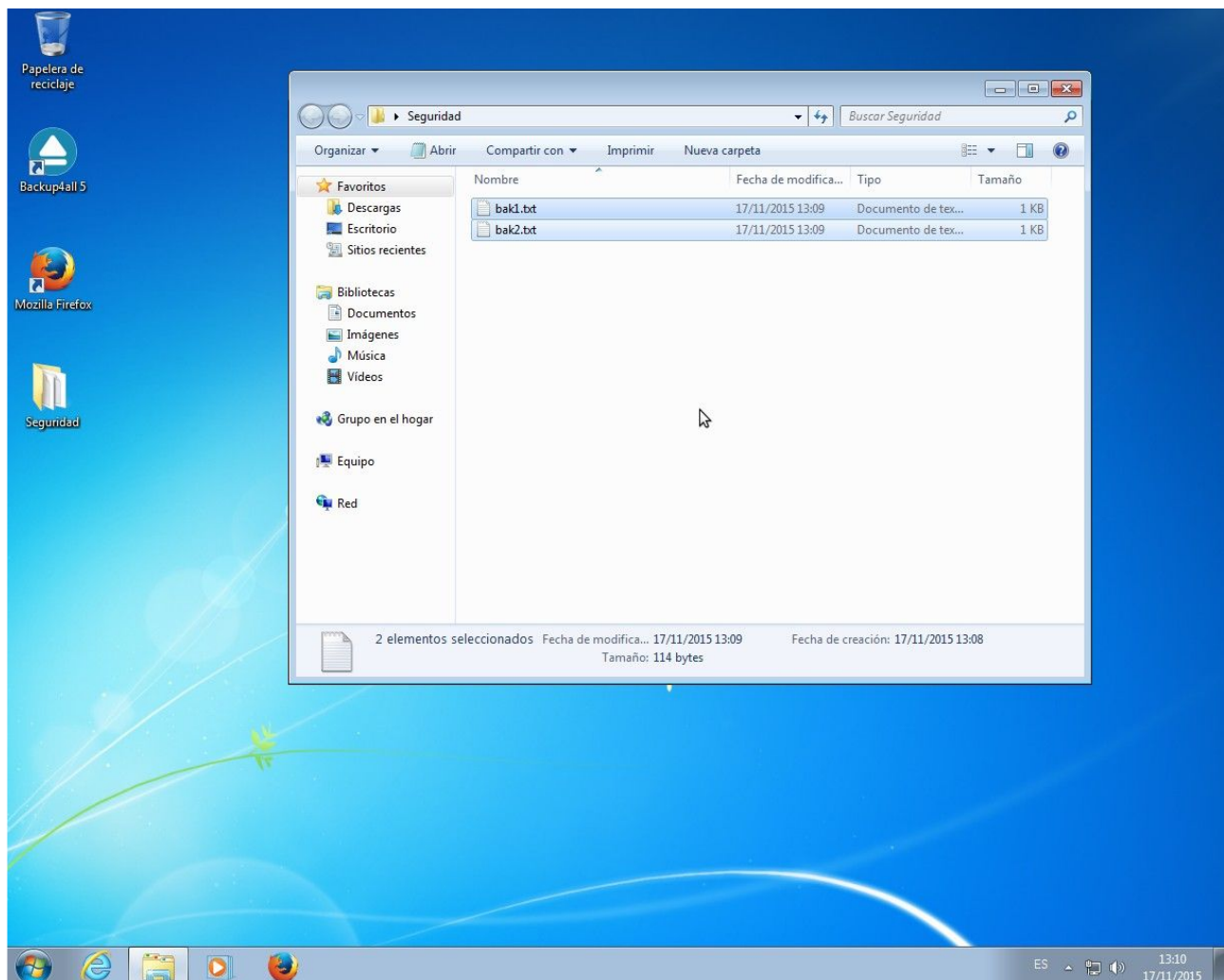
En esta práctica vamos a realizar una copia de seguridad o "backup" y una restauración de dicha copia en Windows.

Para realizar esta práctica utilizaremos la herramienta Backup4All. Podemos descargar la versión de prueba de 30 días desde este enlace:

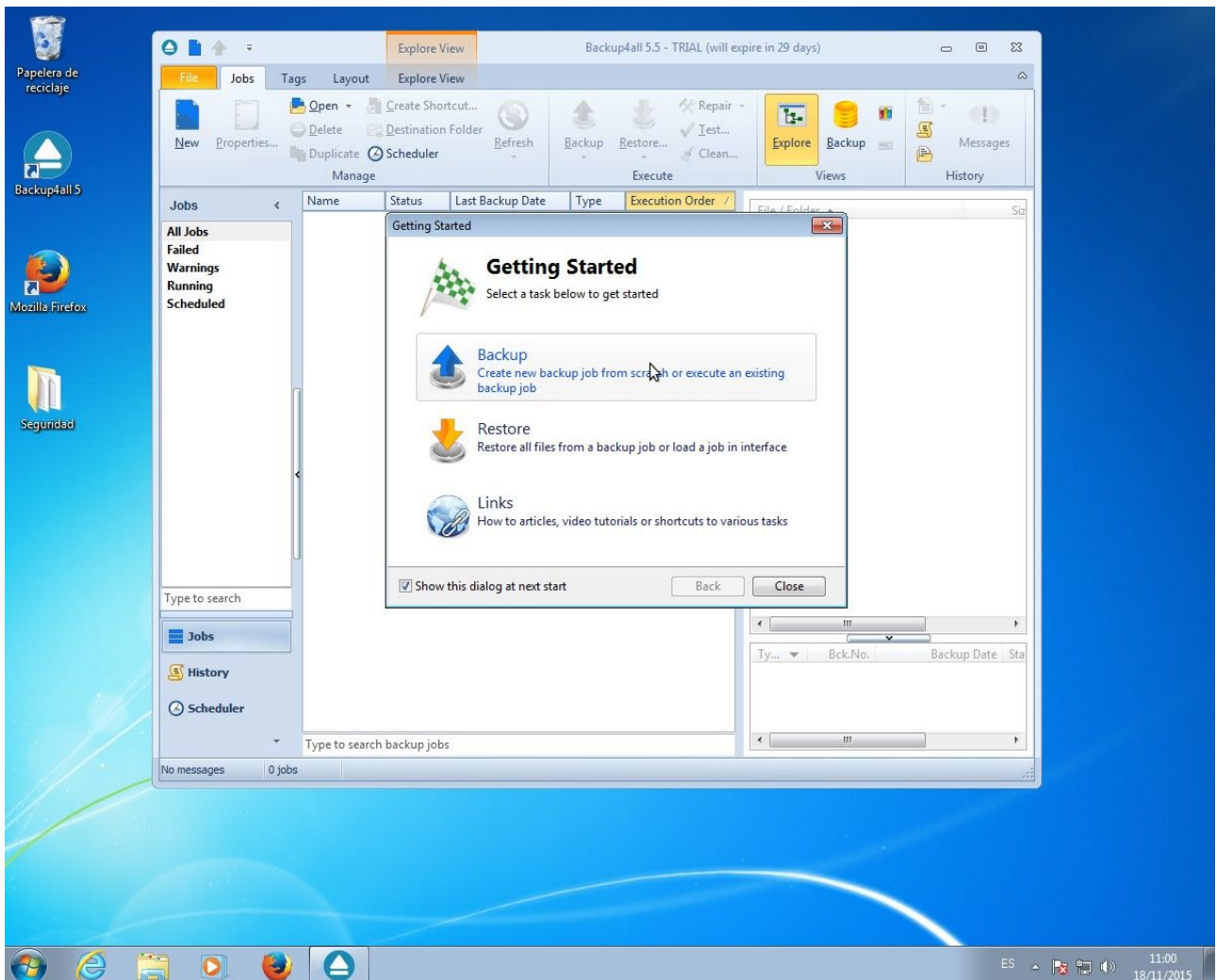
<http://download.backup4all.com/download/setup/b4asetup.msi>

Una vez lo hemos instalado procederemos a realizar el backup.

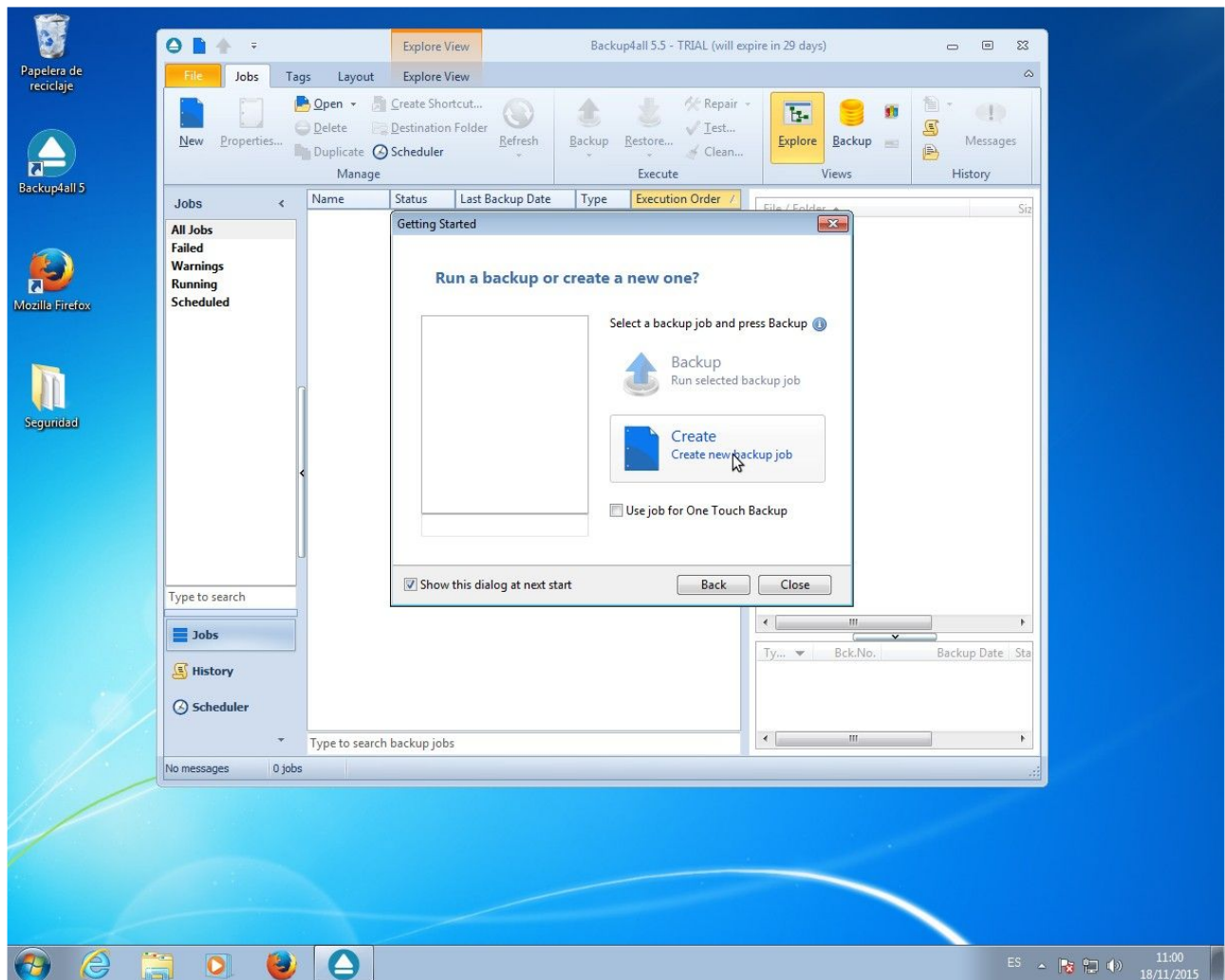
Primero tenemos que elegir de qué carpeta vamos a realizar el backup. En mi caso me he creado una carpeta en el Escritorio que se llama "Seguridad". Dentro de ésta he añadido dos archivos de texto.



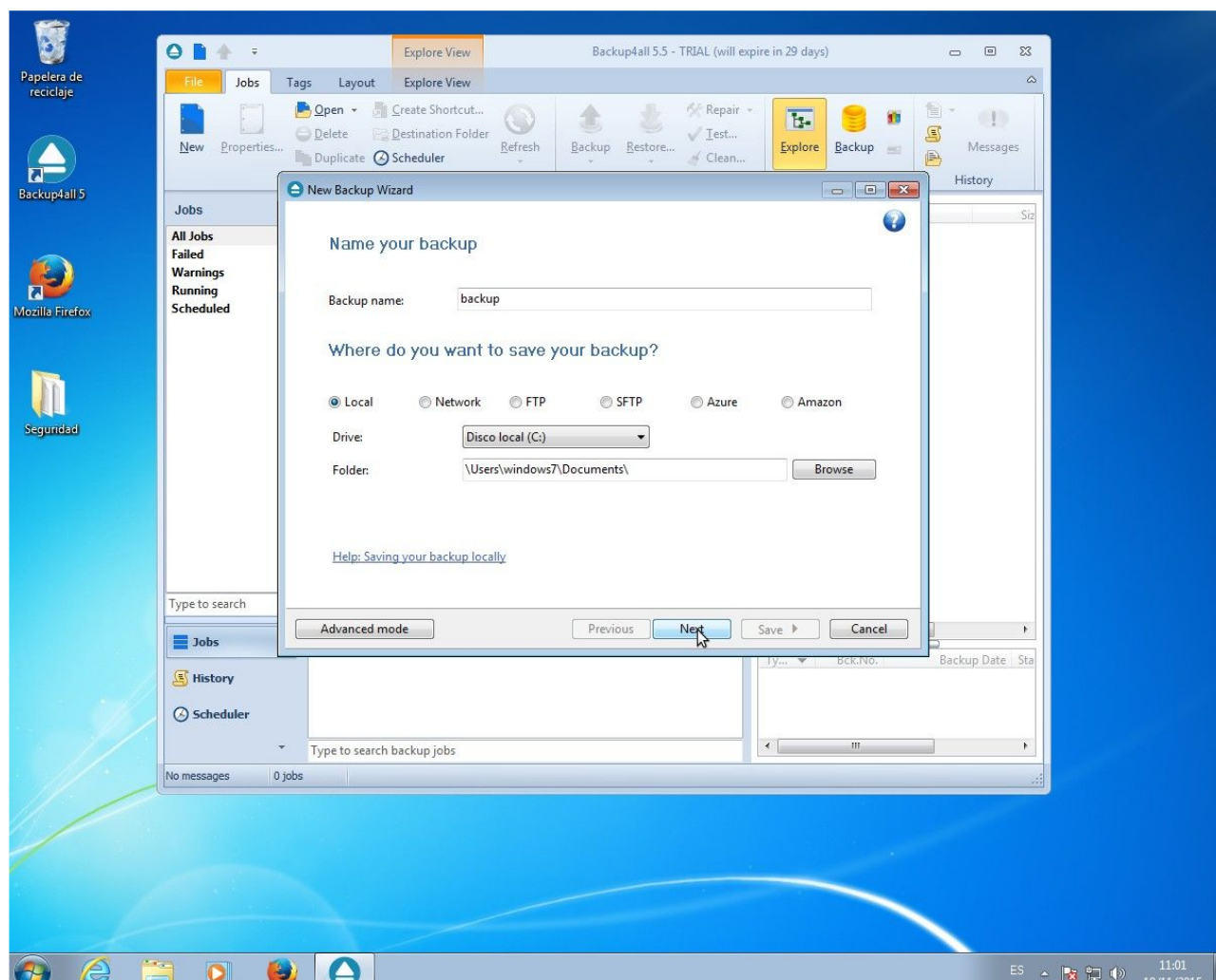
A continuación abrimos el Backup4all. Nos aparecerá una pantalla como la de la imagen de abajo. Hacemos clic en "Backup".



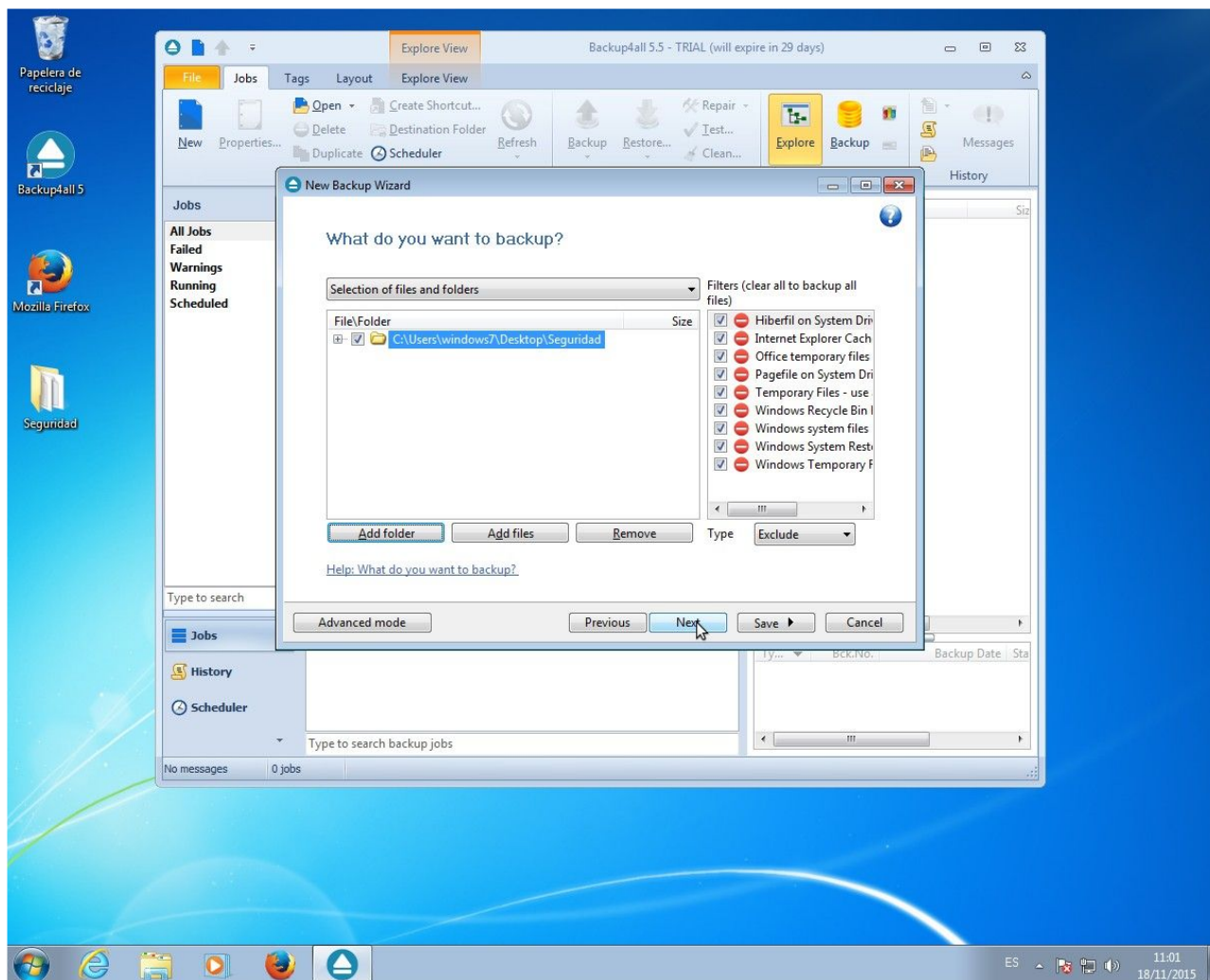
Seguidamente nos sale otra ventana en la que pinchamos sobre "Create".



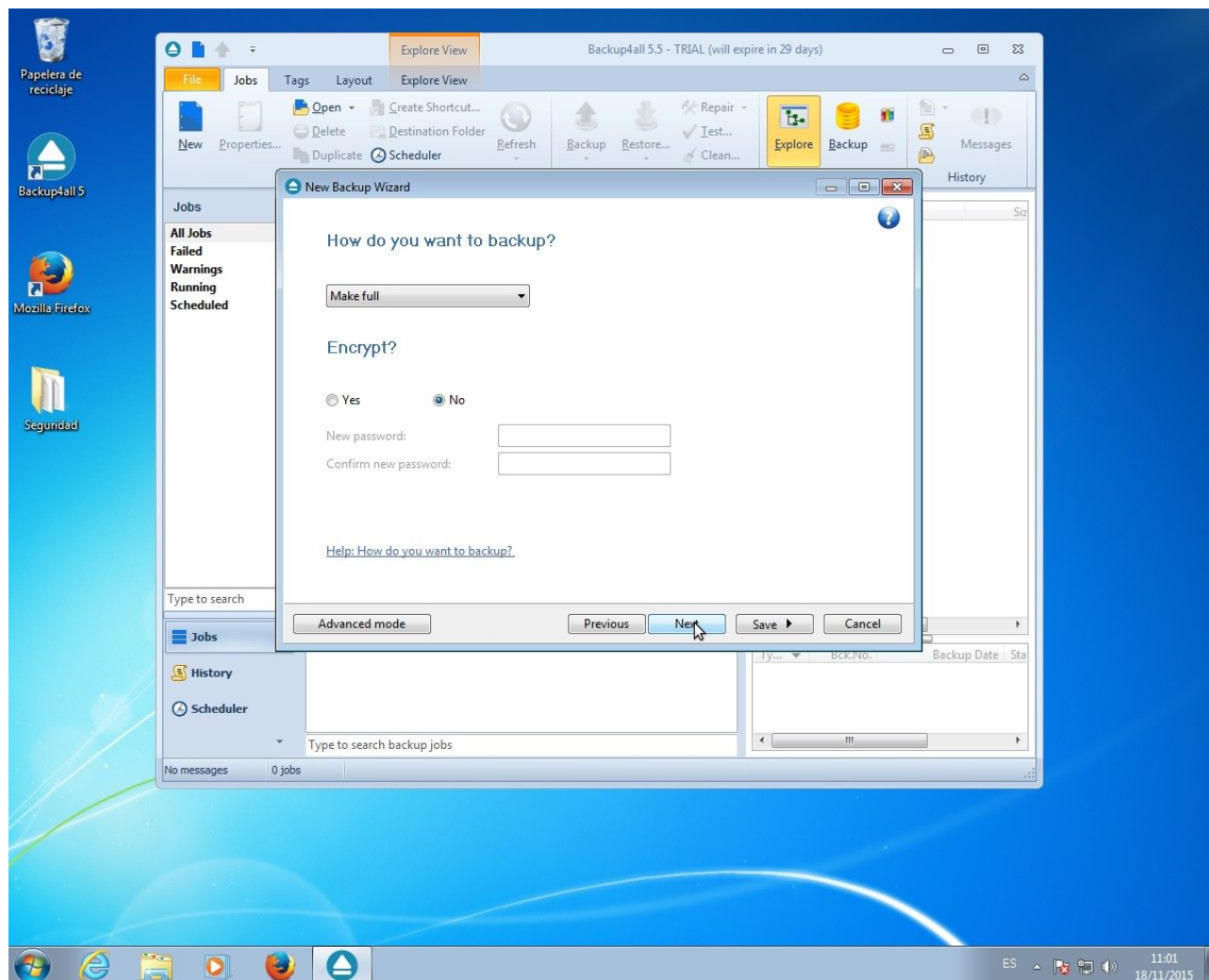
En la siguiente pantalla aparecen las opciones para elegir la ruta donde guardar el backup, así como el nombre que le daremos a dicho archivo. Se puede elegir entre guardarlo en el disco local, FTP o servicios de nube como Azure o Amazon. Nosotros elegiremos en local. Le damos a "Next".



Seguidamente tenemos que elegir de qué carpeta o que archivo queremos hacer el backup. Para seleccionarlo pinchamos en "Add folder" y buscamos la carpeta o archivo en cuestión. Una vez lo tengamos hacemos clic en "Next".

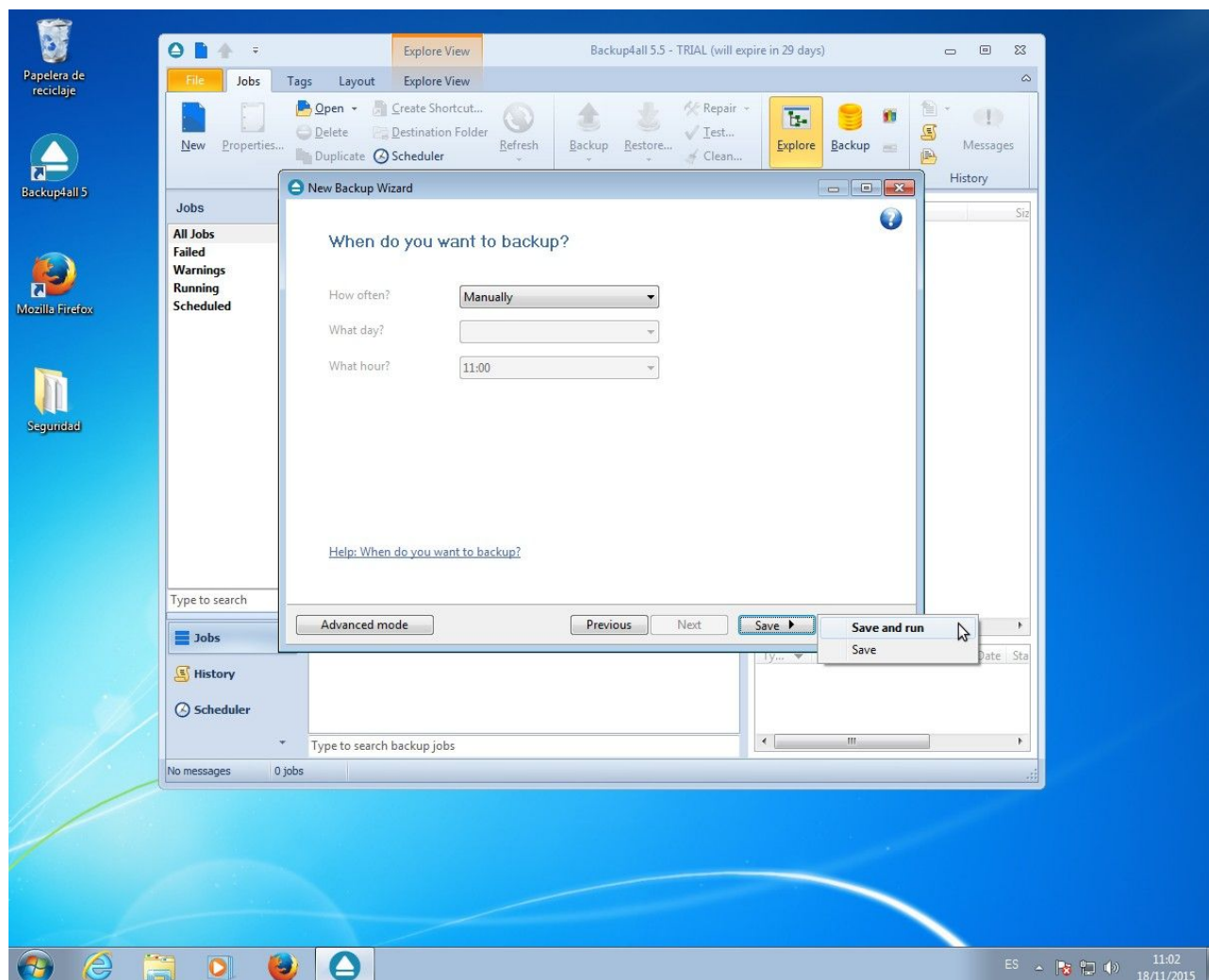


En el siguiente cuadro de diálogo nos pregunta de qué manera queremos hacer el backup. Podemos elegir entre hacerlo TOTAL, DIFERENCIAL o INCREMENTAL. Nosotros elegiremos TOTAL ya que es la primera copia que vamos a realizar.

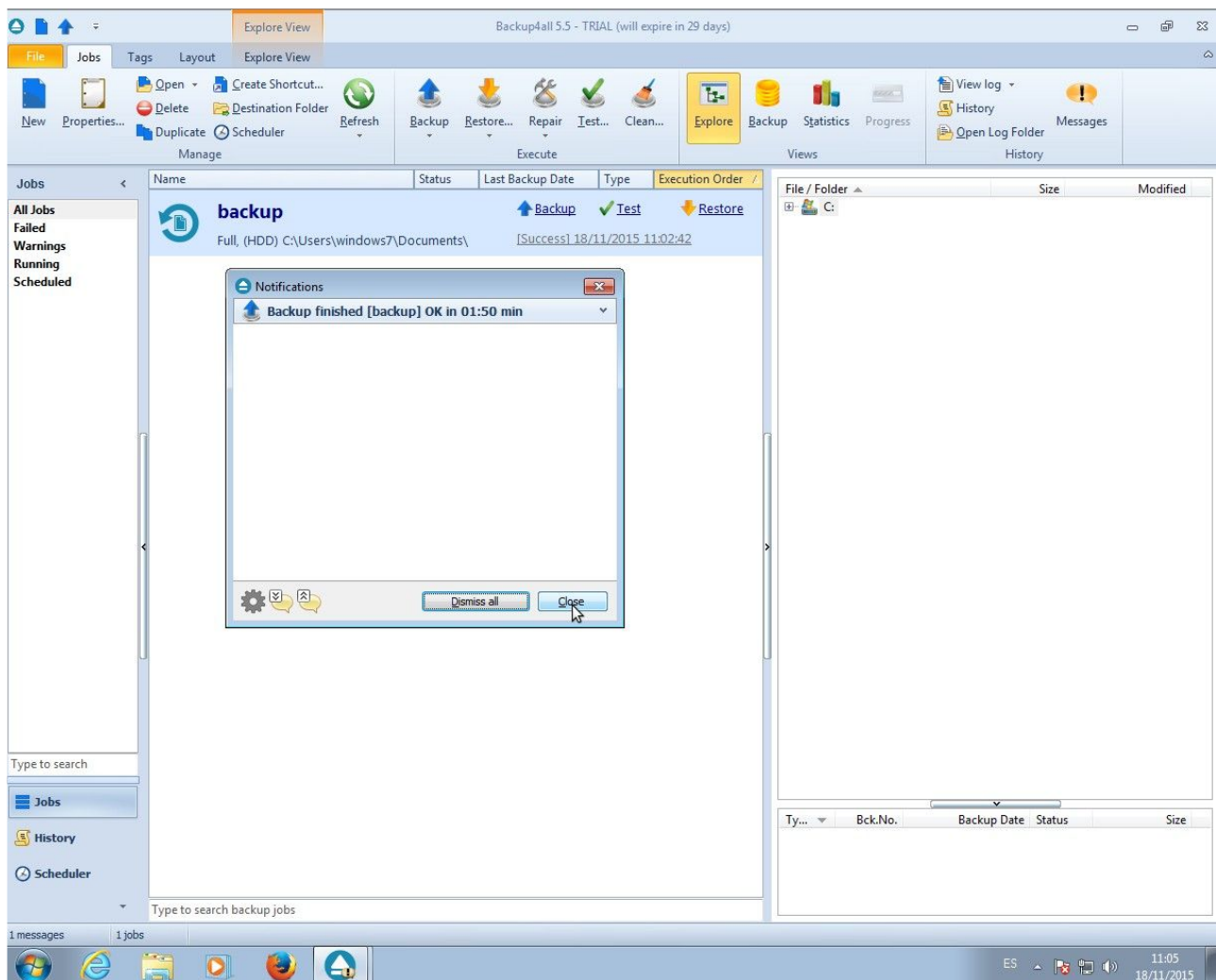


En la siguiente ventana nos da la opción de hacer la copia de seguridad manual o automática. Si elegimos la opción automática podemos elegir el día de la semana, la semana, el mes o el año y seleccionar la hora en la que queremos que realice la copia.

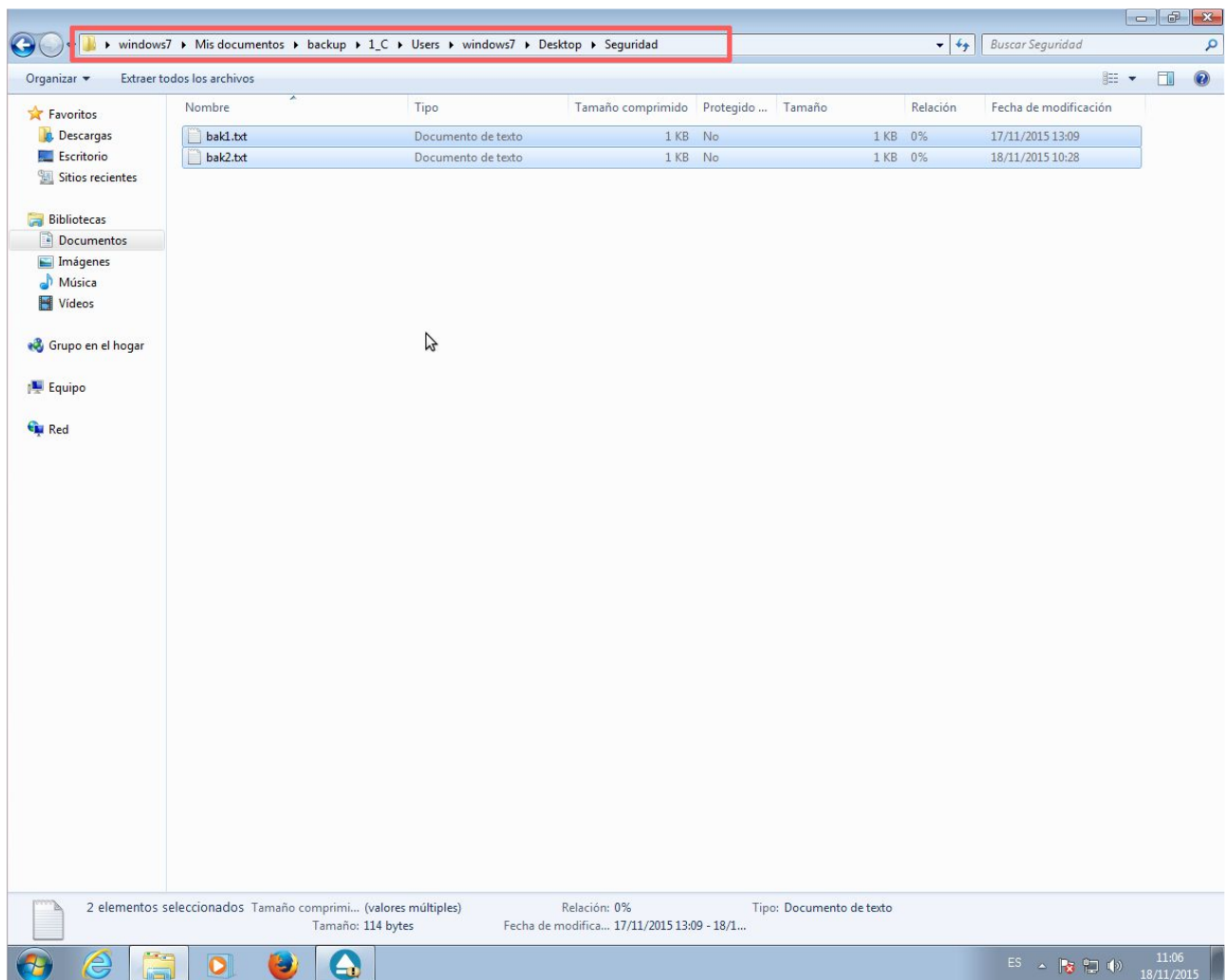
Nosotros lo dejamos en "Manually". Hacemos clic en "Save" y en "Save and run".



Esperamos a que el backup se realice. Una vez acabado nos aparecerá un cuadro de diálogo que nos indica que se ha realizado correctamente la copia.

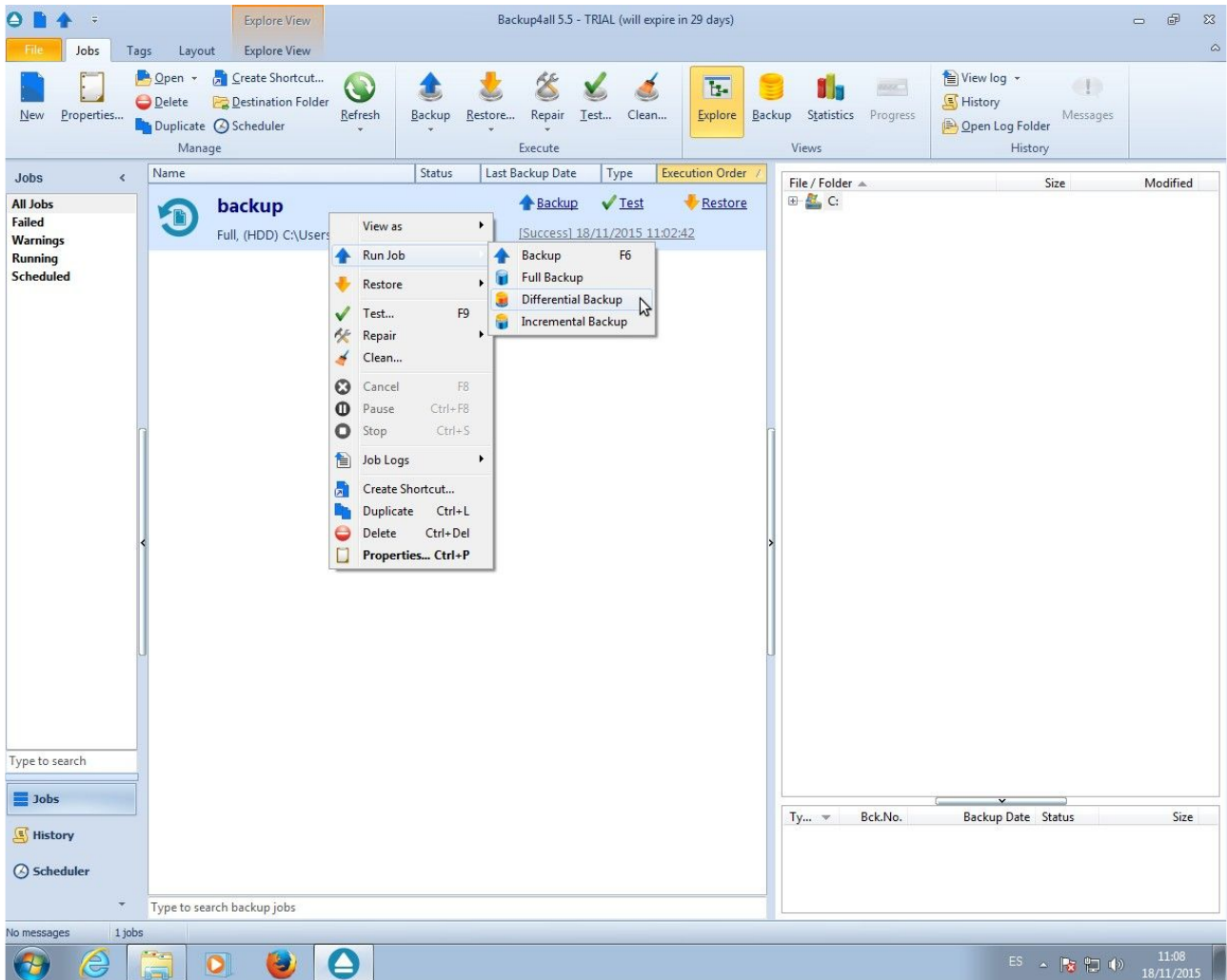


Como podéis ver en la siguiente imagen la copia se ha realizado correctamente en la ruta que hemos especificado.

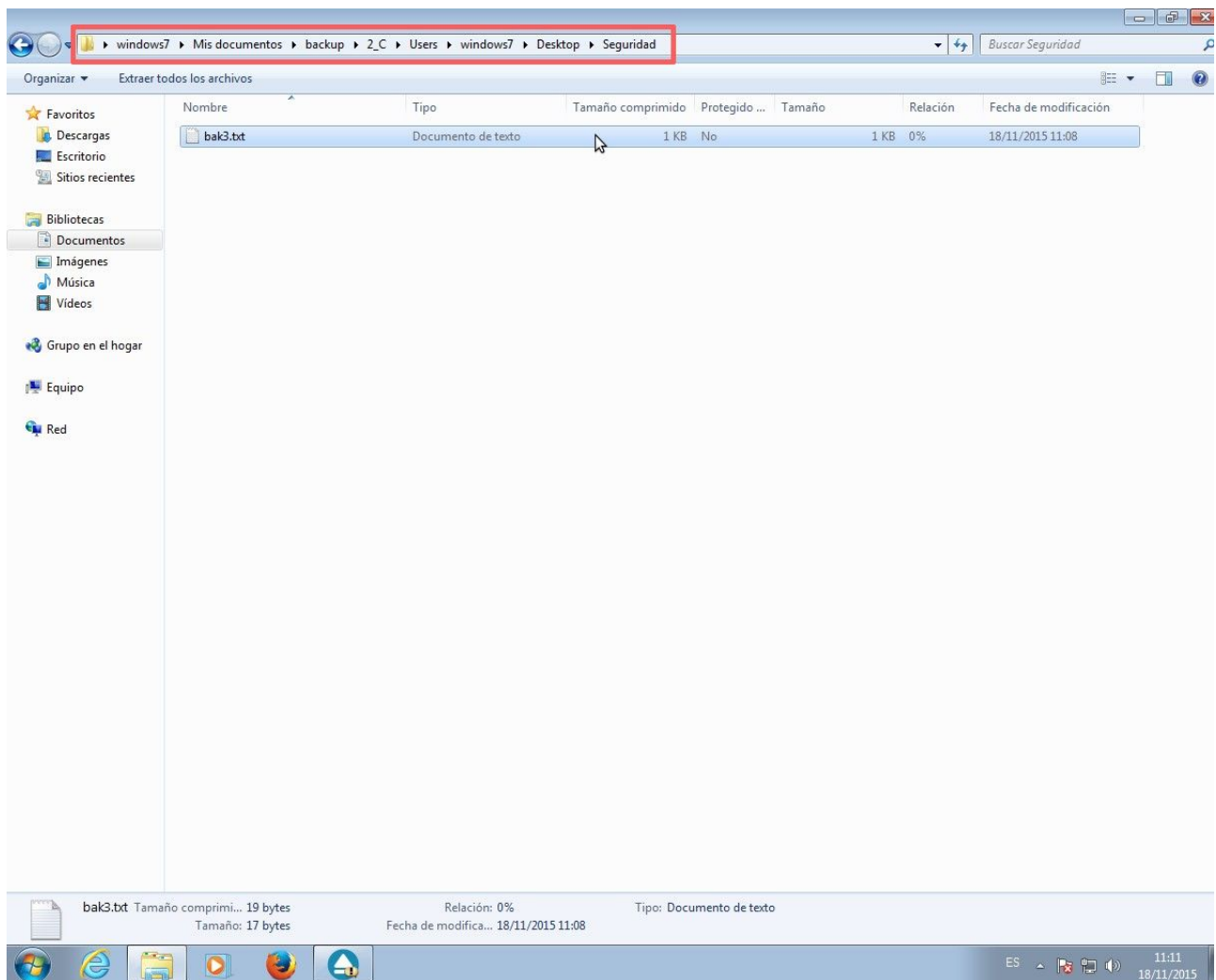


Ahora vamos a realizar una copia diferencial. En la carpeta de "Seguridad" añadimos un nuevo archivo de texto y escribimos algo en él.

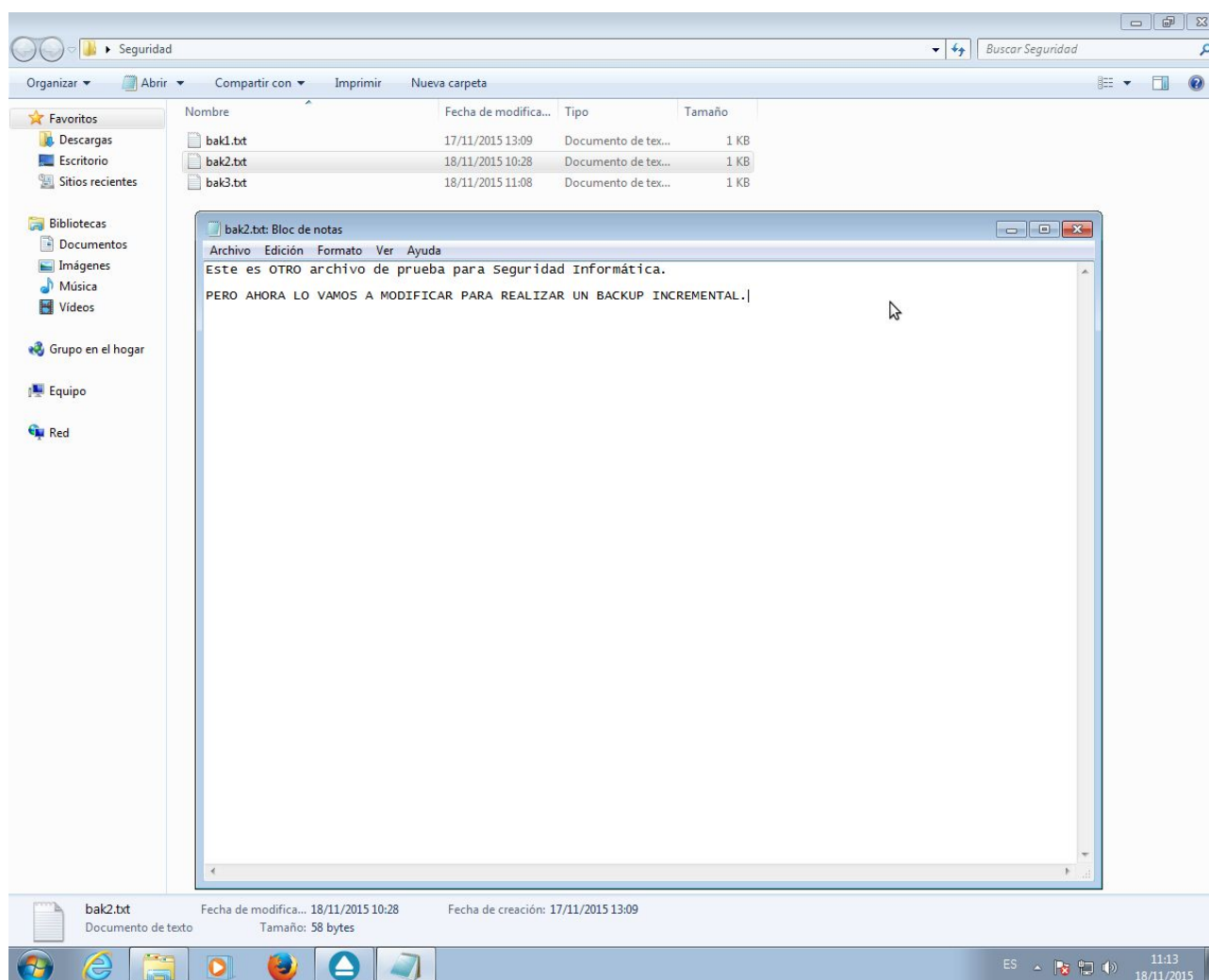
Abrimos backup4all y en la pestaña "Jobs" nos aparece las copias de seguridad que hemos realizado anteriormente. Hacemos clic con el botón derecho y nos dirigimos a Run Job → Differential Backup.



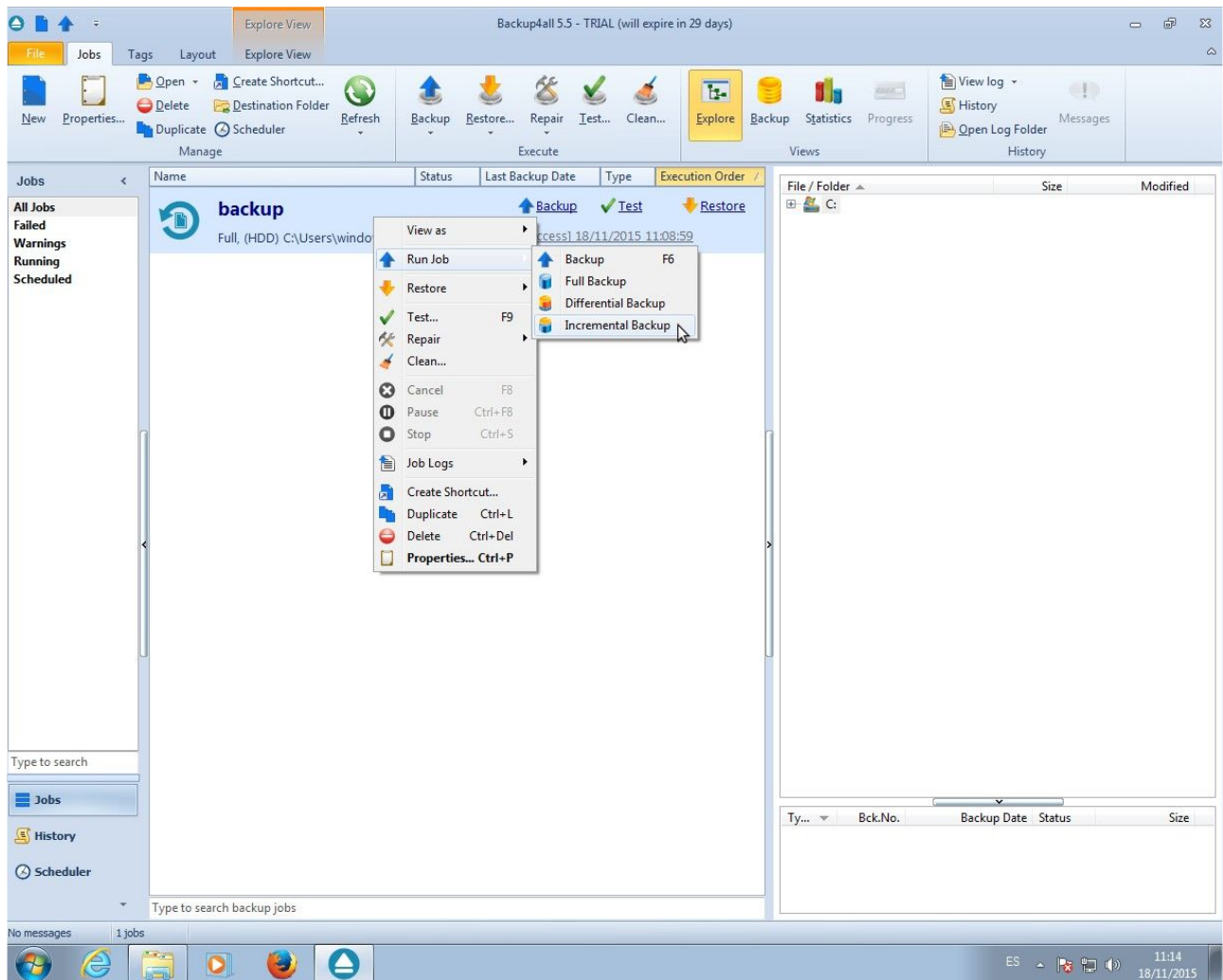
Esperamos a que acabe y nos vamos a la ruta que hemos definimos para guardar la copia. Vemos que nos ha creado otra carpeta (2_C) en la cual se encuentra nuestro nuevo archivo.



A continuación vamos a realizar el último tipo de copia que nos falta: la copia incremental. Para ello basta con modificar un archivo de los que ya tenemos creado.



Como en el apartado de la copia diferencial volvemos a abrir backup4all y en la pestaña "Jobs" nos aparece las copias de seguridad que hemos realizado anteriormente. Hacemos clic con el botón derecho y nos dirigimos a Run Job → incremental Backup.

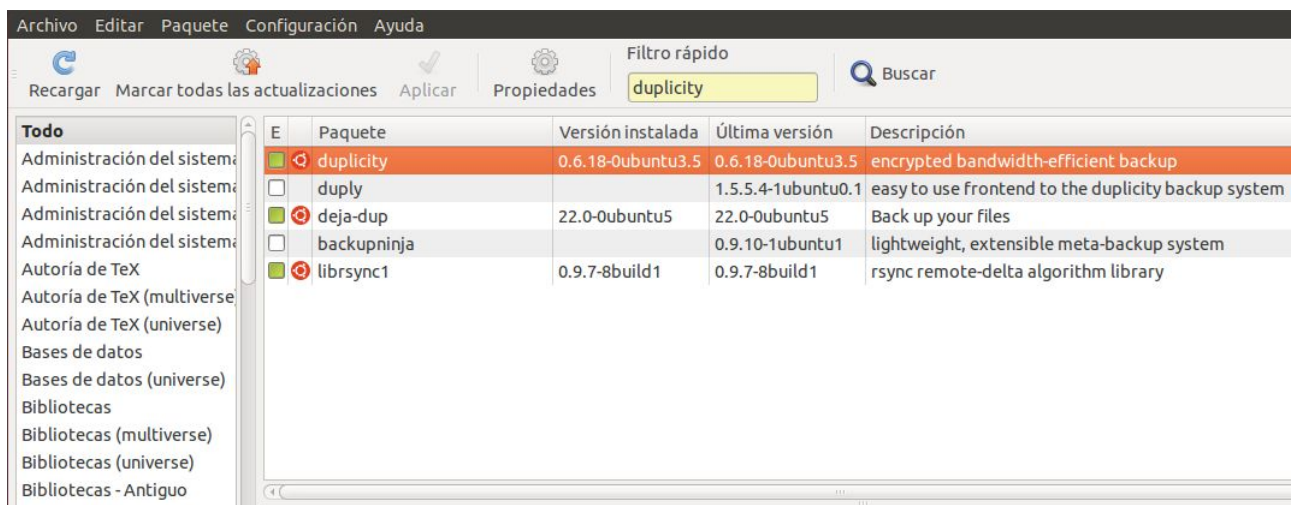


4 Backup y restore en Ubuntu

En esta práctica vamos a aprender a realizar un backup total, uno incremental y una restauración de dicha copia. También realizaremos una copia en un servidor FTP si es posible. Para ello vamos a utilizar duplicity, una herramienta mediante línea de comandos para SO Linux. Para ello seguiremos los siguientes pasos:

El primer paso es instalar duplicity. Podemos utilizar el gestor de paquetes Synaptic o bien en línea de comandos con:

```
sudo apt-get install duplicity
```



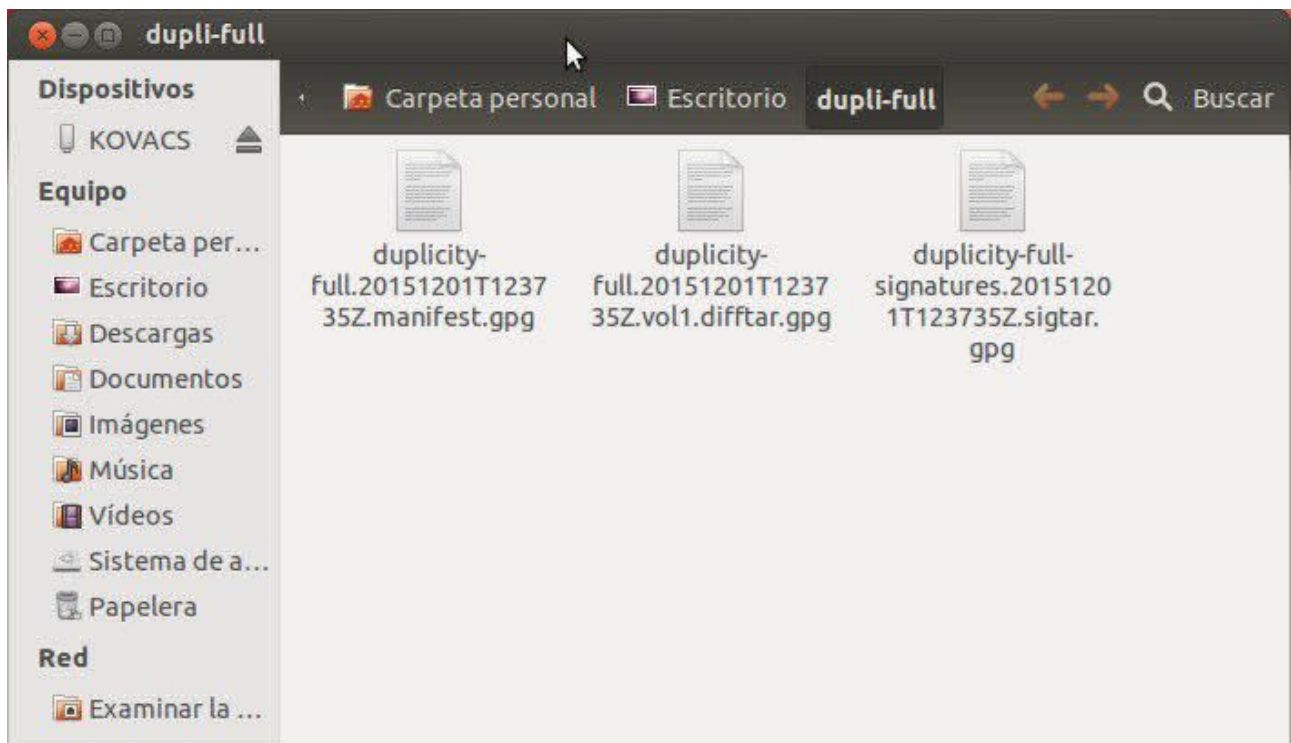
Vamos a ver como se hace una copia dentro de la misma máquina.

```
sudo duplicity full /ruta_carpeta_original file:///ruta_carpeta_backup
```

En el comando anterior hemos especificado lo siguiente:

- `duplicity full`
 - Indicamos que tipo de copia vamos a realizar.
- `/ruta_carpeta_original`
 - Ruta absoluta de la carpeta que queremos copiar.
- `file:///ruta_carpeta_backup`
 - Aquí indicamos la ruta dentro de nuestra máquina donde queremos que guarde el backup.
 - Si no tenéis creada una carpeta tranquilos ya que se creará una automáticamente.

Abajo veis la imagen de como se ha creado la carpeta y los archivos cifrados de la copia.



A continuación vamos a realizar un backup incremental. Lo primero es crear o modificar un archivo nuevo. Yo he creado un documento llamado "incremental". Debemos crearlo en la **misma** carpeta de la que hemos hecho la copia.



El comando que necesitamos es igual que el de la copia total, sólo que cambiaremos el “full” por un “incremental”.

```
sudo duplicity incremental /ruta_carpeta_original file:///ruta_carpeta_backup
```

```
smr2pc04@smr2pc04:~$ sudo duplicity incremental /home/smr2pc04/Escritorio/diseño\ web/ file:///home/smr2pc04/Escritorio/dupli-full
Import of duplicity.backends.sshbackend Failed: No module named paramiko
Los metadatos en local y remoto están sincronizados, no es necesario sincronizar.
Fecha del último respaldo completo: Tue Dec 1 13:37:35 2015
Frase de contraseña GnuPG:
Repita la contraseña para confirmar:
¡La primera y segunda contraseña no coinciden! Por favor inténtelo de nuevo.
Frase de contraseña GnuPG:
Repita la contraseña para confirmar:
-----[ Estadísticas de respaldo ]-----
StartTime 1448973749.50 (Tue Dec 1 13:42:29 2015)
EndTime 1448973749.53 (Tue Dec 1 13:42:29 2015)
ElapsedTime 0.03 (0.03 seconds)
SourceFiles 136
SourceFileSize 1690752 (1.61 MB)
NewFiles 3
NewFileSize 4123 (4.03 KB)
DeletedFiles 0
ChangedFiles 0
ChangedFileSize 0 (0 bytes)
ChangedDeltaSize 0 (0 bytes)
DeltaEntries 3
RawDeltaSize 27 (27 bytes)
TotalDestinationSizeChange 279 (279 bytes)
Errors 0
-----
smr2pc04@smr2pc04:~$
```

Ahora nos vamos a la carpeta que hayamos establecido para guardar la copia y veremos que se ha creado unos ficheros nuevos. Como podéis observar los archivo nuevos empiezan su nombre con "duplicity-inc". Eso indica que la copia incremental se ha realizado correctamente.



A continuación vamos a realizar una **restauración** de la copia que acabamos de hacer. Yo he eliminado el archivo "incremental" de la carpeta "diseño web".



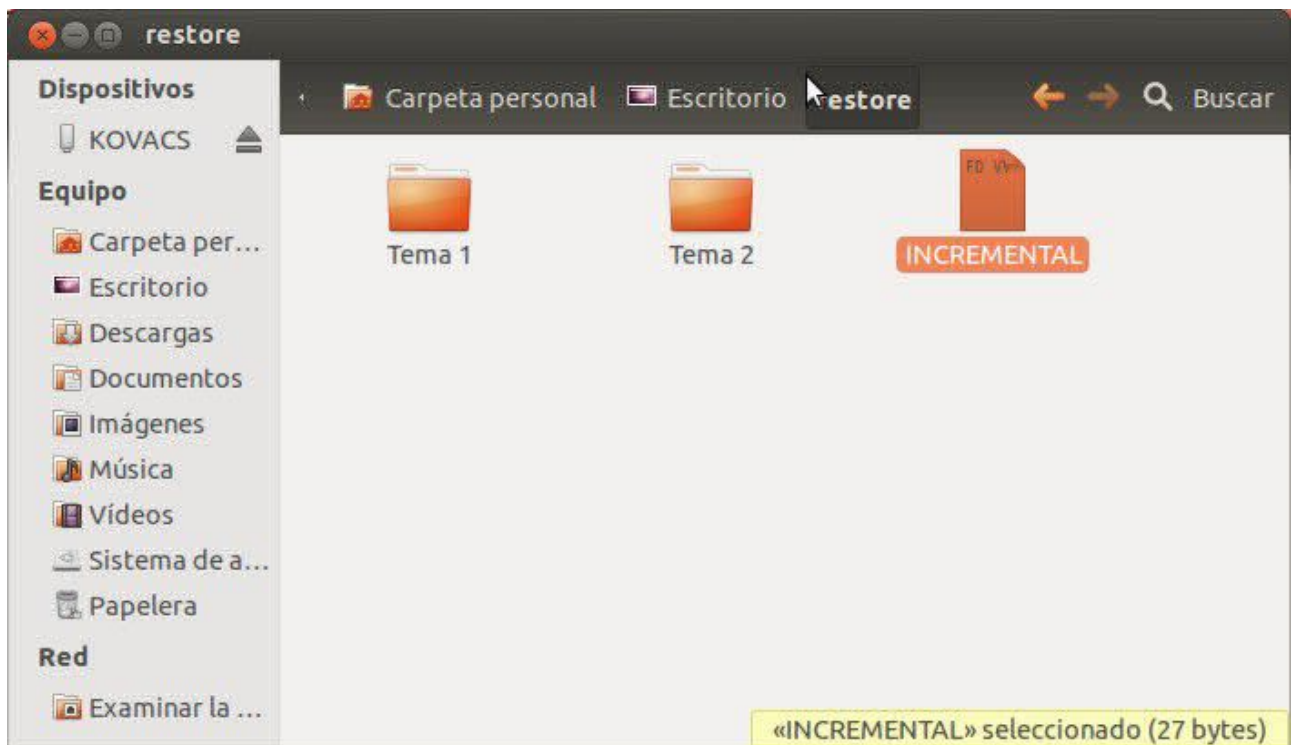
Para realizar un restore utilizaremos este comando:

```
sudo duplicity restore file:///ruta_carpeta_backup /ruta_carpeta_original
```

En nuestro caso he utilizado una carpeta de salida distinta a “diseño web” a la que he llamado “restore”.

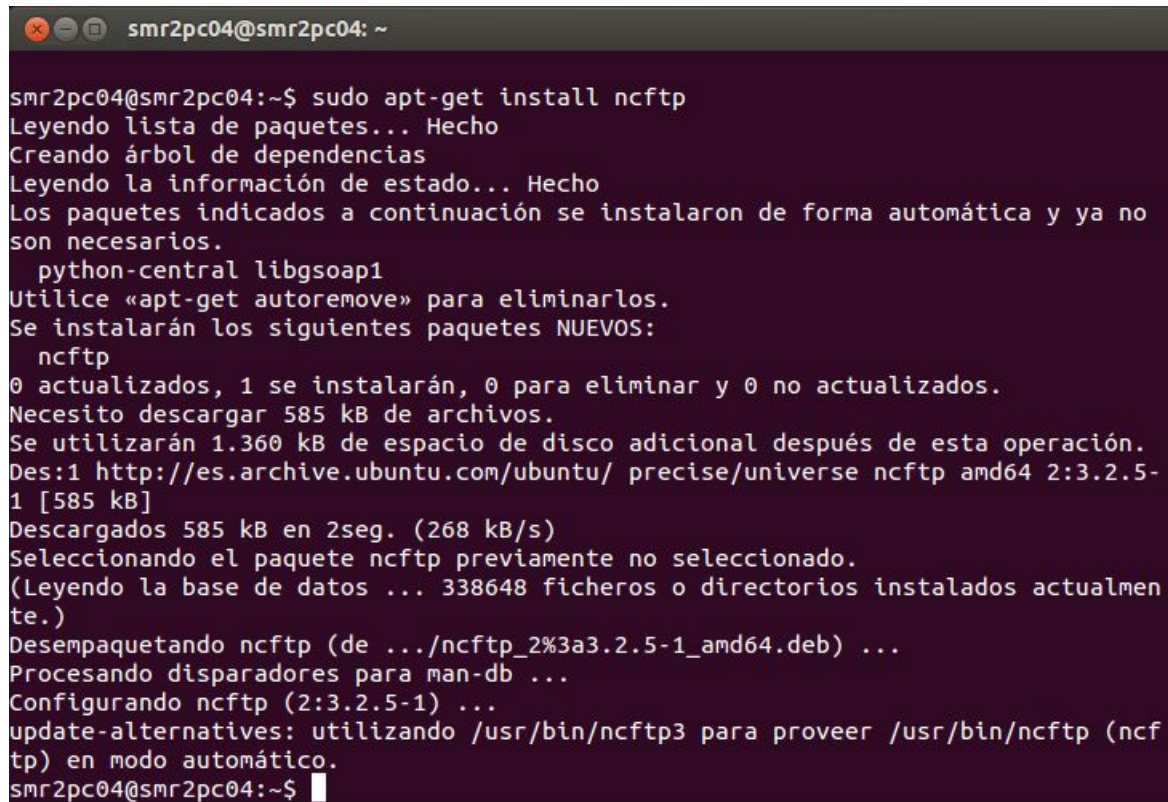
```
smr2pc04@smr2pc04:~$ sudo duplicity restore file:///home/smr2pc04/Escritorio/dupli-full/ /home/smr2pc04/Escritorio/restore
Import of duplicity.backends.sshbackend Failed: No module named paramiko
Sincronizando metadatos remotos con la caché local...
Frase de contraseña GnuPG:
Copiando duplicity-full-signatures.20151201T123735Z.sigtar.gpg a la caché local.
Copiando duplicity-full.20151201T123735Z.manifest.gpg a la caché local.
Copiando duplicity-inc.20151201T123735Z.to.20151201T124215Z.manifest.gpg a la caché local.
Copiando duplicity-new-signatures.20151201T123735Z.to.20151201T124215Z.sigtar.gpg a la caché local.
Fecha del último respaldo completo: Tue Dec 1 13:37:35 2015
smr2pc04@smr2pc04:~$
```

El siguiente paso es comprobar que los archivos han sido restaurado correctamente.



Para poder hacer el backup en el servidor FTP necesitaremos la utilidad ncftp. La instalaremos a través del terminal con el siguiente comando:

```
sudo apt-get install ncftp
```



```
smr2pc04@smr2pc04: ~  
  
smr2pc04@smr2pc04:~$ sudo apt-get install ncftp  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Los paquetes indicados a continuación se instalaron de forma automática y ya no  
son necesarios.  
  python-central libgsoap1  
Utilice «apt-get autoremove» para eliminarlos.  
Se instalarán los siguientes paquetes NUEVOS:  
  ncftp  
0 actualizados, 1 se instalarán, 0 para eliminar y 0 no actualizados.  
Necesito descargar 585 kB de archivos.  
Se utilizarán 1.360 kB de espacio de disco adicional después de esta operación.  
Des:1 http://es.archive.ubuntu.com/ubuntu/ precise/universe ncftp amd64 2:3.2.5-  
1 [585 kB]  
Descargados 585 kB en 2seg. (268 kB/s)  
Seleccionando el paquete ncftp previamente no seleccionado.  
(Leyendo la base de datos ... 338648 ficheros o directorios instalados actualmen  
te.)  
Desempaquetando ncftp (de .../ncftp_2%3a3.2.5-1_amd64.deb) ...  
Procesando disparadores para man-db ...  
Configurando ncftp (2:3.2.5-1) ...  
update-alternatives: utilizando /usr/bin/ncftp3 para proveer /usr/bin/ncftp (ncf  
tp) en modo automático.  
smr2pc04@smr2pc04:~$
```

Seguidamente abrimos el terminal otra vez y procedemos a realizar la copia **total** de una carpeta o fichero que elijamos. En mi caso he seleccionado una llamada "diseño web". El comando que tenemos que poner es el siguiente:

```
sudo duplicity full /ruta_carpeta_original ftp://usuarioftp@servidorftp:21/public_html
```

En el comando anterior hemos especificado lo siguiente:

- duplicity full
 - Indicamos que tipo de copia vamos a realizar.
- /ruta_carpeta_original
 - Ruta absoluta de la carpeta que queremos copiar
- ftp://usuarioftp@servidorftp:21/public_html
 - Aquí indicamos que vamos a realizar una copia en un servidor FTP.
 - Seguidamente tenemos que poner el usuario@servidorftp.
 - 21 es el puerto que utiliza el protocolo FTP.
 - /public_html es la carpeta dentro del servidor donde se va a guardar el backup.

```
smr2pc04@smr2pc04:~$ sudo duplicity full /home/smr2pc04/Escritorio/diseño\ web/ ftp://u980776371.angelsr@ftp.angelsmr2.esy.es:21/public_html
Import of duplicity.backends.sshbackend Failed: No module named paramiko
NcFTP version is 3.2.5
Password for 'u980776371.angelsr@ftp.angelsmr2.esy.es':
Los metadatos en local y remoto están sincronizados, no es necesario sincronizar.
Fecha del último respaldo completo: ninguna
Frase de contraseña GnuPG:
Repita la contraseña para confirmar:
-----[ Estadísticas de respaldo ]-----
StartTime 1448972473.27 (Tue Dec 1 13:21:13 2015)
EndTime 1448972474.39 (Tue Dec 1 13:21:14 2015)
ElapsedTime 1.12 (1.12 seconds)
SourceFiles 133
SourceFileSize 1690725 (1.61 MB)
NewFiles 133
NewFileSize 1690725 (1.61 MB)
DeletedFiles 0
ChangedFiles 0
ChangedFileSize 0 (0 bytes)
ChangedDeltaSize 0 (0 bytes)
DeltaEntries 133
RawDeltaSize 1621093 (1.55 MB)
TotalDestinationSizeChange 1464399 (1.40 MB)
Errors 0
-----
smr2pc04@smr2pc04:~$
```

¿Nos pide una contraseña?

Como veis en la imagen inferior la copia se ha realizado correctamente. El contenido de la copia no se puede ver, ya que va cifrada.



Index of /public_html

- [Parent Directory](#)
- [duplicity-full-signatures.20151201T122051Z.sigtar.gpg](#)
- [duplicity-full.20151201T122051Z.manifest.gpg](#)
- [duplicity-full.20151201T122051Z.vol1.difftar.gpg](#)

5 Copia de seguridad en Windows

Los pasos para hacer esta práctica son:

1. Realizar la copia de seguridad de la carpeta mis documentos, sin cifrar, con el software gratuito Cobian y como destino de la copia nuestro servidor NAS accediendo por FTP:
 - a. Se realizará una copia completa
 - b. Se realizará una diferencial que generará copia completa cada 5 diferenciales y guarda 5 copias. Se deberán realizar las pruebas correspondientes.
2. Restauraremos las copias de seguridad que tenemos en el servidor NAS.
 - a. Todo el directorio
 - b. Sólo algunos ficheros seleccionados a mano
 - c. Sólo los ficheros *.doc.
3. Realizar las mismas copias de seguridad pero esta vez irán cifradas y comprimidas y el destino de la copia será nuestro servidor NAS pero accediendo por CIFS.
4. Restauraremos las copias de seguridad que tenemos en el servidor NAS.
 - a. Todo el directorio
 - b. Sólo algunos ficheros seleccionados a mano
 - c. Sólo los ficheros *.doc.
5. Realizaremos otra copia de seguridad donde sólo se copiarán los ficheros *.doc del directorio mis documentos.

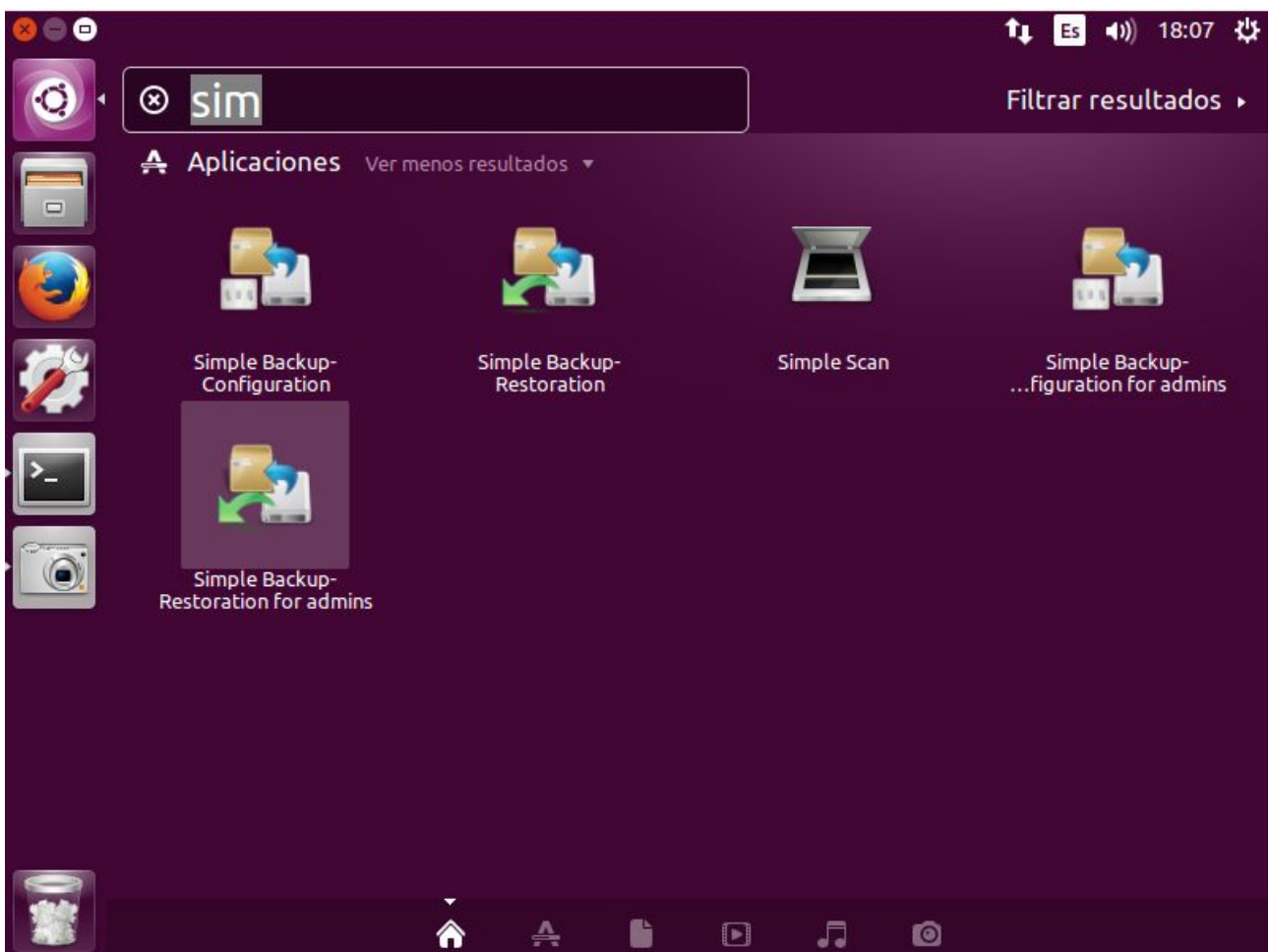
6 Backups cno sbackup

SBackup es una aplicación sencilla de escritorio para hacer copias de seguridad. Esta herramienta puede realizar copias de seguridad de cualquier subconjunto de archivos y directorios.

Diseñado inicialmente para Ubuntu, cuenta con una interfaz de usuario para GNOME y paquetes para todas las distribuciones derivadas de Debian. En Ubuntu Desktop debería estar inicialmente integrado en el menú de Sistema > Preferencias. Si no estuviese instalado, se puede instalar de la siguiente manera:

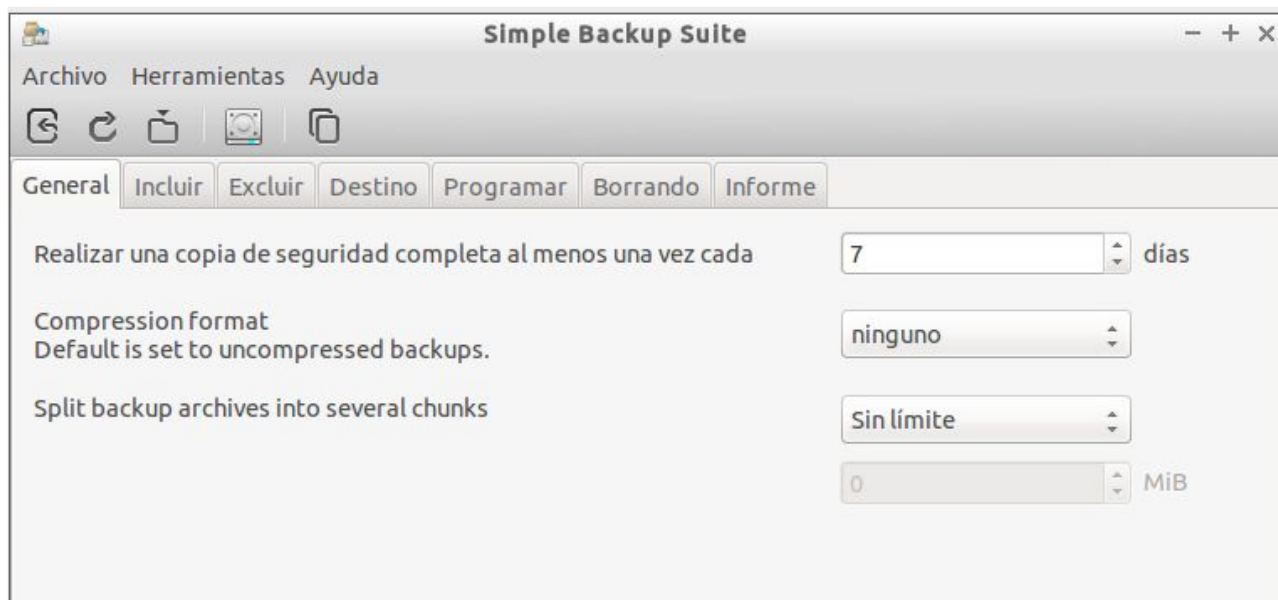
```
apt-get update
apt-get install sbackup
```

Como ya se ha comentado, se puede acceder por Herramientas del Sistema > Simple Configuration Backup for admins. Si no, búscalo de la siguiente manera:



En la ventana principal tenemos:

- **General:** Información global sobre las copias de seguridad: compresión, periodicidad máxima, tamaño del fichero.
- **Incluir:** Las que queremos que aparezcan en la copia de seguridad.
- **Excluir:** Las que no vamos a querer que aparezcan.
- **Destino:** Carpeta donde se va a guardar la copia de seguridad.
- **Programación:** Cada (Semana, mes, etc.)/Conservar (Si la queremos mantener).
- **Borrado:** periodo para eliminar copias viejas.



Como práctica, realiza los 3 tipos de backups.

Backups en Ubuntu

Busca la siguiente imagen en configuración del sistema:



Explica cómo funciona cada uno de los apartados haciendo un ejemplo.

7 Backup GNU/Linux

Bajo los sistemas GNU/Linux las operaciones de administración son habituales realizarlas mediante comandos del sistema, en este caso se propone un modelo de gestión de copias de seguridad con 2 comandos, **tar** para el empaquetado y **cron** para la automatización de tareas.

Primero vamos a realizar un backup completo

```
tar -cpvzf mibackup.tar.gz /home/miusuario
```

¿Qué significan esas opciones?

Podemos usar **-j** para comprimir con bzip2 o **-J** para comprimir con xz (ambos suelen ofrecer mejor resultados que gzip, solo que este último es más común)

Ahora vamos a realizar backups incrementales, para ello, primero vamos a realizar un backup completo y luego incrementales.

Primero creamos el backup completo del directorio que queremos respaldar (hay que usar la opción **-g** como se indica):

```
tar -cpvzf "fullbackup_`date +%d%m%Y`.tgz" -g /home/usuario/backup/backup.snap  
/home/usuario/Escritorio/*
```

Nota: Podemos crear mejor el backup moviéndonos hasta **./Escritorio** e indicando en el comando tar la ruta relativa **'./*'**. De la manera en la que lo hemos hecho deberemos de tener cuidado a la hora de desempaquetar. Si lo hacemos desde el directorio raíz machacaremos los archivos del home.

IMPORTANTE: El archivo backup.snap es el que guarda los metadatos que informan sobre los cambios que han ocurrido en el directorio. Si este archivo no existe se creará. Será el archivo que se lea cuando se haga el backup incremental. Si lo eliminamos, tar no encontrará información sobre los cambios realizados en el directorio, por lo que volverá a crear un full backup.

A partir de este backup completo, podemos crear los incrementales de esta manera:

```
tar -cpvzf "inc_backup_`date +%d%m%Y`.tgz" -g /home/usuario/backup/backup.snap  
/home/usuario/Escritorio/*
```

A continuación crearemos backups diferenciales con tar.

Para realizar backups diferenciales con tar usaremos su opción -N. Lo que nos permite esta opción es ordenar a tar que sólo archive aquellos datos que han sido cambiados o agregados desde una determinada fecha, hasta la fecha de ejecución del comando. Por ejemplo imaginemos que la fecha del fullbackup es del Lunes 9 de Febrero del 2015 y hoy (día en el que realizamos el backup diferencial es Miércoles 11 de Febrero del mismo año), haremos lo siguiente.

Primero crear la copia total (la del día 9 de Febrero)

```
tar -cpvzf "fullbackup_`date +%d%m%Y`.tgz" /home/usuario/Escritorio/*
```

A continuación vamos a crear copia diferencial con los cambios ocurridos desde el Lunes 9 al Miércoles 11 del 2015.

```
tar -cpvzf "dif1_backup_`date +%d%m%Y`.tar.gz" /home/usuario/Escritorio/* -N 09-feb-15
```

Nota: Si volviésemos a crear otro diferencial el Jueves o el Viernes con fecha 09-feb-15, contendrían también los cambios reflejados en dif1 es por ello que su tamaño va aumentando en comparación con los backups incrementales.

Establece los parámetros necesarios para que se ejecute la copia de seguridad todos los días a las 24:00h

Backups con rsync

rsync es una herramienta muy potente cuyo objetivo es sincronizar archivos y directorios.

Ésta no será una práctica guiada, sino que has de documentarte y realizarla. La documentación está en una sola página, con lo que en principio, es relativamente sencillo de entender.

Para hacer esta práctica:

1. Lee la siguiente página de Vicente Navarro:
 - a. Antes de nada hay que mencionar que si ves en algún momento que habla de entrar en modo **transparente**, no prestes atención a ello, pues se verá en otras unidades de trabajo.
 - b. <http://www.vicente-navarro.com/blog/2008/01/13/backups-con-rsync/>
2. Realiza un script que haga un backup completo por ssh a otra máquina.
3. Realiza un script que haga un backup incremental por ssh a otra máquina.
4. Realiza un documento donde expliques por qué has hecho los scripts como los has hecho.