

Copias de seguridade

Amalia Falcón Docampo
Laura Fernández Nocelo

Definición

As copias de seguridade, copias de respaldo ou backups (polo seu nome en inglés) son unha medida preventiva na seguridade informática que consiste en copias dos datos orixinais, ou mesmo programas, para dispor dun xeito de recuperarlos en caso de perda, calquera que sexa a circunstancia que a provoque.

As copias de seguridade garanten dúas características da información, vistas na primeira unidade:

Integridade: refírese á calidade da información, xa que esta debe ser precisa e completa e non sufrir ningunha manipulación nin alteración respecto á orixinal sen a debida autorización.

Dispoñibilidade: a información debe estar accesible en calquera momento para calquera usuario que teña permisos para poder acceder a ela.

Almacenamento das copias de seguridade

Recoméndase que as copias de seguridade se realicen en dispositivos de almacenamento externos polos seguintes motivos:

- Poida que o sistema operativo non arranque e non sexamos quen de acceder á información e, aínda que poidamos, o tempo necesario pode ser moi alto debido á súa complexidade.
- Borrado accidental dos datos.
- O disco ríxido deixa de estar inaccesible.
- O equipamento informático estrágase.
- Virus que borra a información.
- Roubo do equipamento informático.
- Desastres no contorno, como incendio, inundación, problemas eléctricos ou calquera outra catástrofe, que no mellor dos casos deixan temporalmente non dispoñible e accesible a información, e nos peores dos casos leva consigo unha perda total da información.

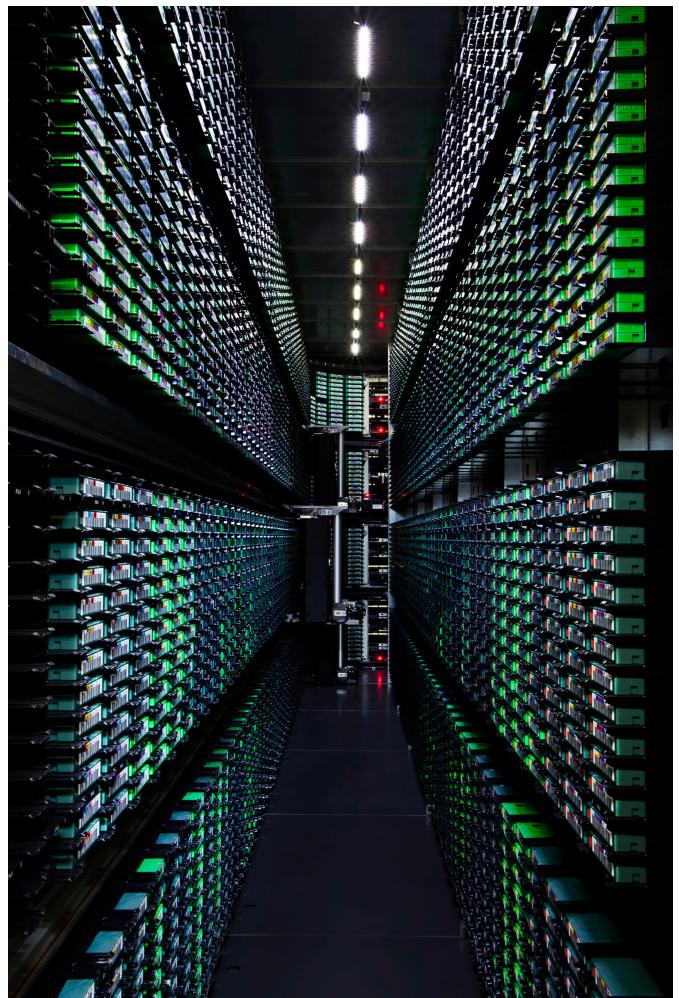
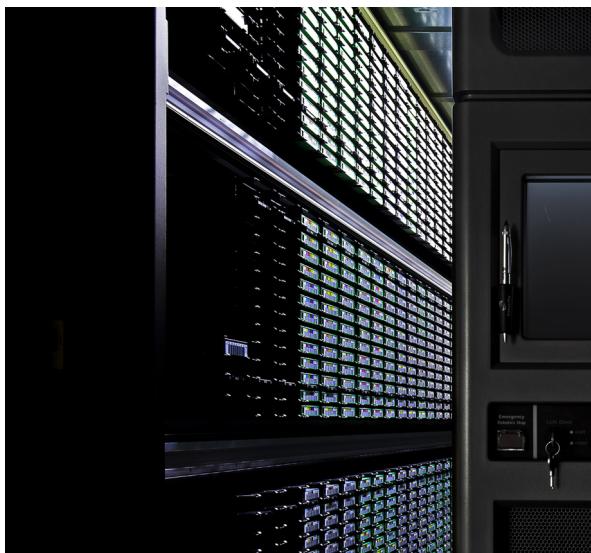
Os soportes de almacenamento externo onde se poden gardar as copias de seguridade son moi variados. Pódese consultar a unidade de almacenamento de información, onde se definen diversos dispositivos para almacenar información. Cada un destes soportes ten as súas vantaxes e desvantaxes, que hai que ter en conta á hora de elixilos como soporte para gardar a copia de seguridade.

Hai uns anos, a estratexia máis empregada para almacenar as copias de seguridade eran as cintas magnéticas, pero estas están a ser desprazadas polos discos como soporte de destino dos *backups*. Os motivos principais deste fenómeno, entre outros son:

1. Abaratamento dos discos.
2. Mellora da fiabilidade.

Os discos ríxidos de estado sólido ou SSD (*solid-state drive*) son unha boa proposta para almacenar copias de seguridade, xa que usan memoria non volátil (como a memoria flash) para o almacenamento en lugar dos pratos xiratorio magnéticos dos discos ríxidos convencionais. Desta forma, as unidades de estado sólido son menos sensibles a golpes, son praticamente inaudibles e teñen un menor tempo de acceso e de latencia (ao ser memorias de acceso aleatorio, o tempo de procura de datos é sempre o mesmo). Outra característica é que consomen menos que un disco ríxido convencional.

As cintas, por outra banda, ofrecen unha serie de vantaxes que as fan un



soporte de almacenamento para ter en conta:

1. Son moi fiables.
2. Doadamente transportables.
3. Escaso custo para o seu almacenamento remoto de grandes volumes de datos.
4. Sistema ecolóxico, posto que durante o almacenamento non emprega corrente eléctrica. A robótica e as unidades de biblioteca consomen enerxía, pero habitualmente menos que unha matriz de discos de capacidade similar.

Nas seguintes dúas imaxes pódese ver a biblioteca de cintas de Google do seu centro de datos no condado de Berkeley, en Carolina do Sur. Na imaxe da esquerda tense unha visión das cintas de copia de seguridade da biblioteca de cintas. Cada unha das cintas dispón dun código de barras para que o sistema robótico poida atopar a correcta. Na imaxe da dereita, ao fondo, pódense ver os brazos robóticos que se encargan de coller e almacenar a cinta cando é necesario.

Boas prácticas

Á hora de realizar as copias de seguridade cómpre ter en conta unha serie de aspectos para previr problemas, xa que non só é importante seguir unha boa estratexia para realizar as copias, senón que tamén hai que gardalas correctamente, elixir unha localización idónea e conservalas adecuadamente.

A continuación lístase unha serie de boas prácticas que se deberían seguir cando se realice unha copia de seguridade:

O dispositivo en que se garde a copia de seguridade non debe ser o mesmo que conteña os datos sobre os que esta se realiza, xa que se se dana o dispositivo se perderán tanto os datos orixinais como a copia.

Os dispositivos que conteñen as copias de seguridade non se deberían gardar na mesma sala nin, incluso, no mesmo edificio que onde estea o sistema que conteña os datos orixinais. A razón é que se hai algunha situación que provoque algúun tipo de dano na área ou no recinto e que provoque que se perdan os datos orixinais, daquela tamén se perderían as copias. Por exemplo, se un incendio destrúe a localización onde están os equipamentos e, por tanto, os datos, as copias que estean no mesmo espazo físico tamén se perderán.

As copias de seguridade deberán etiquetarse seguindo unha estratexia que permita identificalas axiña, para poder dispor delas no menor tempo posible

cando cumpra recuperar a información que conteñen. A etiquetaxe non debería conter información demasiado exhaustiva, de forma que se algún atacante pretende subtraela non poida identificar rapidamente o seu contido. Unha política correcta é a de utilizar códigos impresos en cada etiqueta, de maneira que o seu significado sexa coñecido polos usuarios que teñen acceso ás copias pero non por un potencial atacante.

Con certa frecuencia, debería verificarse o estado correcto das copias de seguridade, por se no momento de facer uso delas ocorre un erro inesperado. Como restaurar unha copia completa pode resultar demasiado traballo, poderíanse recuperar varios ficheiros aleatorios da copia, asumindo que se a recuperación funciona toda a copia é correcta.

Os dispositivos de almacenamento non deberían reutilizarse por tempo indefinido, xa que poden chegar a ter errores, co que convén substituílos para evitar calquera problema.

Un bo costume é realizar as copias de seguridade en momentos en que o sistema non estea a traballar a pleno rendemento. Deberíase procurar o momento en que o sistema está menos saturado e no que haxa a menor posibilidade de poder afectar os usuarios. Dependendo do sistema, en horas da noite e mesmo en fins de semana sería o mellor momento para realizar as copias.

Política de copias de seguridade

Para estarmos preparados ante calquera desastre que elimine a información do sistema, debemos planificar unha política de realización de copias de seguridade periódicas. Esta planificación axeitada das copias de seguridade forma parte do plan de continxencia dunha empresa, xa que a perda de datos pode pór en perigo a continuidade do negocio.

Algúns dos requisitos que debe cumplir a planificación de copias de seguridade son:

- Identificar os datos que requiran ser preservados. Son aqueles cuxa perda afectaría a continuidade do negocio. Débense indicar os discos, directorios, ficheiros, etc., que se deben copiar.
- Establecer a frecuencia coa que se van realizar os procesos de copia, así como o tipo de copia. Esta frecuencia inflúe na cantidade de información que se pode perder con respecto á fonte orixinal. Este parámetro é de suma importancia e require unha análise exhaustiva. Por exemplo, se se realiza unha copia cada noite e o soporte se estraga ás 12 horas, toda a

información xerada dende a noite anterior ata esa hora non estará na copia de seguridade.

- Establecer o esquema de rotación: a rotación refírese á forma en que se almacenan e resguardan as copias de seguridade. Un esquema de rotación indica cantas cintas (ou outro tipo de soporte de almacenamento) se utilizan para realizar a copia de seguridade.

Nas seguintes ligazóns pódese obter información adicional sobre as copias de seguridade, así como dos esquemas de rotación:

<http://www.htcspain.com/foro/seguridad-informatica-48/artitulo-2-copias-de-seguridad-que-son-que-sirven-y-se-14184/>

<http://searchdatacenter.techtarget.com/es/consejo/Como-optimizar-su-estrategia-de-rotacion-de-cintas-de-respaldo>.

- Dispor o almacén físico para as copias. Este almacén determinase en función da seguridade que requira a información, entre almacéns no mesmo edificio ou remotos en edificios externos. Por exemplo, se se produce un incendio no edificio da empresa, a información almacenada nun edificio externo segue a estar dispoñible.
- Procurar unha probabilidade de erro mínima, asegurándose de que os datos se copien integralmente do orixinal e nuns soportes fiables e en bo estado. Non se deben utilizar soportes que estean preto de cumplir a súa vida útil, para evitar que fallen cando se vaia recuperar a información que conteñen.
- Controlar os soportes que conteñen as copias, gardándoo nun lugar seguro e restrinxindo o seu acceso só ás persoas autorizadas.

Planificar a restauración das copias:

- Formando o persoal técnico encargado de realizaras.
- Dispondo de soportes para restaurar a copia, diferentes dos de producción.
- Establecendo os medios para dispor da devandita copia no menor tempo posible.
- Probar o sistema de forma exhaustiva, para comprobar a súa correcta planificación e a eficacia dos medios dispostos.

- Definir a vixencia das copias, establecendo un período no que estas deixan de ter validez e poden substituírse por outras más actualizadas de información.
- Controlar a obsolescencia dos dispositivos de almacenamento. Para o caso das copias que almacenen información histórica da organización, por exemplo proxectos xa pechados, débese ter en conta o tipo de dispositivo en que se realizara a copia, para evitar que no momento que se requira a restauración da devandita información non existan xa lectores axeitados para o dispositivo.

Cando se desboten os soportes de almacenamento, porque cheguen ao límite da súa vida útil fixado na política de copias de seguridade, é importante realizar un proceso de borrado seguro ou destrucción, para asegurar que a información que conteñan non poida ser recuperada posteriormente.

Especificar os sistemas de copias de seguridade, sobre todo cando cumpra realizar copias de seguridade en sistemas que non sexa posible deter para realizar a copia en frío, polo que se debe indicar a estratexia que se va utilizar para realizar a copia en quente.

Tipos de copias de seguridade

Hai tres tipos de copias de seguridade: completa, diferencial e incremental.

Copia completa

Neste tipo de copia créase unha copia de todos os ficheiros e directorios seleccionados. A primeira vez que se realiza unha copia sobre a información adoita ser deste tipo. Como estas copias ocupan grande cantidade de espazo de almacenamento, non é práctico utilizalas sempre, senón que se deben alternar cos dous tipos seguintes.

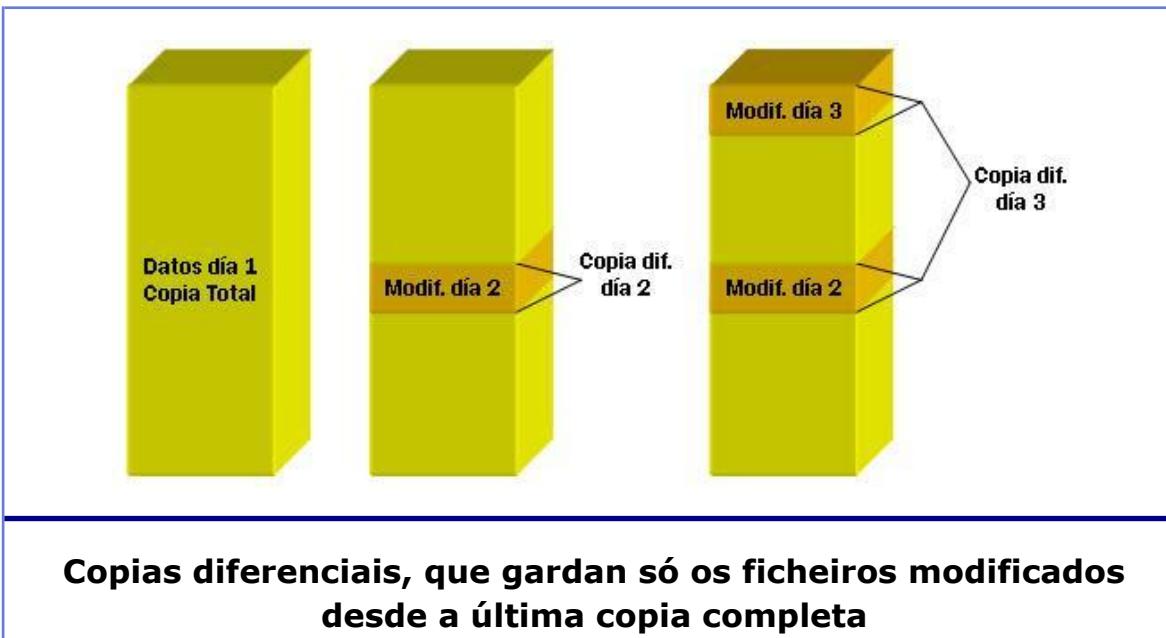
Vantaxe: a recuperación total ou parcial dunha copia completa é doada.

Desvantaxes:

Dependendo do tamaño dos ficheiros, pode consumir moito tempo e espazo.

Tamén o tempo de procura e recuperación pode ser alto.

.



Copia diferencial

A copia de seguridade diferencial conterá todos os ficheiros que se crearan ou modificaran desde a última copia completa. Para restaurar os datos necesítase a última copia completa e a última copia diferencial.

Vantaxe: require menos tempo e menos espazo para o seu almacenamento que a copia completa.

Desvantaxes:

É más lenta que as copias incrementais e non ten un uso tan eficiente do espazo, xa que todos os ficheiros engadidos ou modificados despois da copia completa serán duplicados en cada copia diferencial.

A restauración é más lenta e un pouco máis complexa que nas copias completas, pero máis sinxela que nas copias incrementais.

Na seguinte imaxe pódese ver como funciona este tipo de copia. O día 2 hai unha serie de modificacións respecto á copia realizada o día 1. Se se realiza unha copia diferencial, esta só conterá estes datos modificados. O día 3 modifícanse os datos novamente. Se se realiza unha nova copia diferencial, esta conterá todos os datos modificados desde a última copia completa, que foi o día 1. Xa que logo, conterá tanto os datos modificados do día 2 coma os do día 3

Copia incremental

Neste caso só se xera unha copia dos datos que foron creados ou modificados desde a última copia completa ou diferencial realizada. Para restaurar os datos, necesítase a última copia completa e todas as copias incrementais realizadas desde entón.

Vantaxes:

É o tipo de copia máis rápido.

Fai un uso eficiente do espazo de almacenamento, xa que os ficheiros non están duplicados.

Necesítase menos espazo de almacenamento, comparado coas copias completas e diferenciais.

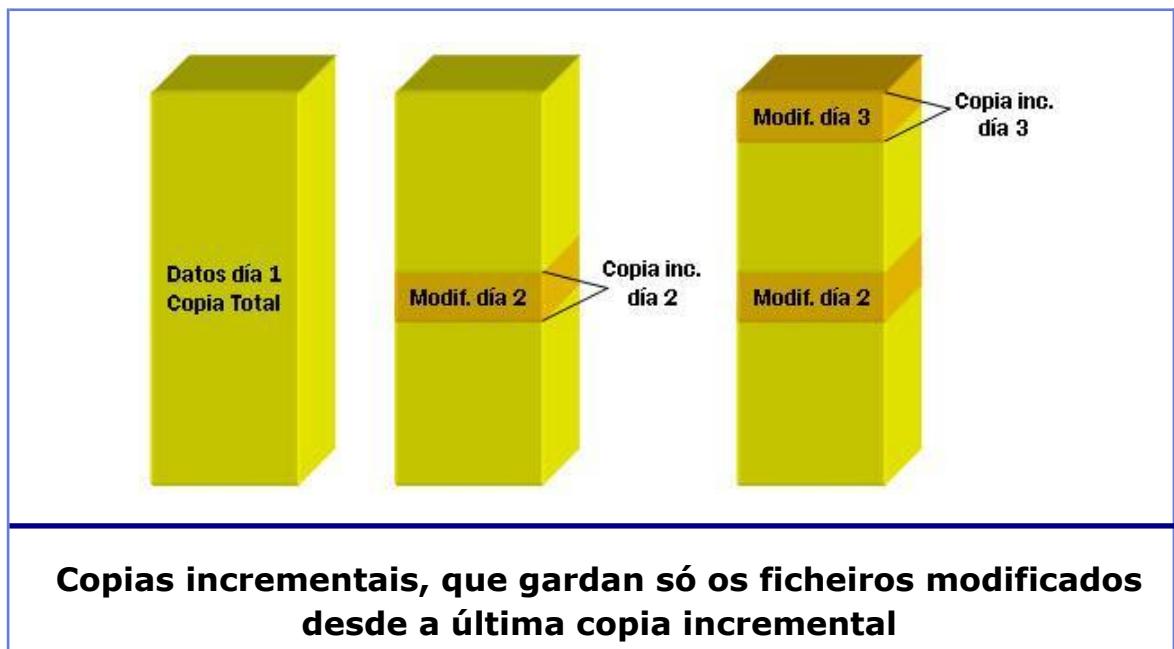
Desvantaxes:

As restauracións son más lentas que nas copias completas e diferenciais.

As restauracións tamén son un pouco más complexas, ao necesitarse a copia completa e todas as copias incrementais.

Aplicación práctica das copias de seguridade

Hai multitud de ferramentas que permiten realizar copias de seguridade dos datos nos sistemas operativos. Algunhas ferramentas son propias do sistema e outras son de terceiros, que permiten realizar diferentes tipos de copias de seguridade.



Copias de seguridade con ferramentas do sistema

Tanto o sistema operativo Windows como o Linux teñen ferramentas propias que permiten realizar copias de seguridade.

Windows

Este sistema operativo proporciona dous métodos para realizar e restaurar copias de seguridade dos volumes existentes localmente:

Liña de comandos coa utilidade wbadmin: permite ademais configurar ou modificar unha programación de copia de seguridade diaria.

Ferramenta gráfica *Copias de seguridade de Windows*: permite programar a realización das copias para que se realicen nun determinado momento, por exemplo, semanalmente.

Linux

Linux ofrece unha serie de comandos básicos que son estándares e están presentes en todas as distribucións, o cal supón unha grande vantaxe, xa que é posible realizar as copias de seguridade en calquera distribución, así como restauralas en caso de necesidade. Isto non ocorre do mesmo xeito coas ferramentas propias que proporcionan moitas distribucións, xa que se se realizan as copias con estas ferramentas se necesitarán as mesmas ferramentas para restaurar as copias. Isto significa que se falla o computador onde realizamos as copias, debemos de dispor doutro coa mesma distribución para poder acceder as copias de seguridade e poder traballar con elas para posibles restauracións.

Entre os comandos básicos está o programa *tar* (de *Tape Ariver -arquivador en cinta-*), que se deseñou para almacenar ficheiros en cintas magnéticas. Este programa úsase para almacenar ficheiros ou directorios nun só ficheiro. *Tar* é unha orde que pode ser executada desde un terminal, e o seu formato comunmente é:

```
tar <opciones><archivoSalida> <archivo1> <archivo2> .. <archivoN>
```

onde <archivoSalida> é o ficheiro resultado e <archivo1> <archivo2> ... <archivoN> son os diferentes ficheiros que serán empaquetados en <archivoSalida>.

Para acceder a toda a información do comando tar, podemos desde un terminal executar man tar. Tamén se pode consultar a seguinte ligazón, que contén información detallada:

<http://www.gnu.org/software/tar/manual/>

Despois de realizar a empaquetaxe de ficheiros, o ficheiro empaquetado con extensión .tar, que se tratará coma unha copia de seguridade, deberá almacenarse noutra localización, co cal sería conveniente almacenar o ficheiro noutro dispositivo de almacenamento ou, mesmo, nun dispositivo de almacenamento remoto. Deberíanse aplicar as boas prácticas das copias de seguridade comentadas nun apartado anterior a este ficheiro empaquetado.

Indicando a opción apropiada, *tar* tamén permite crear copias de seguridade diferenciais.

Linux proporciona tamén unha forma para a automatización de tarefas usando *crontab* ou o programador de tarefas, que é unha interface gráfica para *crontab*. Para utilizar *crontab* débese coñecer a diferenza del con *cron*. *Cron* é un servizo, un proceso que se executa en segundo plano, sen interactuar co usuario, que se usa para programar tarefas que serán executadas nun tempo específico. Por outra banda, *crontab* é un ficheiro de texto e cada usuario posúe o seu. Neste ficheiro o usuario pode especificar o momento en que se executará unha determinada tarefa. É así como no interior do ficheiro *crontab* se atopa unha lista de comandos e os seus respectivos tempos de execución. Ambos os factores son controlados polo servizo *cron* e lévanse a cabo en segundo plano polo sistema.

Como usuario pódese usar *cron* de dúas formas: editando o ficheiro *crontab* ou mediante o programador de tarefas.

A estrutura dunha entrada no ficheiro *crontab* é a seguinte:

[m] [h] [dom] [mon] [dow][command]

Na seguinte táboa vemos o que significa cada parámetro

Parámetro	Significado	Rango
m	minute (minuto)	0-59
h	hour (hora)	0-23
dom	day of month (día do mes)	1-31
mon	month (mes)	1-12
dow	day of week (día da semana)	1-7

Na seguinte liña podemos ver un exemplo onde se desexa executar un *script* chamado copia_completa.sh o primeiro día de cada mes, ás 9 da tarde:

```
* 21 1 * * /home/proba/copia_completa.sh
```

Pódese obter información máis detallada de *cron* e *crontab* nos seguintes enderezos:

<http://blog.desdelinux.net/cron-crontab-explicados/>

<https://help.ubuntu.com/community/CronHowto>

Outra ferramenta de interese que proporciona Linux é *rsync*, que vén instalada por defecto en Ubuntu. Esta ferramenta é moi potente; permite sincronizar cartafoles de xeito incremental e tamén permite traballar con datos comprimidos e cifrados. Mediante unha técnica de *delta decoding*, permite sincronizar ficheiros e directorios entre dúas máquinas dunha rede ou entre dúas localizacións nunha mesma máquina, reducindo o volume de datos transferidos.

Para obter información máis detallada desta ferramenta pódense consultar as seguintes ligazóns:

<http://www.linuxforu.com/2011/10/backups-and-more-with-rsync/>

<https://help.ubuntu.com/community/rsync>

<http://en.wikipedia.org/wiki/Rsync>

A invocación máis sinxela da aplicación a través da liña de comandos é cando se usa de forma local:

```
rsync [OPCIONS] ... ORIXE [ORIXE]...DESTINO
```

Para o acceso remoto temos dúas opcións:

Cando se realiza a sincronización desde unha orixe local a un destino remoto:

```
rsync [OPCIONS] ... ORIXE [ORIXE]...[USUARIO@]HOST:DESTINO
```

Cando se realiza a sincronización desde un orixe remoto a un destino local:

```
rsync [OPCIONS] ... [USUARIO@]HOST:ORIXE [DESTINO]
```

Onde:

ORIXE: é o ficheiro ou directorio (ou unha listaxe de múltiples ficheiros e directorios) dos que realizar a copia.

DESTINO: é o ficheiro ou directorio onde se realizará a copia.

OPCIONS: opcións para indicar como se realizará a sincronización. As más habituais son:

Opción	Descripción
-a, --archive	Modo arquivado, para obter unha copia exacta da xerarquía de ficheiros e directorios. Igual a usar como opcións -rlptgoD.
-v, --verbose	Para amosar máis información.
-r, --recursiv e	Para copiar de forma recursiva a estrutura dos directorios indicados.
-z, --compres s	A información é comprimida para ser enviada á máquina destino, co que se reduce a cantidad de datos transmitidos.
--delete	Borra ficheiros estranhos desde o lado que recibe os datos, pero só dos directorios que están a ser sincronizados.
-b, --backup	Realiza copias de seguridade. Ficheiros de destino preexistentes son renomeados cando o ficheiro é transferido ou borrado.
-p	Para que se manteñan os permisos.
-o, --owner	Para que se conserve o propietario.
-g, --group	Para que se manteña o grupo.
-t, --times	Para que se manteña a hora do ficheiro.

-D	Para que se manteñan os ficheiros de dispositivo (só para root) e ficheiros especiais.
-l, --links	Para que copie ligazóns simbólicas como ligazóns simbólicas.

Como para usar *rsync* simplemente temos que executar un comando, podemos utilizar *cron* ou a aplicación *Tarefas planificadas* para programar a sincronización. Tamén se pode crear un script que conteña o comando para realizar a sincronización e logo executalo de forma automática, como se fixo en tareas anteriores.

Copias de seguridade con aplicacións específicas

Existe multitud de ferramentas, moitas delas gratuítas, que permiten facer copias de seguridade en Windows ou en Linux. Algunhas delas mesmo son multiplataforma, de xeito que se poden empregar ben en Linux ou ben en Windows. Ao ser más específicas que as ferramentas incluídas nos sistemas operativos, fan que teñan opcións moi interesantes á hora de realizar copias de seguridade, como son que poden elixirse distintos algoritmos de cifraxe ou que permiten compresión.

Windows

Cobian Backup é unha das ferramentas gratuítas para sistemas operativos Windows. Este programa é multitarefa, co que se poden crear copias de seguridade de xeito local, nunha rede local ou mesmo en/desde un servidor FTP.

As características que achega esta aplicación son as seguintes:

Consumo poucos recursos e pode estar funcionando en segundo plano.

Permite programar tarefas para realizarse no instante, de xeito diario, semanal, mensual, anual ou nun tempo especificado.

Permite realizar calquera tipo de copias de seguridade: completa, incremental ou diferencial.

Soporta compresión ZIP ou 7Zip.

Ofrece a opción de protexer todas as funcións do programa por contrasinal.

Existe a opción de cifrar os seus ficheiros usando catro métodos diferentes de cifraxe forte.

Pode definir eventos disparados antes ou despois da copia, como por exemplo provocar o pechamento dun determinado programa que utilice un ficheiro que se vai copiar e facer que logo de iniciada a copia se volva iniciar.

Para maior información, pódese consultar a web oficial do programa en:

<http://www.cobiansoft.com>

Outra aplicación que podemos usar en Windows para facer copias de seguridade e restauracións é Areca. A súa principal vantaxe é que é "open source" e pode executarse tanto en Windows como en Linux. Así, todas as características e a tarefa realizada con este software poden aplicarse tanto a un sistema operativo Linux coma a un Windows. A ferramenta, ademais, pódese utilizar coa interface gráfica ou a través da liña de comandos.

Para consultar más información e características detalladas, pódese consultar a páxina web oficial:

<http://www.areca-backup.org>

Linux

En Linux tamén se poden instalar ferramentas específicas, como en Windows, para poder realizar copias de seguridade. Por exemplo, a aplicación Areca Backup pode tamén instalarse en Linux, co cal o modo de traballo e as características van ser idénticas. Así que, se instalamos Areca nunha máquina con Linux, poderíamos realizar a mesma tarefa que a Tarefa.

Na seguinte ligazón amósase unha táboa con máis aplicacións que se poden utilizar en Ubuntu para crear copias de seguridade:

<https://help.ubuntu.com/community/BackupYourSystem>