

Copias de Seguridad

Administración Avanzada de Sistemas Operativos

Eduardo Iniesta Soto (eniesta@dittec.um.es)

CONTENIDOS

- Contexto
 - Almacenamiento de la información
 - Motivación
 - Tipos de copia
 - Política de copia

- Tipos de soporte

- Sistema de backup nativos
 - Windows
 - Linux

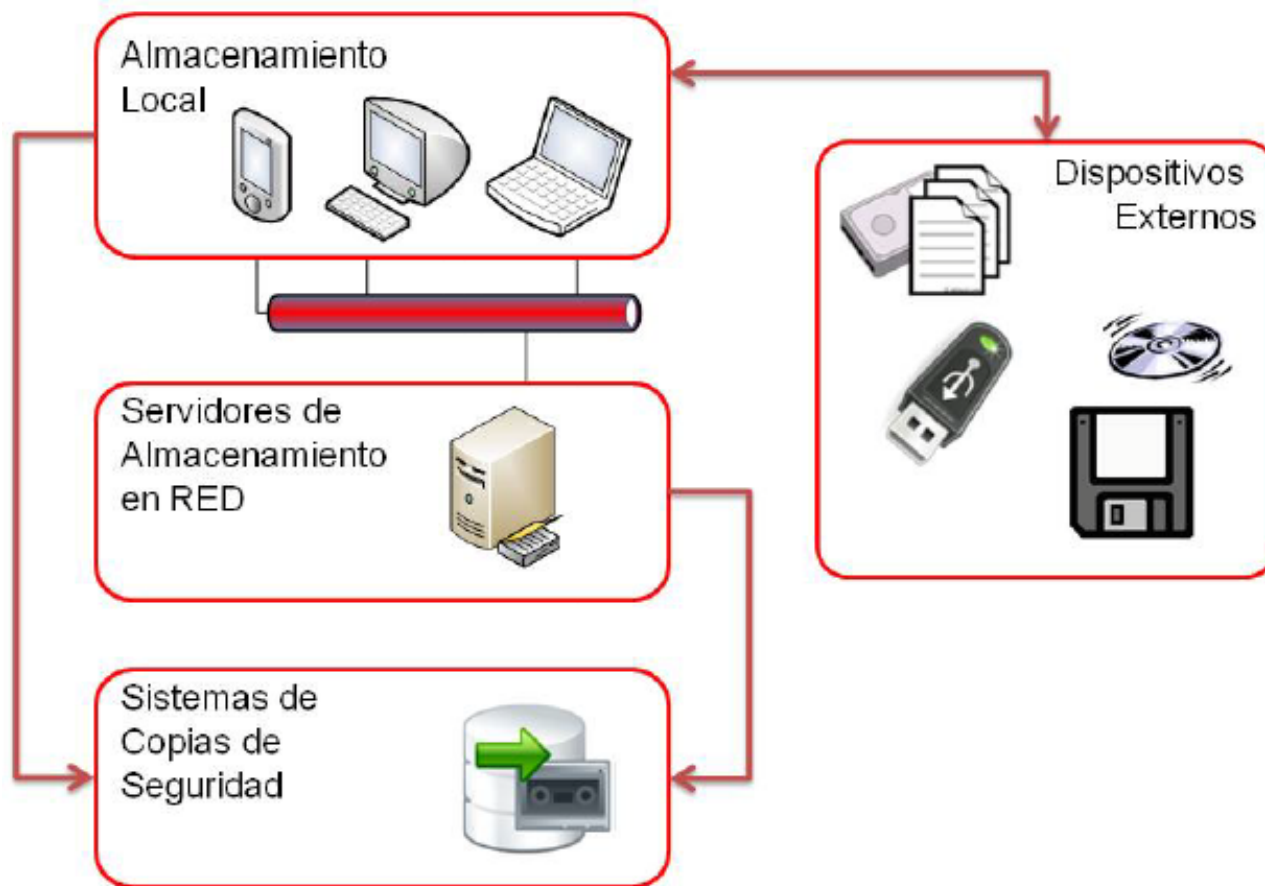
CONTENIDOS

- Copias de seguridad en la nube
 - Ventajas y riesgos
 - Dropbox

- Sistemas de versionado
 - Instantáneas de volumen
 - Subversion

CONTEXTO

- Almacenamiento de la información:
 - La mayoría de las organizaciones utilizan varios sistemas de almacenamiento.



CONTEXTO

- Almacenamiento de la información (cont.):
 - Almacenamiento local:
 - Disco duro de equipos de sobremesa y portátiles.
 - Política:
 - ¿Qué archivos está permitido guardar?
 - ¿En qué directorios?
 - ¿Cuáles de esos archivos deberían estar cifrados?
 - ¿Durante cuánto tiempo se permite su existencia?
 - Dispositivos externos:
 - CD/DVD, pendrives, discos externos por USB o Firewire.
 - Política:
 - ¿Puede el usuario de un equipo de sobremesa utilizarlos?
 - ¿Qué información es posible guardar en ellos?

CONTEXTO

- Almacenamiento de la información (cont.):
 - Servidores de almacenamiento:
 - También denominados “servidores de ficheros”. Disponen de discos de gran capacidad y elevadas prestaciones.
 - Política:
 - Normalmente cada usuario de la organización tiene asignada una carpeta personal de uso exclusivo.
 - Además, existen otras carpetas comunes en donde se guarda la información que deba ser compartida por todos los usuarios.
 - Implementación:
 - Windows: carpetas compartidas en grupos de trabajo ó Active Directory.
 - Linux: NFS combinado con NIS ó con OpenLDAP.
 - Se recomienda instalar un servidor FTP, y clientes FTP en los equipos locales.

CONTEXTO

- Almacenamiento de la información (cont.):
 - Sistemas de copia de seguridad (o “backup”):
 - Pueden estar basados en software nativo (del propio sistema operativo) o propietario (adquirido por separado).
 - Están relacionados con todo tipo de servidores (no sólo con servidores de ficheros).
 - Dispositivos más utilizados: cinta magnética, discos externos, CD/DVD.
 - Política:
 - Es de suma importancia realizar un diseño adecuado.
 - Se deben tener en cuenta todos los factores con posible incidencia en su eficacia: frecuencia de las copias, dispositivos de respaldo, pruebas, etc.

CONTEXTO

- Motivación: Corregir las consecuencias de...
 - Fallo físico en el dispositivo de almacenamiento:
 - Por causas exógenas (picos de tensión en la red eléctrica).
 - Por causas endógenas (degradación del propio dispositivo).
 - Fallo lógico en el software:
 - “Cuelgues” del sistema operativo.
 - Funcionamiento anómalo del SGBD.
 - Errores humanos:
 - Equívocos a la hora borrar archivos.
 - Cambios indebidos/inadvertidos en el contenido de los ficheros.

CONTEXTO

- Motivación (cont.): Corregir las consecuencias de...
 - Virus:
 - Corrupción de archivos infectados.
 - Desastres:
 - Originados por la naturaleza: inundaciones, terremotos...
 - Originados por el hombre: incendios, terrorismo...

CONTEXTO

- Tipos de copia:
 - **Ámbito:** en todos los casos, un sistema de ficheros o una parte de él (uno o varios de sus directorios).
 - **Copias de seguridad completas:**
 - Copia de todos los ficheros del ámbito seleccionado.
 - **Copias de seguridad incrementales:**
 - Copia de todos los ficheros del ámbito seleccionado que hayan cambiado desde otra copia que se utiliza como referencia. Sistema de niveles:
 - Nivel 0: Equivale a una copia de seguridad completa.
 - Nivel 1: Sólo se incluyen en la copia aquellos ficheros que hayan sido modificados desde la última copia de nivel 0.

CONTEXTO

- Tipos de copia (cont.):
 - Copias de seguridad incrementales:
 - Sistema de niveles (cont.):
 - Nivel 2: Sólo se incluyen en la copia aquellos ficheros que hayan sido modificados desde la última copia de nivel 1. Si no existiese ninguna copia de nivel 1, se considera que la copia de nivel 2 es realmente una copia de nivel 1.
 - ...
 - Nivel **n**: Sólo se incluyen en la copia aquellos ficheros que hayan sido modificados desde la última copia de nivel **n-1**. Si no existiese ninguna copia de nivel **n-1**, se considera que la copia de nivel **n** es realmente una copia de nivel **n-1**.

CONTEXTO

- Tipos de copia (cont.):

- Ejemplos:

- Sistema de ficheros con pocos cambios a lo largo del tiempo:
 - Copia de seguridad completa el último día de cada mes.
- Sistema de ficheros con cambios muy frecuentes:
 - Copia de seguridad completa a las 02:00 AM de cada día.
- Sistema de ficheros con cambios relativamente frecuentes:
 - Copia de nivel 0 a las 00:00 AM del primer día de cada mes.
 - Copia de nivel 1 a las 02:00 AM del primer día de cada semana.
 - Copia de nivel 2 a las 04:00 AM de cada día.

CONTEXTO

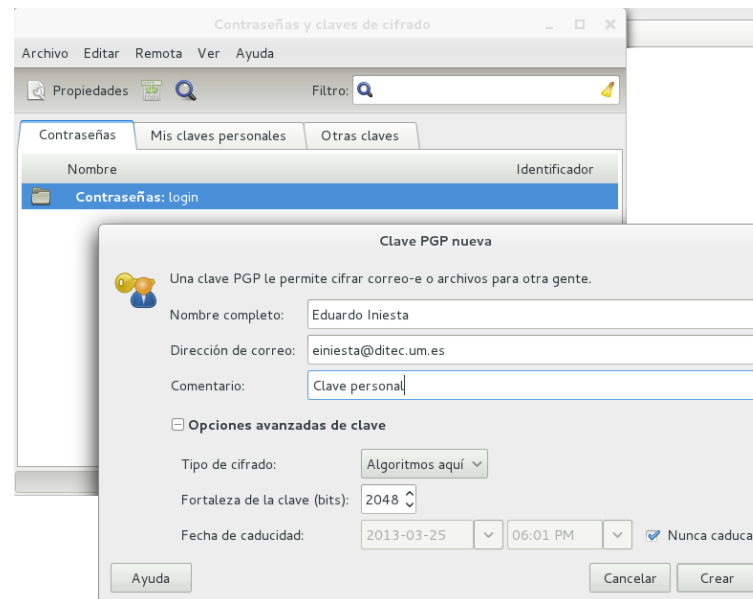
- Tipos de copia (cont.):
 - Algoritmo de recuperación de copias incrementales:
 - 1. Restaurar la copia de nivel 0 más reciente.
 - 2. De todas las copias de nivel 1, restaurar la más reciente.
 - 3. De todas las copias de nivel 2 posteriores a la copia anterior, restaurar la más reciente.
 - 4. De todas las copias de nivel 3 posteriores a la copia anterior, restaurar la más reciente.
 - 5. Repetir el proceso hasta restaurar la última copia incremental.
 - Ejemplo (restauración el 28/03/12 -miércoles-):
 - Restaurar la copia de nivel 0 del 01/03/12 - 00:00 AM.
 - Restaurar la copia de nivel 1 del 26/03/12 - 02:00 AM (lunes).
 - Restaurar la copia de nivel 2 del 28/03/12 - 06:00 AM.

CONTEXTO

- Política de copia:
 - Identificar los datos a incluir en la copia:
 - ¿Sistema de ficheros completo?
 - Ver las ventajas de un esquema de particiones bien diseñado.
 - Automatizar las copias y fijar su frecuencia:
 - Llevar a cabo las copias en los momentos de baja actividad.
 - Utilizar sistemas de ejecución automáticos (**crontab** en Linux, **programador de tareas** en Windows, etc).
 - Planificar copias completas y/o incrementales en función de la frecuencia de los cambios y de la inmediatez exigible a las restauraciones.
 - Etiquetar los soportes de copia adecuadamente:
 - Qué contiene el soporte y la fecha de copia.
 - Instrucciones para recuperar su contenido (breves y claras).

CONTEXTO

- Política de copia (cont.):
 - Proteger los soportes y su contenido:
 - Protección física: pestaña contra escritura, almacenamiento bajo llave, condiciones ambientales apropiadas, etc.
 - Protección lógica: si la ley o la prudencia lo exigen, cifrar los datos de la copia. Posibilidades:
 - Encriptar ficheros:



CONTEXTO

- Política de copia (cont.):
 - Proteger los soportes y su contenido:
 - Protección lógica: si la ley o la prudencia lo exigen, cifrar los datos de la copia. Posibilidades:
 - Encriptar particiones:



CONTEXTO

- Política de copia (cont.):
 - Almacenar las copias en un edificio distinto al del centro de datos:
 - La ubicación en una planta distinta no garantiza que un hipotético desastre no afecte simultáneamente al centro de datos y al almacenaje de las copias.
 - Mal menor: duplicar copias mensuales y enviar una de las copias a otro edificio.
 - Probar las copias periódicamente:
 - La primera vez de forma completa y exhaustiva, restaurándola por completo en un entorno de prueba para constatar su validez.
 - Periódicamente realizar restauraciones para comprobar el buen estado de los soportes de almacenamiento.
 - Anticiparse al tiempo máximo de vida del soporte, sustituyéndolo con cierto margen de antelación.

CONTEXTO

- Política de copia (cont.):
 - Antes de desechar un soporte, asegurarse de que su información ya no es accesible:
 - Soportes magnéticos: formateo.
 - Soportes ópticos: destrucción.

CONTEXTO

➤ Referencias normativas:

- Ley Orgánica de Protección de Datos de Carácter Personal:
 - El reglamento que la desarrolla exige el cifrado de las copias cuando contengan datos que deban gozar de una protección especial (medidas de seguridad de nivel alto).
- ISO 27002:
 - Control 10.5.1: Establecimiento de procedimientos de copia de seguridad.

TIPOS DE SOPORTE

- Soportes magnéticos:
 - Discos duros internos:
 - Rápidos, de gran capacidad y relativamente económicos.
 - Recomendación: acceder a los discos de copia mediante la red (compartición NFS -Linux- o CIFS -Windows-).
 - Discos duros externos:
 - Portables, de gran capacidad y económicos, pero más lentos que los discos internos.
 - Interfaces: USB / Firewire.

TIPOS DE SOPORTE

- Soportes magnéticos (cont.):

- Cintas:

- De copia y restauración lentas, pero económicas y de gran capacidad.
 - Ejemplo: LTO (Linear Tape Open). Última versión: LTO-5 (1.5 TB de capacidad).



TIPOS DE SOPORTE

- Soportes electrónicos:
 - Pendrives:
 - Muy portables y económicos, pero con baja capacidad de almacenamiento.
 - Útiles para transportar información off-line, pero se desaconseja su uso como soportes para copia de seguridad.

- Soportes ópticos:
 - CD/DVD/Blu-Ray:
 - Muy económicos y con capacidad de almacenamiento moderada.
 - Vida útil superior a 10 años, en condiciones ambientales apropiadas.
 - Recomendables para copias que previsiblemente no vayan a ser recuperadas en mucho tiempo.

SISTEMAS DE BACKUP NATIVOS

➤ Windows:

- Existe el atributo booleano **Archivo**, que se activa en un fichero cada vez que éste cambia. Las distintas modalidades de copia “pivotan” sobre el atributo **Archivo**:
 - Copia completa: Se incluyen en la copia todos los ficheros seleccionados, tengan o no activo el atributo **Archivo**. Se desactiva el atributo **Archivo** de todos los ficheros copiados.
 - Copia por copia: Similar, pero el atributo **Archivo** no se desactiva.
 - Copia diferencial: Se incluyen en la copia sólo aquellos archivos que tengan activo el atributo **Archivo**. Con la copia de cada fichero no se desactiva **Archivo**.
 - Copia incremental: Se incluyen en la copia sólo aquellos archivos que tengan activo el atributo **Archivo**. En este caso, sí se activa el atributo **Archivo**.
 - Copia diaria: No se lee ni se actualiza el atributo **Archivo**. Sólo se consideran los ficheros con fecha de modificación igual a la actual.

SISTEMAS DE BACKUP NATIVOS

- Windows (cont.):
 - Windows Server 2003:
 - **ntbackup:**
 - Ejecutable por línea de comandos o por interfaz gráfica.
 - Permite realizar copias completas, incrementales y diferenciales.
 - Windows Server 2008:
 - **Copia de seguridad:**
 - Interfaz gráfica.
 - Guarda automáticamente un histórico de las copias realizadas.
 - Permite realizar copias completas, por copia e incrementales.
 - **wbadmin:**
 - Ejecutable por línea de comandos.
 - Guarda automáticamente un histórico de las copias realizadas.
 - No tiene en cuenta el atributo **Archivo**.

SISTEMAS DE BACKUP NATIVOS

➤ Linux:

• Todas las distribuciones:

- **tar:**

- Realiza copias de seguridad de ficheros y/o directorios.
- Por defecto sólo empaqueta, aunque se le puede indicar que comprima.
- Sólo lleva a cabo copias completas (no permite las incrementales).
- El destino puede ser un fichero o un dispositivo.

- **cpio:**

- Realiza copias de seguridad de un conjunto arbitrario de ficheros.
- Sólo empaqueta.
- Sólo permite copias completas.
- El destino puede ser un fichero o un dispositivo.

SISTEMAS DE BACKUP NATIVOS

➤ Linux (cont.):

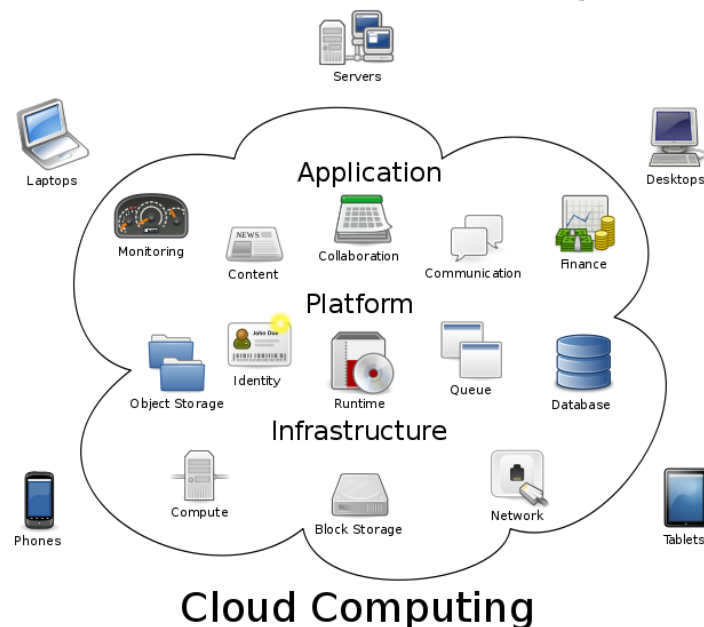
• Todas las distribuciones:

- **dump:**

- Hace copias completas de un sistema de ficheros Linux.
- El destino ha de ser necesariamente un dispositivo (una partición o una cinta, por ejemplo).
- Permite copias que ocupan más de una cinta.
- Conserva el usuario y grupo propietarios de cada fichero, y también sus permisos.
- Permite copias completas (nivel 0) e incrementales (niveles del 1 al 9).
- En el modo de restauración (comando restore) se puede recuperar un sistema de ficheros completo, o ficheros/directorios aislados (de forma interactiva).

COPIAS DE SEGURIDAD EN LA NUBE

- Computación en la nube:
 - Características generales:
 - Uso de recursos hardware y/o software por vía telemática.
 - Estos recursos se encuentran en una “nube” de Internet y -generalmente- no son nuestros (pagamos por su utilización).
 - Al ser un acceso telemático basado -generalmente- en una interfaz web, se pueden consumir desde cualquier dispositivo.

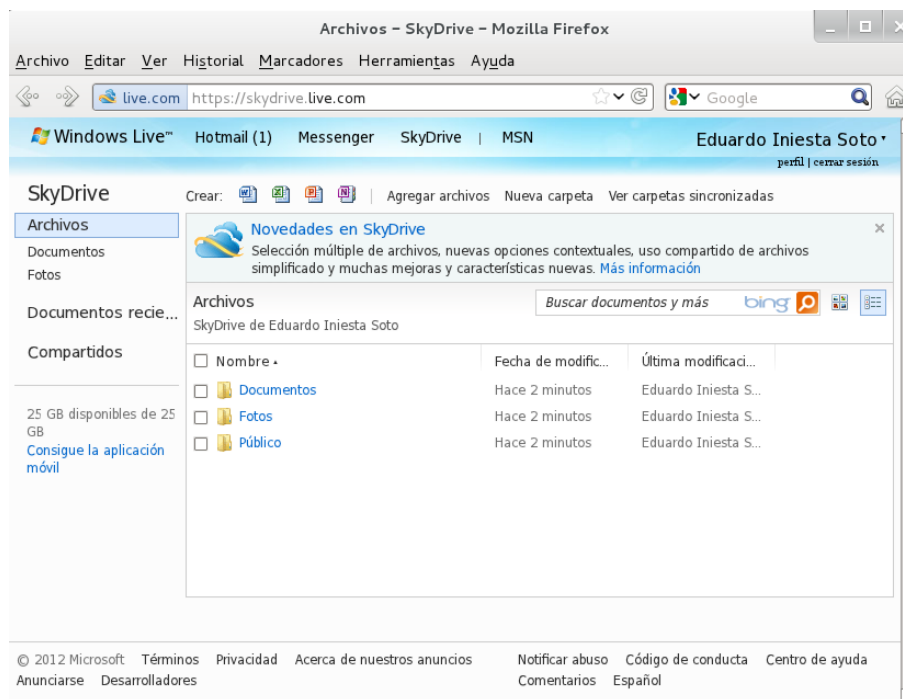


COPIAS DE SEGURIDAD EN LA NUBE

- Computación en la nube:
 - Niveles de Servicio:
 - Infraestructura como servicio:
 - El proveedor de la nube ofrece servidores (casi siempre en entornos virtualizados) y discos; el cliente de la nube puede disponer de estos recursos para instalar su propio sistema operativo y el resto de software.
 - Se paga en función de la capacidad de cómputo del servidor alquilado, o, si es un disco, del espacio disponible.
 - Ejemplos:
 - Uso de servidores virtualizados:
 - Amazon EC2.

COPIAS DE SEGURIDAD EN LA NUBE

- Computación en la nube:
 - Niveles de Servicio:
 - Infraestructura como servicio:
 - Ejemplos (cont.):
 - Uso de espacio en disco:
 - Amazon S3, DropBox, Microsoft SkyDrive, etc.



COPIAS DE SEGURIDAD EN LA NUBE

- Computación en la nube:
 - Niveles de Servicio:
 - Plataforma como servicio:
 - El proveedor de la nube ofrece un entorno de programación determinado, o un lugar en el que alojar las aplicaciones desarrolladas.
 - Ejemplos:
 - Google App Engine: Aplicaciones web escritas en Java o Python, utilizando el IDE Eclipse.
 - Windows Azure: Aplicaciones web escritas en .NET, Java o PHP (entre otros), utilizando el IDE Microsoft Visual Studio 2010.

COPIAS DE SEGURIDAD EN LA NUBE

➤ Computación en la nube:

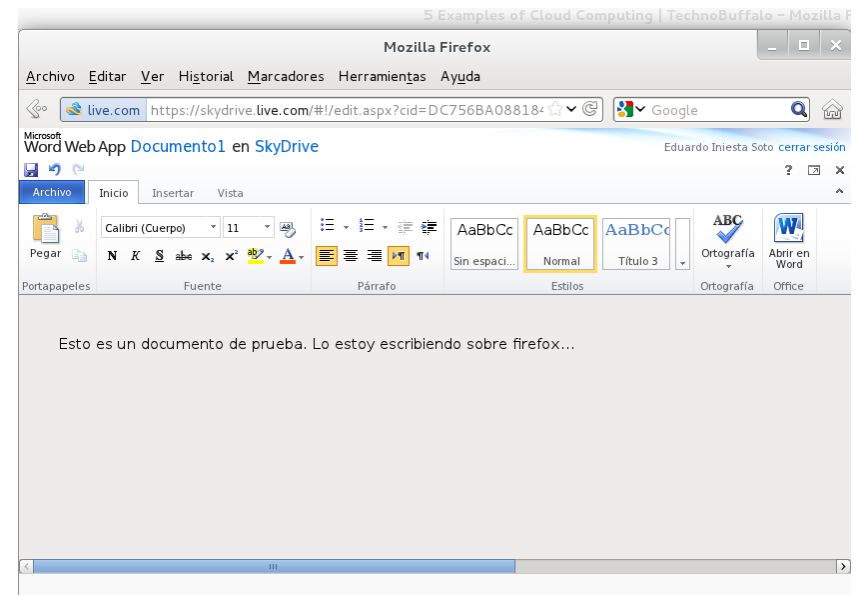
• Niveles de Servicio:

- Software como servicio:

- El proveedor de la nube ofrece un programa completo, ejecutable desde un navegador (sin necesidad de instalar nada).

• Ejemplos:

- Gmail.
- Microsoft Skydrive.
- Microsoft Office 365.



COPIAS DE SEGURIDAD EN LA NUBE

➤ Computación en la nube:

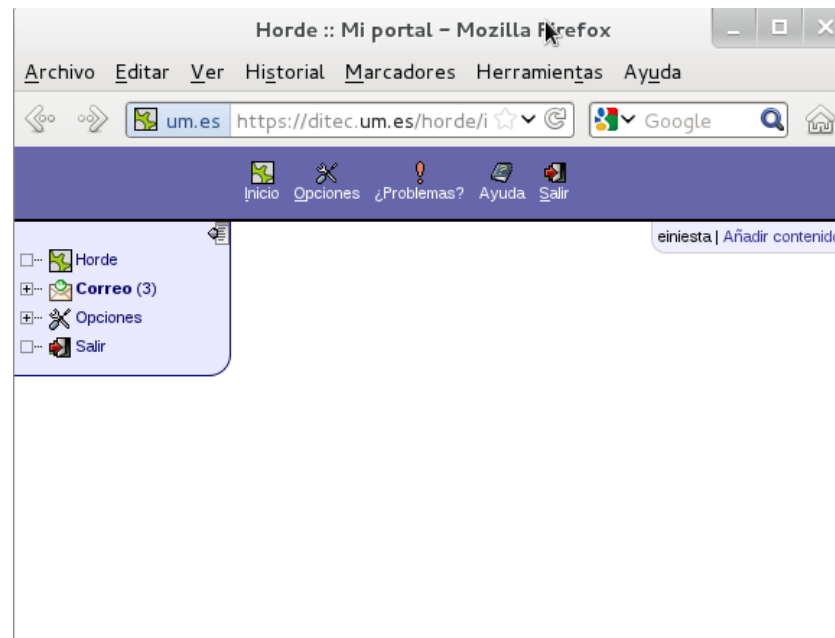
• Tipos de nubes:

- Nubes públicas: Gestionadas y administradas por grandes compañías que prestan servicio a muchos clientes.

• Ejemplos: Google, Microsoft, Amazon, Dropbox...

- Nubes privadas: Gestionadas y administradas sólo por el propio cliente que las consume.

• Ejemplo: Nube de DITEC.



COPIAS DE SEGURIDAD EN LA NUBE

- Computación en la nube:

- Ventajas:

- Servicios accesibles desde cualquier dispositivo con acceso a Internet.
 - Inversión inicial menor.
 - Mantenimiento del hardware y software a cargo del proveedor.
 - Confidencialidad e integridad de los datos aseguradas.
 - Alto nivel de escalabilidad.
 - Ahorro en costes energéticos.

COPIAS DE SEGURIDAD EN LA NUBE

➤ Computación en la nube:

• Inconvenientes:

- ¿Estamos seguros de que el proveedor cuenta con una conexión a Internet de alta velocidad y estable?
- ¿Confiamos en que el proveedor proteja nuestros datos ante ataques?
- ¿Hasta qué punto podemos asumir nuestra dependencia del proveedor?
- ¿Se utilizan en la transmisión de información protocolos seguros?
- Para datos protegidos legalmente (LOPD, por ejemplo), ¿cumple el proveedor con la ley?

COPIAS DE SEGURIDAD EN LA NUBE

➤ Dropbox:

• Características generales:

- Servicio de almacenamiento en la nube (infraestructura como servicio).
- Gratuito hasta 2 GB.
- Opciones:
 - Acceso a nuestra cuenta dropbox vía web.
 - Instalar un cliente dropbox en uno o varios equipos (Windows o Linux).
- En el equipo cliente se crea una carpeta “Dropbox” en el perfil local del usuario, cuyo contenido se mantiene sincronizado con otras carpetas “Dropbox” que ese mismo usuario esté utilizando en otros equipos.
- La sincronización también existe con el almacenamiento web de Dropbox para ese usuario.

COPIAS DE SEGURIDAD EN LA NUBE

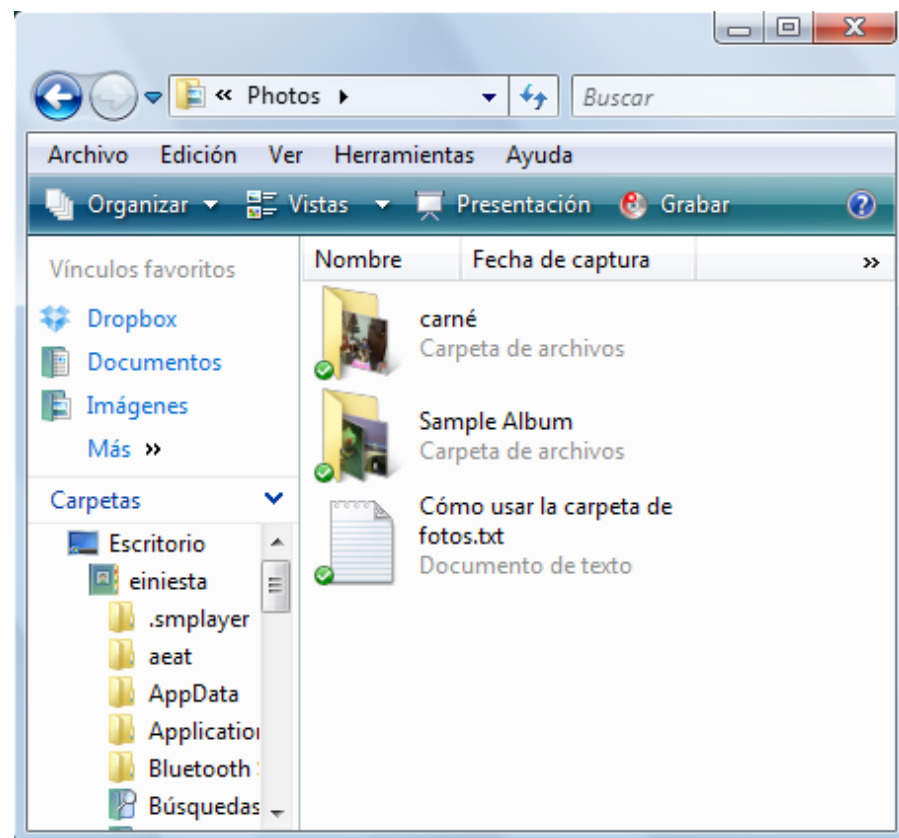
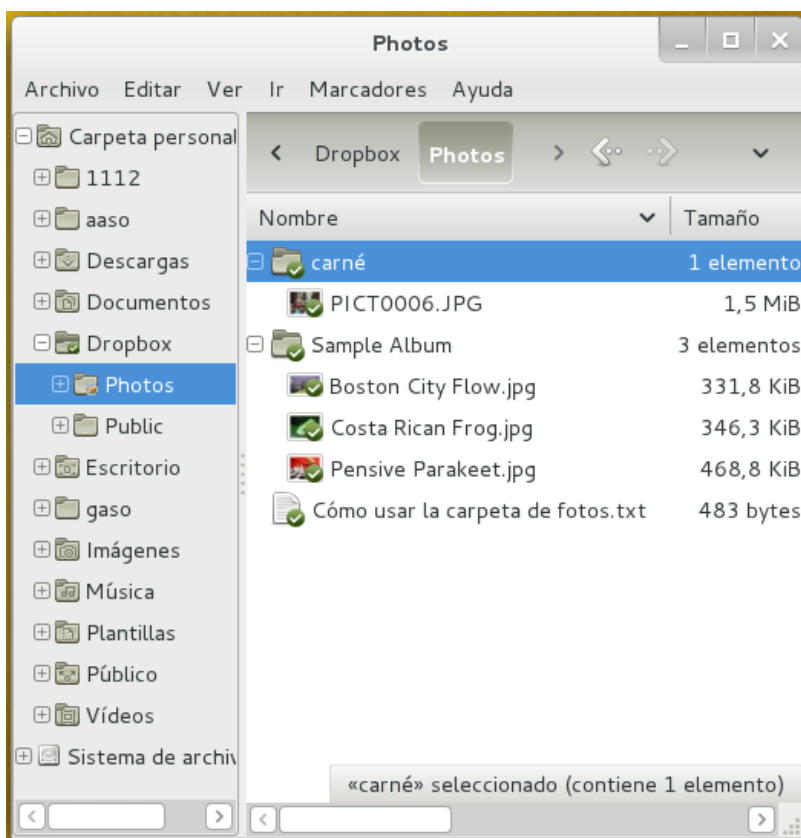
➤ Dropbox:

• Características generales (cont.):

- Posibilidad de compartir una carpeta entre varios usuarios con cuenta de Dropbox.
- Control de versionado.
- Comunicaciones cifradas entre los clientes y el servidor Dropbox (basadas en SSL).
- Ficheros encriptados en el servidor (AES-256).

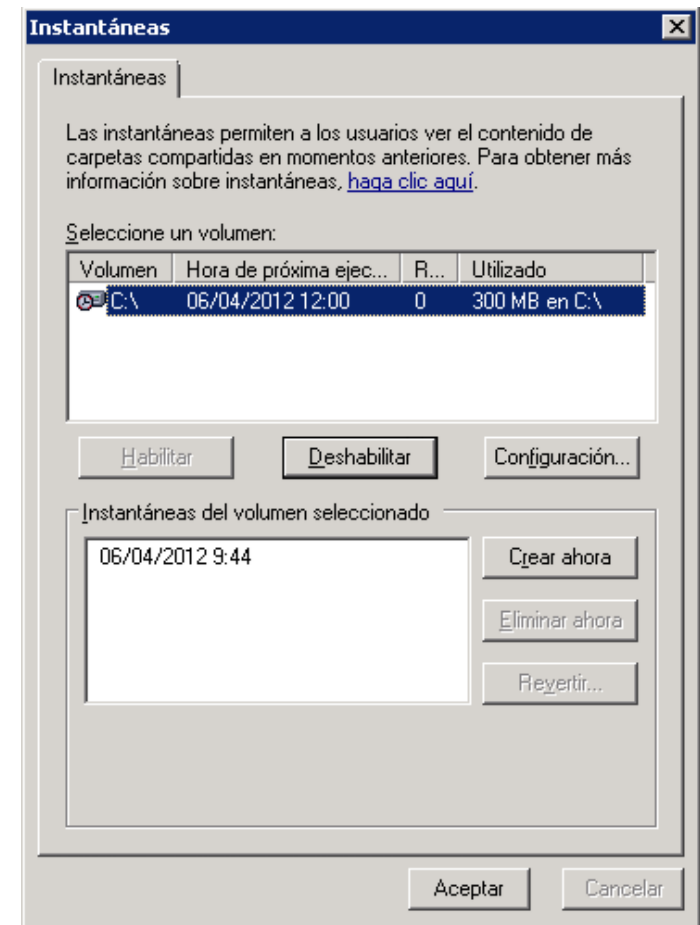
COPIAS DE SEGURIDAD EN LA NUBE

- Dropbox:
 - Ejemplo de sincronización: una misma cuenta de Dropbox accedida desde un cliente Linux y otro Windows:



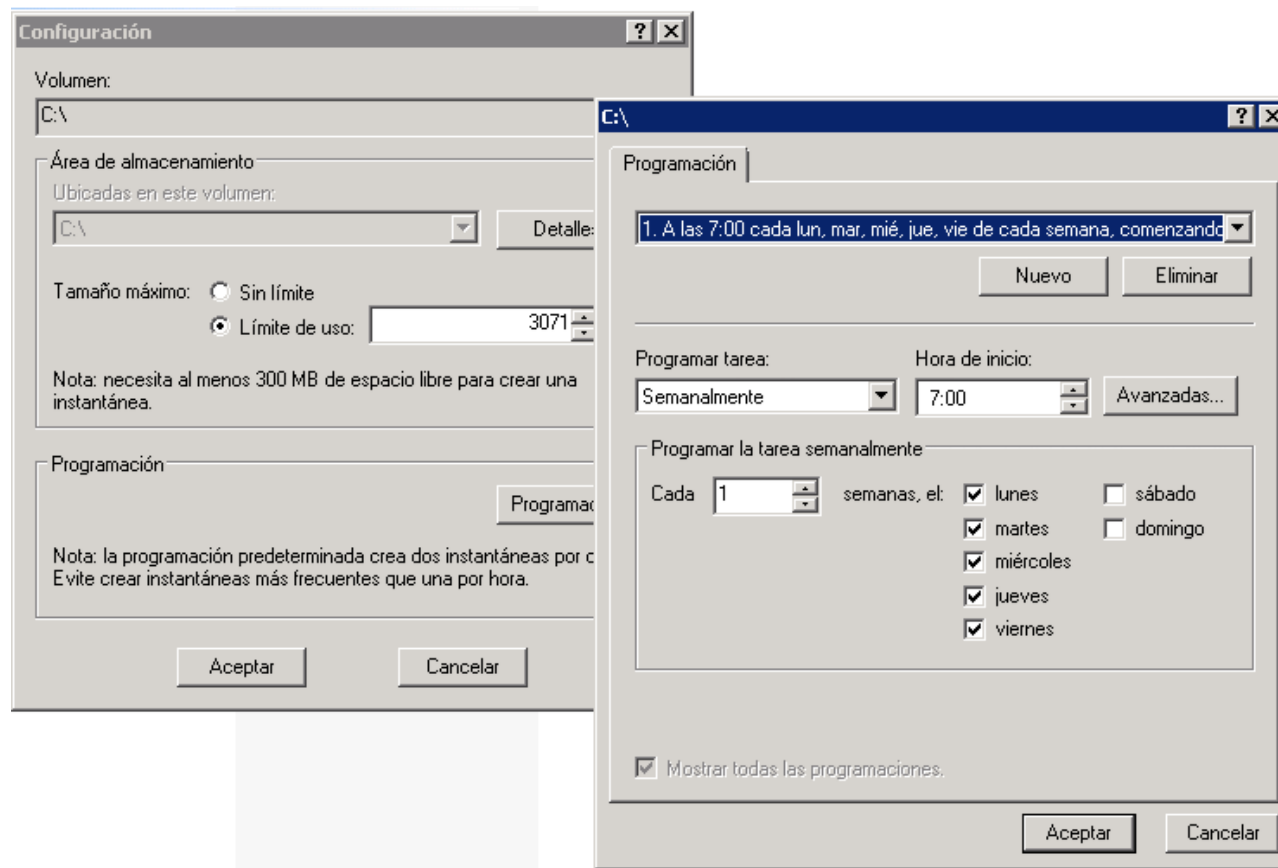
SISTEMAS DE VERSIONADO

- Instantáneas de volumen:
 - Servicio disponible en Windows Server.
 - Permite guardar “fotografías” de un volumen en un instante determinado.
 - Características generales:
 - Servicio: VSS (Volume Shadow Copy).
 - Ubicación por defecto: \
 - Espacio consumido: configurable (por defecto, el 10% del volumen).
 - Número máximo de instantáneas: 64.



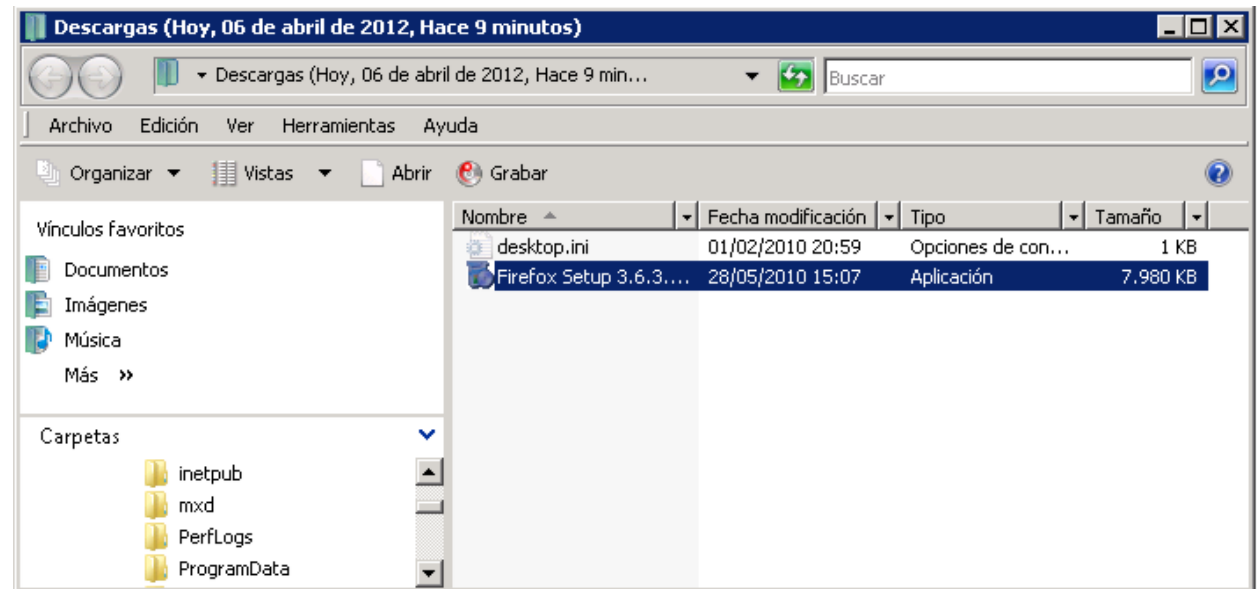
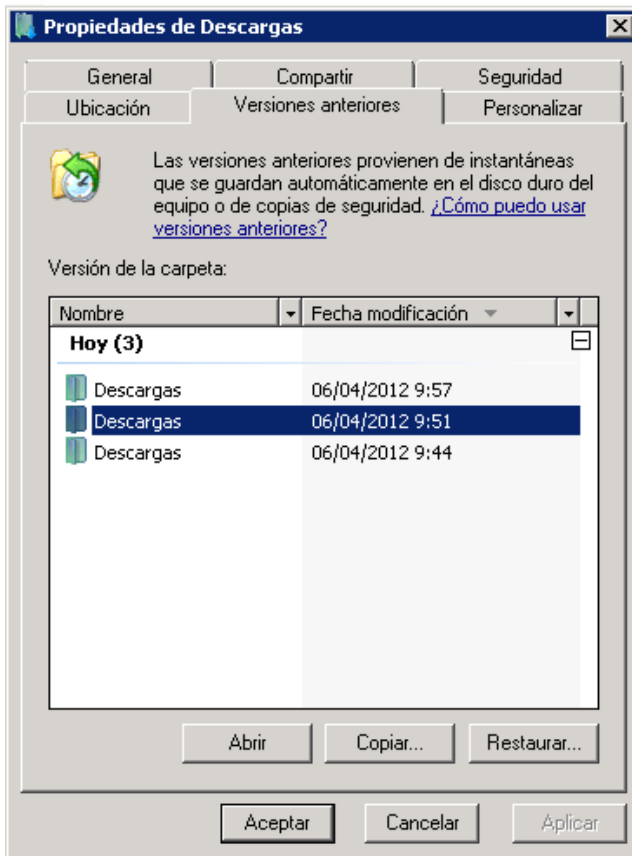
SISTEMAS DE VERSIONADO

- Instantáneas de volumen:
 - Características generales (cont.):
 - Periodicidad de las instantáneas: configurable.



SISTEMAS DE VERSIONADO

- Instantáneas de volumen:
 - Recuperación de versiones parcial o total (no se exige recuperar la “fotografía” del volumen completo).



SISTEMAS DE VERSIONADO

➤ Subversion:

- ¿Qué es?

- Sistema de control de versiones de archivos que son compartidos por varios usuarios.
- Muy apropiado para favorecer la comunicación y colaboración en entornos académicos y profesionales.
- Infraestructura: una nube privada, con...
 - Un servidor Subversion, bajo Linux.
 - Varios clientes Subversion, bajo Linux o Windows.

SISTEMAS DE VERSIONADO

➤ Subversion:

• Características generales:

- Todas las versiones permanecen guardadas en un repositorio del servidor Subversion.
- Cada version está identificada por un número de revisión, e integra una “fotografía” de todos los archivos gestionados por Subversion.
- Permite la recuperación separada de versiones de archivos.
- Envía por la red sólo los archivos nuevos o modificados.
- Gestión de versiones transaccional.
- Posibilidad de exigir autenticación a los usuarios.
- Posibilidad de implementar permisos de acceso diferentes (sólo lectura ó lectura/escritura) para cada posible usuario (incluyendo, si se desea, al “usuario anónimo”).

SISTEMAS DE VERSIONADO

➤ Subversion:

• Servidor Subversion:

- Paquete: “subversion”.
- Demonio: “svnserve”.
- Protocolo utilizado: svn.
- Puerto utilizado (por defecto): 3690.
- Comandos:
 - **svnadmin create:** Creación del repositorio.
 - **svn import:** Importación directa al repositorio de un directorio.
- Ficheros de configuración (en **<rutaRepos>/conf**):
 - **svnserve.conf:** Parámetros de configuración generales.
 - **authz:** Permisos de L o L/E para los usuarios.
 - **passwd:** Contraseñas asignadas a los usuarios.

SISTEMAS DE VERSIONADO

➤ Subversion:

• Cliente Subversion:

- Paquete: “subversion”.

- Comandos:

- **svn checkout:** Descarga el repositorio completo.
- **svn add:** Añade un fichero a la lista de altas.
- **svn delete:** Añade un fichero a la lista de bajas.
- **svn revert:** Deshace los cambios hechos en local.
- **svn commit:** Envía cambios al repositorio.
- **svn update:** Actualiza a una versión (la última, por defecto).
- **svn status:** Lista el historial de cambios en local.
- **svn log:** Lista el historial de versiones del repositorio.

SISTEMAS DE CONTROL DE VERSIONADO

- Subversion:
 - Otros clientes Subversion:
 - Subclipse: plugin para Eclipse.
 - TortoiseSVN: cliente Windows.

