Trabajo Final de Carrera

Copias de seguridad:
Estudio y metodología.

Memoria

Autor: Rafael Santamaría Carmona

Consultor: Juan José Cuadrado Gallego

CONTENIDO

1 INTRODUCCIÓN

En el año 2011, sólo en la red se generaron alrededor de 1.8 Zettabytes[1] de datos, y según las previsiones la cifra se duplicará en el transcurso del año 2013.

A medida que la cantidad de datos generada por la sociedad actual aumenta, lo hace en igual medida el riesgo de perder parte de ellos (o todos) de una manera irreversible si no se aplican políticas de copia de seguridad adecuada.

El verdadero problema surge cuando esa posible pérdida se produce en el seno del mundo empresarial, ya que puede llegar a afectar muy negativamente a la estabilidad de las empresas debido, no únicamente a pérdidas económicas, sino también a daños de imagen corporativa, pérdida de confianza o confidencialidad.

Según un estudio realizado por *Price Whaterhouse coopers* (MKM Publicaciones, 2012), un solo incidente de pérdida de datos cuesta a las empresas una media de 7.000 Euros. Otro estudio realizado en este caso por *Gartnes* revela que el 25% de los usuarios de ordenadores personales pierden datos cada año y que el 80% de las empresas que sufren una importante pérdida de datos o un fallo de seguridad durante más de 24 horas cierran al cabo de un año.

Cibecs, en su informe anual correspondiente al año 2011, titulado *"Business Data Loss Survey"* (Cibecs, 2012), en el que tomaron parte más de 250 empresas con un número de empleados comprendido entre 1 y más de 10.000, concluyó que las principales causas de pérdida de datos en las empresas son cinco:

- **Robo (18%)**: principalmente de ordenadores portátiles y memorias USB[2].
- **Negligencia (29%)**: borrado accidental de datos, modificaciones no deseadas, sobre escritura de archivos, etc.
- **Fallo del Hardware (36%)**: fallo de dispositivos, drivers, corrupción de archivos, etc.
- **Virus (9%)**: virus, troyanos, gusanos, etc.
- **Fallos de migración de datos (8%)**.

[1] Un Zettabyte equivale a 10^{15} Gb, o lo que es lo mismo, a 10^{21} Bytes.
[2] Un estudio realizado por *Kingston Technology* y el *Instituto Ponemon* desvela que el 62% de las empresas europeas pierden datos confidenciales por el extravío o robo de memorias USB (Techweek Informes, 2011).

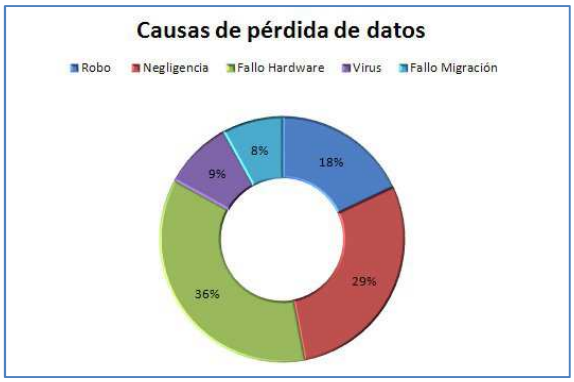


Ilustración 1. Principales causas de pérdida de datos en las empresas.

Ante estos hechos es pues, fundamental la aplicación de políticas de copias de seguridad adecuadas, ya que son la única manera de proteger la inversión realizada en los datos.

1.1 OBJETIVOS

El presente estudio tiene como objetivo el servir de referencia a futuros trabajos de ingeniería del software orientados a la planificación y creación de políticas de copias de seguridad.

Una vez finalizado el estudio se habrá alcanzado una compresión suficiente acerca de, entre otras, cuestiones tales como qué son, de qué manera funcionan y cuáles son las distintas modalidades y modos de gestión disponibles a la hora de diseñar una aplicación de copias de seguridad.

1.2 METODOLOGÍA

Con motivo de alcanzar el objetivo marcado, se ha estructurado el trabajo a desarrollar en tres fases distintas que, de una manera progresiva, servirán para asentar las bases de conocimiento necesarias para elaborar la planificación de una buena estrategia de copias de seguridad.

En la primera fase, además de efectuar un breve recorrido a lo largo de la historia de las copias de seguridad, se expondrán las herramientas de las que en la actualidad se dispone para la elaboración de copias de respaldo.

En una segunda fase, de marcado carácter didáctico, se expondrá la metodología a seguir a la hora de planificar correctas políticas de copias de seguridad.

Finalmente en la tercera y última fase, se desarrollará un caso práctico en el que se planificarán las copias de seguridad en el seno de una organización de tamaño medio, concretamente una notaría. Para la consecución de dicha tarea se aplicará, de una manera concreta y comentada, la metodología explicada en la fase anterior.

La división metodológica del trabajo realizado en las tres fases anteriormente comentadas, ofrecerá como resultado un documento estructurado en ocho capítulos[3] que a continuación se citan de manera esquemática:

Fase 1	Capítulo II – Las copias de seguridad a lo largo de la historia. Capítulo III – Dispositivos de almacenamiento. Capítulo IV – Las copias de seguridad y el estándar ISO. Capítulo V – Modelos de copias de seguridad. Capítulo VI – Gestión de copias de seguridad.
Fase 2	Capítulo VII – Metodología de copias de seguridad. Capítulo VIII – Plan de recuperación de desastres. Fundamentos.
Fase 3	Capítulo IX – Caso práctico

[3] La estructura en ocho capítulos no tiene en cuenta los correspondientes a la introducción, bibliografía y anexos.

2 LAS COPIAS DE SEGURIDAD A LO LARGO DE LA HISTORIA

El diccionario de la Universidad de Oxford, en su edición online (*http://oxforddictionaries.com/*), define el término *backup* como la copia de un archivo u otro dato, hecho en caso de que el original se pierda o dañe.

Entender la evolución de los sistemas de copias de seguridad implica conocer en primer lugar la evolución de los dispositivos de almacenamiento y de procesamiento de los datos que respaldan.

En las siguientes secciones se efectuará un recorrido cronológico a lo largo de la historia de las copias de seguridad en el que se pondrá de manifiesto cómo los distintos dispositivos utilizados para almacenamiento de copias de respaldo se han ido adaptando, tanto a los medios técnicos que en cada momento han existido, como a las necesidades que esos, cada vez más potentes y modernos, medios han demandado: a medida que los dispositivos informáticos han ido desarrollándose, también lo ha hecho su capacidad de generar datos más deprisa y en mayor cantidad, datos que ha sido necesario respaldar mediante políticas de copias de seguridad.

En un primer lugar se hablará del primer medio para realizar copias de seguridad, las tarjetas perforadas, y se continuará con los primeros dispositivos de cintas magnéticas y los discos duros y flexibles, para finalizar con los discos ópticos, las memorias US y la irrupción en el panorama tecnológico de la nueva Computación en la nube o *Cloud Computing*.

2.1 TARJETAS PERFORADAS

La aparición de la tarjeta perforadora como medio de suministrar información a una máquina se remonta al siglo XVIII, cuando el francés Joseph-Marie (1753 – 1834) ideó un telar controlado por medio de tarjetas perforadas. Las tarjetas se perforaban de manera que indicaran a la máquina el diseño del tejido (este tipo de telares aún se utilizan en la actualidad) (Lubar, 2009).

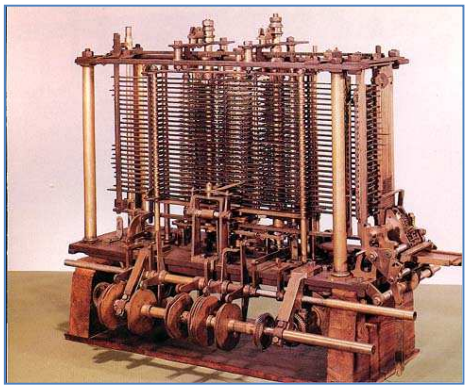


Ilustración 2. Telar de Joseph-Marie

Ilustración 3. Detalle tarjetas perforadas

Ya en el siglo XIX, el fundador de IBM, Herman Holleritz (1860 – 1929), se dio cuenta de que la mayoría de las preguntas contenidas en los formularios que recababan información para la elaboración de los censos de población en Estados Unidos podían ser contestadas con un simple *sí* o *no*.

Teniendo esta información en cuenta ideó una tarjeta de cartulina perforada en la que dependiendo de que existiera perforación o no y de la posición de ésta, se contestaba afirmativa o negativamente a la correspondiente pregunta. Holleritz patentó su máquina tabuladora basada en tarjetas perforadas en 1889 y el año siguiente el gobierno de Estados Unidos eligió su máquina para elaborar el censo.

Holleritz patentó en 1901 su perforadora. Era un dispositivo para la inserción manual de datos en tarjetas perforadas. Practicaba perforaciones precisas en las localizaciones que indicaba el operador al oprimir las teclas correspondientes y avanzaba directamente a la siguiente columna con cada perforación. En los primeros modelos fueron únicamente mecánicas y sólo se podían introducir caracteres numéricos. En versiones posteriores se incluyó un motor y un teclado completo similar al de una máquina de escribir normal. Algunas máquinas perforadoras incluso podían imprimir al comienzo de las columnas de agujeros el carácter perforado en cada una de ellas.

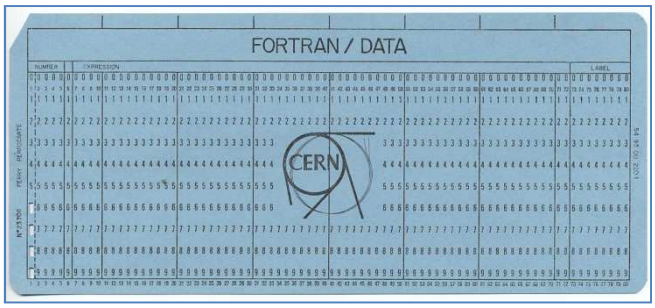


Ilustración 4. Tarjeta perforada usada en el CERN

Las dimensiones de la tarjeta se mantuvieron durante años pero el número de columnas creció de 20 en 1890 a 80 en 1928 (Jones, 2011). El número de filas fue de 12 desde el comienzo, pero las dos primeras en la parte superior generalmente no se usaron hasta los años 1930.

La lectura de las tarjetas perforadas se realizaba en el tabulador (Da Cruz, 2011). Su función básica consistía en contar o sumar la información de las tarjetas perforadas que se le suministraba y reflejar el resultado hallado en diales. Posteriormente los resultados pudieron ser mostrados en pantallas, imprimidos en papel o incluso transferidos a nuevas tarjetas perforadas que podían ser utilizadas en subsecuencias de procesamiento.

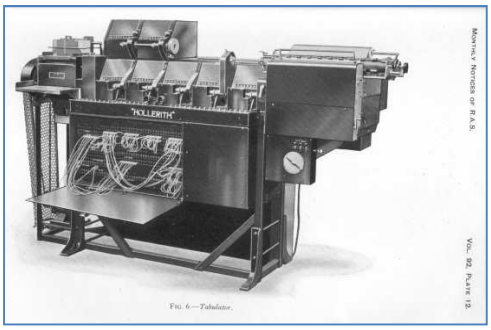


Ilustración 5. Tabulador de Holleritz.

Estos tres inventos (el tabulador, la máquina perforadora y las tarjetas perforadas) fueron la base de la industria moderna de procesamiento de información.

El rápido desarrollo de la era moderna de los sistemas de computación tuvo el germen antes y durante la segunda guerra mundial, cuando los circuitos electrónicos remplazaron a sus equivalentes mecánicos y los cálculos digitales hicieron lo propio con los analógicos.

Las máquinas procesadoras de esos primeros momentos se hacían de una manera artesanal, montados pieza a pieza por el hombre, utilizando circuitos compuestos por válvulas, tubos de vacío, relés y usando como medio de introducción y almacenamiento de datos tarjetas perforadas o rollos de papel continuo perforado.

En este periodo surgen dos figuras clave Alan Turing y John Von Neumann.

Alan Mathison Turing (1912 – 1954) desarrolló su vida profesional alrededor de la matemática, la lógica y la criptografía. Se le considera el padre de la ciencia de la computación y de la inteligencia artificial. Fijó los conceptos de algoritmo y computación con la *máquina de Tuning* (Copeland, 2000).

Tuning estaba interesado en la cuestión de qué significa para una tarea que sea computable, pregunta fundamental en la filosofía de la ciencia de la computación. De manera intuitiva se puede contestar a la pregunta argumentando que una tarea es computable si es posible especificar una secuencia de instrucciones que conduzcan a la resolución de la tarea cuando son llevadas a cabo por una máquina. A ese conjunto de instrucciones se le denomina *procedimiento efectivo* o *algoritmo*, para la tarea a desarrollar. El problema que subyace en esta respuesta intuitiva es que lo que asumimos como procedimiento efectivo depende de la máquina que lo va a llevar a cabo, es decir, distintas máquinas podrán realizar distintos algoritmos dependiendo de cómo estén construidas.

Ilustración 6. Alan Mathison Turing (1912 – 1954)

Turing propuso un tipo de dispositivo matemático (no físico) llamado *máquina de Turing*. Estos dispositivos condujeron a una noción formal de computación denominada *Turing-computacional*, es decir, una tarea es *Turing-computacional* si puede llevarse a cabo por una máquina de Turing (Barker-Plummer, 2011).

John Von Neumann (1903 – 1957) fue pionero entre otros campos, en el de la mecánica cuántica y en el de análisis de funciones. Miembro de primer orden en el Proyecto Manhattan y en el Instituto de Estudios Avanzados en Princeton fue figura clave en el desarrollo de la teoría del juego (más conocida comúnmente como teoría de decisiones), los conceptos de autómatas celulares, constructores universales y computación digital (Bochner, 2958).

Ilustración 7. John Von Neumann (1903 – 1957)

La influencia de Von Neumann en el campo de la computación fue crucial. Definió una arquitectura que usa la misma memoria tanto para el almacenamiento de programas como de datos de que se alimentan. Todos los computadores de hoy en día virtualmente utilizan a nivel interno la arquitectura de Von Neumann o alguna de sus variantes.

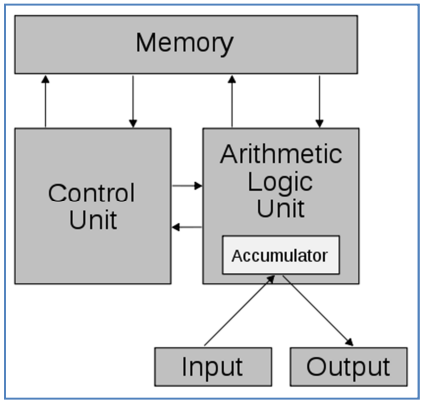


Ilustración 8. Diseño de la arquitectura de von Neumann (1947)

Apoyándose en los hallazgos de Nemann y Turing, entre 1941 y 1949 se construyeron nuevos modelos de computadores siguiendo distintas vías de investigación (alguna de las cuales mantenida en el más absoluto secreto debido a la Segunda Guerra Mundial, tal es el caso de *Colossus* en Reino Unido). A continuación se puede observar un esquema de las más importantes; en él se pueden encontrar sus principales características.

Nombre	Fecha	Sistema numérico	Mecanismo computación	Programación	Turing
Zuse Z3 (Alemania)	Mayo 1941	Binario, coma flotante	Electro - mecánico	Programa controlado por película de 35mm perforada	En teoría
Atanasoff – Berry Computer (USA)	1942	Binario	Electrónico	No programmable (un solo uso)	No
Colossus Mark I (Reino Unido)	Febrero 1944	Binario	Electrónico	Programa controlado por cables de conexión e interruptores	No
Harvard Mark I – IBM ASCC (USA)	Mayo 1944	Decimal	Electro - mecánico	Programa controlado por cinta de papel perforado de 24 canales	No
Colossus Mark 2 (Reino Unido)	Junio 1944	Binario	Electrónico	Programa controlado por cables de conexión e interruptores	En teoría
Zuse Z4 (Alemania)	Marzo 1945	Binario, coma	Electro – mecánico	Programa controlado por película de 35mm	Sí

		flotante		perforada	
ENIAC (USA)	Julio 1946	Decimal	Electrónico	Programa controlado por cables de conexión e interruptores	Sí
Manchester Small-Scale Experimental Machine (Baby) (Reino Unido)	Junio 1948	Binario	Electrónico	Programa almacenado en memoria de tubo catódico Williams	Sí
ENIAC Modificada	Septiembre 1948	Decimal	Electrónico	Mecanismo de programación de solo lectura utilizando tablas de funciones como programa ROM	Sí
EDSAC (Reino Unido)	Mayo 1949	Binario	Electrónico	Programa almacenado en memoria de linea de retardo de mercurio	Sí
Manchester Mark 1 (Reino Unido)	Octubre 1949	Binario	Electrónico	Programa almacenado en memoria de tubo catódico Williams y memoria de tambor magnético	Sí
CSIRAC (Australia)	Noviembre 1949	Binario	Electrónico	Programa almacenado en memoria de linea de retardo de mercurio	Sí

Las primeras computadoras de uso comercial fueron las denominadas Ferrati Mark 1 y UNIVAC 1.

Ferrati Mark 1, entregada a la Universidad de Manchester en febrero de 1951, era capaz de almacenar información en cintas de papel perforado. El flujo de información se podía hacer en los dos sentidos, es decir, podía tanto escribir en el papel perforado los resultados que ofrecían sus cálculos realizando las correspondientes perforaciones o leerlo interpretando los agujeros del papel.

UNIVAC 1 (Universal Automatic Computer 1), desarrollada por John Pespert Eckert (1919 – 1995) y John William Mauchly (1907 – 1980), fue entregada a la oficina del censo de Estados Unidos el 31 de marzo de 1951 y puesta en servicio el 14 de Junio del mismo año (Goldschmidt & Akera, 2003).

Aunque originariamente no dispuso de interfaz para la lectura o perforación de tarjetas se corrigió este hecho añadiendo un equipo de procesamiento de tarjetas fuera de línea.

Como se ha podido observar, la gran mayoría de las computadoras construidas hasta la aparición de UNIVAC en 1951 utilizaban como medio de suministro de información, ya se tratara del programa a desarrollar o los datos que necesitaba el programa para obtener su resultado, las tarjetas perforadoras o las cintas de papel perforado.

En muchos de los casos se utilizaban dichas tarjetas como medio para recuperar información perdida o corrompida, por lo que cumplían con la definición de lo que es una copia de seguridad (backup) que se ha dado al principio de este capítulo. Por lo tanto no es un error afirmar que el primer medio que se utilizó para almacenar copias de seguridad fueron las tarjetas perforadas (más tarde las cintas de papel perforado).

El uso de tarjetas perforadas como medio de almacenamiento de copias de seguridad tenía principalmente dos inconvenientes.

El primero era su baja capacidad, haciendo necesario en muchas ocasiones una gran cantidad de tarjetas para el almacenamiento de la información generada, aumentando consecuentemente tanto el volumen de material a almacenar como el gasto económico que ocasionaba (no sólo en material sino también en logística).

El segundo lugar, la utilización de las tarjetas suponía una ralentización en el conjunto global del proceso, a más cantidad de información más dificultad para procesar, encontrar o restaurar la deseada.

Estos problemas se solucionaron en gran medida con la aparición de las computadoras que utilizaban cinta magnética como medio de transmisión y almacenamiento de datos y programas, la primera de las cuales fue, como ya se ha comentado con anterioridad UNIVAC.

2.2 CINTAS MAGNÉTICAS

En 1928 el austríaco-alemán Fritz Pfleumer (181 – 195), patentó la primera cinta magnética de la historia. Experto en papeles especiales y procesos relacionados para uso industrial (anteriormente había desarrollado el proceso para incluir línea de bronce en los papeles de cigarrillos) en 1927, después de experimentar con diversos materiales ideó un papel muy fino que recubrió con polvo de óxido de hierro usando laca como aglutinante.

Ilustración 9. Fritz Pfleumer

El invento de Pflemer no se utilizó para la grabación de datos hasta 1951, fecha en la que, como ya se ha comentado anteriormente, vio la luz la máquina de *Maunchly* y *Eckert* UNIVAC I. El dispositivo de entrada y salida utilizado fue bautizado con el nombre de UNISERVO y en su diseño original utilizaba para la grabación de datos una cinta de metal de 12,65 mm de una aleación de níquel, plata y bronce denominada Vicalloy. La densidad de grabación de datos era de 128 caracteres por pulgada en 8 pistas.

El 21 de mayo de 1952 IBM anuncia el lector-grabador de cintas magnéticas IBM 726[4] (IBM Archives). Durante los años 1940, IBM había estado desarrollando la cinta magnética recubierta de plástico. El modelo 726 utiliza por fin ésta tecnología alcanzando una densidad de 100 caracteres por pulgada y convirtiéndole en un estándar de facto.

Las primeras unidades de cinta IBM fueron grandes dispositivos que utilizaban columnas de vacío para almacenar largos bucles de cinta en forma de u. Las cintas estaban enrolladas en dos carretes (a medida que uno se vaciaba el otro se llenaba) y cuando estaban activos giraban en rápidas ráfagas irregulares y asincronizadas. Como curiosidad comentar que dicho movimiento resultaba visualmente impactante fruto de los cual durante bastante tiempo se utilizaban secuencias que incluían estas unidades de cinta cuando en el cine o en la televisión se quería representar alguna computadora.

[4] el sistema IBM 701 contaba con dos unidades del IBM 726

Ilustración 10. IBM 726.

LINCTape (y su derivado DECtape) fue una variación de los grandes rollos descritos anteriormente. LINCTape fue uno de los primeros modelos de almacenamiento de datos personal. Nació al amparo del diseñador *Wesley Clark* en el MIT Lincon Laboratory y era parte integrante de la computadora LINC. Podía ser comparada a un disquete lineal con un lento tiempo de búsqueda. En contraste a las unidades de cinta contemporáneas era pequeña, y almacenaba alrededor de 400 k. Tenía una pista de formato fijo que, a diferencia de las estándar, permitía que los datos fueran leídos y escritos repetidamente en la misma localización. Tardaba menos de un minuto en recorrerse entera. La cinta se formateaba en bloques de tamaño fijo y se utilizaba para albergar un directorio y el sistema de archivos. Una instrucción simple del hardware permitía buscar y entonces leer y escribir multitud de bloques de la cinta en una única operación. LINctapes y DECtapes tenían similar capacidad y tasa de transferencia que los disquetes que los reemplazaron, pero sus tiempos de búsqueda eran del orden de entre treinta segundos a un minuto.

Desde los orígenes hasta nuestros días, tanto los dispositivos de entrada/salida que utilizan cintas de datos, como las mismas cintas han experimentado cambios a todos los niveles. Paulatinamente, a medida que los avances tecnológicos lo han permitido, se ha ido aumentando la densidad de datos, disminuyendo la tasa de transferencia y cambiando el formato.

La cinta magnética de plástico permitió que los computadores fueran alimentados con una cantidad de datos significativamente más grande que con las tarjetas perforadas o los rollos de papel perforado. A demás permitió una disminución en los costes de producción y logística, ventajas que aún permanecen y que siguen haciendo del uso de cintas para copias de seguridad una alternativa viable.

2.3 DISCOS DUROS

En 1956 IBM crea su primer disco duro incluido en el sistema RAMAC 305, con una capacidad inicial de 5MB (Perenson, 2006).

El proyecto que culminó con la máquina RAMAC oficialmente comenzó en septiembre de 1952 bajo la dirección de Arthur J. Critchlow (Pugh, 2005). Inicialmente se le encargó que estudiara la manera en la que la información era organizada, formateada, almacenada y procesada usando un equipo que se alimentaba con tarjetas perforadas y buscara una solución mejor.

Experimentó con numerosos dispositivos de almacenamiento existentes en la época pero ninguno era adecuado para el acceso aleatorio a los datos. La cinta magnética era inaceptable debido al tiempo excesivo que necesitaba para enrollarse y saltar de dato a dato separados. Los tambores magnéticos tenían rápido acceso a la información almacenada, pero la información únicamente se encontraba en la superficie exterior de u cilindro que rotaba y, por tanto, la eficiencia volumétrica era baja y el coste comparativamente alto.

Tras un detenido estudio, el análisis teórico de la situación predecía que un disco magnético podría ser la solución, ya que tendría un tiempo de acceso bajo junto a una eficiencia volumétrica aceptable.

La idea se plasmó con la construcción de un dispositivo que consistía en un conjunto de discos concéntricos que giraban continuamente alrededor de un eje común, con una cabeza lectora / escritora que podía desplazarse arriba o abajo paralelamente al eje y penetrar entre los discos para leer o escribir en el que fuera necesario (posteriormente se sustituiría por varias cabezas lectoras / escritoras insertadas entre cada disco). Su primer uso comercial en diciembre de 1954 marcó el inicio de las unidades de disco duro.

En 1963, con el lanzamiento por parte de IBM de lo que sería el primer disco duro extraíble de la historia (Farrance, 2006), el IBM 1311[5], comienza a atisbarse la posibilidad de utilizar discos duros como contenedores de copias de seguridad, aunque su poca capacidad y fragilidad no lo permitiera aún.

Posteriormente, en marzo de 1973, IBM anuncia el IBM 3340 *Winchester* como componente del IBM System 1370. Las unidades de disco extraíbles *Winchester* estaban selladas y su importante avance radicaba en que al disponer ella misma de una manera integrada los brazos y cabezales necesarios para la lectura y escritura, no

[5] El IBM 1311 disponía de 6 platos de catorce pulgadas que albergaban 2.6 MB.

era necesario mover ninguna cubierta o tapa en la unidad central al insertarlos. Fue desarrollada en San José bajo el liderazgo de Kenneth Haughton, enfocándose en un principio en dos módulos móviles de 30 Mb[6].

En los primeros años de vida de los discos duros su excesivo coste, baja capacidad y extremada fragilidad hacía inviable su uso para albergar copias de seguridad, utilizándose principalmente la cinta magnética, sin embargo desde el año 1978, año en el que se desarrolló el primer RAID (Redundant Arrays of Independent Disks) y principalmente a partir de los años 1980, con el auge de los ordenadores personales, la investigación y desarrollo en el campo de los discos duros magnéticos no ha dejado de ofrecer nuevos modelos de unidades cada vez más rápidas, compactas y con más capacidad de almacenamiento. Este hecho ha posibilitado la paulatina migración desde un sistema de almacenamiento al otro, hasta el punto de que en la actualidad las dos tecnologías pugnan por conseguir el liderazgo en el negocio de los dispositivos de copias de seguridad, batalla en la que paulatinamente va tomando ventaja el disco duro.

2.3.1 LOS DISCOS DUROS EN EL SENO DE HOGARES Y PEQUEÑAS O MEDIANAS EMPRESAS

En 1983 Compaq Computer lanza los primeros PC portátiles compatibles IBM. Estos utilizaban un nuevo disco de 3.5" que era mucho más resistente a la vibración y los golpes (Kerekes, 2011).

Aun así en los 1980 el coste de los discos duros extraíbles les alejaba de la meta de constituirse en los dispositivos más utilizados mayoritariamente como medio de copias de seguridad.

Durante los 1990, el medio para hacer copia de seguridad para la mayoría de los usuarios de casa y medianas o pequeñas empresas eran los discos flexibles o discos *Zip*.

En 1997 Iomega, compañía que años atrás había lanzado el disco *Zip*, comercializa el disco *jazz* con una capacidad de 1 Gb. La unidad *jazz* usaba la interfaz SCSI, pero gracias a un adaptador conocido como *jazz traveler*, podía conectarse a un puerto paralelo estándar. No está alejado de la verdad decir que el disco *jazz* fue el primer ejemplo de un sistema de copias de seguridad disco a disco.

Alrededor del año 2001 las nuevas generaciones de discos duros diseñadas para ordenadores portátiles y cámaras eran lo suficientemente robustas como para ser utilizados como dispositivos de almacenamiento de copias de seguridad, con poca o

[6] Debido a la configuración inicial 30/30, el IBM 3340 obtuvo su nombre clave por el fusil Winchester 30-30.

ninguna protección añadida. Siendo conectados por puertos USB y Fireware, un disco externo ha sido la opción más barata y fiable para el almacenamiento de copias de seguridad en hogares, y pequeñas o medianas empresas.

2.4 DISCOS FLEXIBLES

La aportación de los discos flexibles en el ámbito de las copias de seguridad ha sido discreta pero durante bastante tiempo crucial para la mayoría de los usuarios domésticos y las pequeñas empresas.

El dispositivo de disco flexible o floppy disk (FDD) fe inventado para IBM por Alan Shugart en 1967 (Leg, 2009). Los primeros dispositivos utilizaban discos flexibles de 8 pulgadas y fueron evolucionando primero hacia las 5.25 pulgadas (usadas por el primer ordenador personal de IBM en agosto de 1981) con una capacidad de 360Kb y finalmente hasta el modelo de 3,5 pulgadas y 1.4 Mb de capacidad.

Debido a su reducido tamaño, su facilidad de uso y su bajo coste, rápidamente se convirtió en el medio de almacenamiento elegido por los hogares y la pequeña empresa, que o bien no necesitaban almacenar gran cantidad de datos o bien el bajo coste del dispositivo y los discos hacían de ellos la única opción viable para el mantenimiento de una política de copias de seguridad aceptable, aún a costa del aumento del número de discos necesarios para alcanzar tal fin.

Hoy día es un medio que ha caído en desuso, hasta el punto de que es muy difícil encontrar en el mercado de venta de ordenadores personales o portátiles unidades que incluyan este dispositivo, totalmente desplazado por los discos duros externos o extraíbles y las unidades flash de memoria[7].

[7] Sony, el último gran fabricante de floppies, detuvo su producción en marzo de 2011.

2.5 DISPOSITIVOS ÓPTICOS

El problema que constituía la baja capacidad de almacenamiento que ofrecían los discos flexibles de 3.5 pulgadas se solventó con la siguiente generación de medios de almacenamiento: los discos compactos gravables (CD-R) y regrabables (CD-RW).

El disco compacto fue introducido en el mercado japonés por Philips y Sony en noviembre de 1982 y en marzo de 1983 llegó a Europa (Philips).

Posteriormente, en 1988 vio la luz el primer CD-R, originariamente denominado CD-WO (Compact Disk Write-Once), fecha en la que Sony y Philps publicaron sus especificaciones en el Libro Naranja[8].

El CD-R se introdujo en el mercado como uso profesional en 1991 y tras varios años de investigación y desarrollo el CD-RW se comenzó a comercializar en 1997.

Las primeras unidades de grabación eran demasiado costosas para el mercado del consumidor medio-bajo, hasta que en 1996 la compañía Pioneer lanza al mercado una unidad relativamente asequible para la grabación de audio en CD-R. No obstante, fue Philips, la que en 1997 comercializa por primera vez un dispositivo que unificaba CD-R y CD-RW.

Al principio de los años 1990, el elevado coste de las unidades de grabación así como de los discos provocó que esta tecnología no fuera mayoritariamente utilizada para el almacenamiento de copias de seguridad, pero a medida que los dispositivos se fueron comenzando a instalar de serie en la mayoría de los equipos informáticos que se comercializaban, la demanda comenzó a crecer convirtiéndose virtualmente en un estándar, lo que provocó una bajada progresiva del precio.

El gradual descenso en los costes de dispositivos y discos, unido a la gran diferencia de capacidad de almacenamiento y a los avances tecnológicos en el sector, que produjeron un aumento significativo en las velocidades de grabación, provocaron que la utilización de los discos flexibles para copias de seguridad fuera desplazada por esta nueva tecnología, tendencia que culminó en 1997, cuando la compañía Pioneer lanza al mercado el primer DVD gravable de la historia, el DVD-R[9] con una capacidad de 4.7 GB.

[8] El Libro Naranja es el compendio de especificaciones creadas por Sony y Philips para definir las características de la señal óptica, disposición física, métodos de lectura y condiciones de prueba para los discos CD-R (Libro Naranja, Parte II) y CD-RW (Libro Naranja, Parte III). Se publicó por primera vez en 1990, y en un comienzo únicamente incluía cuestiones propias a la grabación simple del CD-R, pero debido a los rápidos avances desarrollados tanto en software como en hardware en el seno de la tecnología multimedia, las especificaciones crecieron para abarcar el CD-RW en 1996.

[9] DVD-R son siglas de Digital Versatile Disk Recordable (Disco Digital Versátil Regrabable).

En la actualidad el uso de DVD y CD (este último cada vez en menor medida) para el almacenamiento de copias de seguridad está bastante extendido entre los usuarios domésticos y la pequeña y mediana empresa, que ven en su bajo coste y sus prestaciones una manera sencilla de almacenar sus datos de una forma cómoda y segura.

2.6 MEMORIAS FLASH USB (USB FLASH DRIVES)

El dispositivo de memoria USB fue inventado en abril de 1999 por tres ingenieros llamados Dov Moran, Oron Ogdan y Amir Ban de M-Systems (USB Memory Direct, 2012). Está compuesto por una memoria flash integrada en un chasis que dispone de una conexión a un puerto USB (Universal Serial Bus).

Ilustración 11. Dispositivos de memoria USB.

Si bien su uso como medio de almacenamiento está ampliamente extendido entre el público en general, su utilización como medio de almacenamiento de copias de seguridad aún no es mayoritario, aunque sus obvias ventajas están haciendo de estos dispositivos una opción cada vez más viable sobre todo para el usuario doméstico y la pequeña empresa.

Pueden utilizarse sin ningún tipo de software especializado, y, una vez conectados casi cualquier equipo informático las reconoce como si de una nueva unidad de disco duro se tratara, por lo que puede ser usado junto con cualquier software de copias de seguridad, permitiendo incluso cualquiera de las opciones avanzadas de copias como las incrementales o diferenciales, llegando hasta la fecha, a capacidades de hasta 512 Gb[10].

En la actualidad muchas de las memorias USB comercializadas incluyen de una manera nativa software de encriptado de datos con lo que se incrementa su nivel de seguridad.

Una de las principales ventajas que ofrecen es su portabilidad y el hecho de que el usuario puede trabajar en distintas localizaciones con sus datos constantemente actualizados.

No obstante, actualmente aún adolecen de ciertos inconvenientes, algunos de ellos intrínsecos a su propia naturaleza:

[10] En un futuro cercano se podrán encontrar de hasta 2 TB de capacidad.

- **Coste**: la utilización de memorias USB para el almacenamiento de copias de seguridad implica el uso de unidades de calidad contrastada. Hoy día el coste de las memorias USB de gama media – alta continúa siendo, comparativamente, más elevado que el de otros sistemas de almacenamiento de datos de respaldo.

- **Tamaño**: una de las ventajas de este tipo de memorias, su pequeño tamaño, también se convierte en inconveniente, al facilitar su pérdida, acceso malintencionado o incluso robo.

- **Durabilidad**: actualmente las memorias USB tienen una vida media inferior a la de los discos duros, incluso aquellas de mayor calidad.

- **Velocidad**: aunque recientemente se ha dado un gran paso en este aspecto con el lanzamiento de los dispositivos USB 3.0, que pueden llegar a alcanzar velocidades de transferencia de 600 MB/s, su velocidad continúa siendo inferior a la de los discos duros convencionales, los cuales a su vez continúan mejorando.

En conclusión, el uso de memorias flash USB en el ámbito de las copias de seguridad aún se encuentra en un punto de crecimiento, aunque los últimos avances, sobre todo en el campo de la velocidad, auguran un brillante futuro a estos dispositivos.

2.7 INTERNET Y "LA NUBE"

Desde sus inicios en la década de los 1960, Internet ha pasado de ser sólo un vehículo de comunicación a convertirse en un potente medio de negocio. Al amparo de las nuevas tecnologías desarrolladas en materia de telecomunicaciones, la *red de redes* ha permitido el nacimiento de multitud de nuevas empresas que basan toda su actividad comercial en su seno, hecho que ha originado el surgimiento de un nuevo modelo de negocio informático en la red denominado computación en la nube o *cloud computing*.

Existen diversas definiciones del término cloud computing, por poner un ejemplo, IBM lo define como "*… un modelo de aprovisionamiento rápido de recursos IT que potencia la prestación de servicios IT y servicios de negocio, facilitando la operativa del usuario final y del prestador del servicio. Además todo ello se realiza de manera fiable y segura, con una escalabilidad elástica que es capaz de atender fuertes cambios en la demanda no previsibles a priori, sin que esto suponga apenas un incremento en los costes de gestión.*"

En términos sencillos se puede decir que la computación en la nube es más un servicio que un producto en sí. Las empresas que ofrecen sus servicios en este medio, sustituyen la manera tradicional de negocio basada en venta de software, servicios de postventa y actualizaciones, con la oferta de servicios integrados de instalación, uso y mantenimiento de aplicaciones no residentes en los sistemas clientes, sino en la red.

Actualmente se ha constituido como el referente de medio a dominar de las grandes compañías de software, que ven el *cloud computing* el futuro escenario del negocio tecnológico, y del que no pueden quedarse descolgados.

Dentro de este marco se encuentran las nuevas empresas de copias de seguridad online. Dichas empresas ofrecen servicios de respaldo remoto, en los que el cliente no tiene que preocuparse de la instalación de un software más o menos complejo, su utilización ni de los dispositivos de almacenamiento necesarios para guardar los respaldos. Son las propias empresas las que realizan todo el proceso, llegando incluso algunas de ellas a almacenar los datos en servidores remotos propios[11].

Por otro lado las copias de seguridad en la nube, por su propia naturaleza, implican el envío de una copia de los datos desde una red, ya sea pública o privada, a un servidor externo, generalmente mediante un software cliente que se encarga de realizar la copia y remitirla a su punto de destino. Debido a la dependencia del medio a través del cual se lleva a cabo dicho envío, este tipo de copias de respaldo no son las adecuadas

[11] Otra modalidad de este tipo de empresas son las que hacen de intermediarias entre los datos y su lugar final de almacenamiento.

si se espera, en caso de desastre, poder recuperar los datos en un lapso de tiempo relativamente pequeño, ya que actualmente existen limitaciones en cuanto a la cantidad de datos que en un determinado espacio de tiempo se pueden mover a través de una red. Por ese motivo se utilizan principalmente para el almacenamiento de datos no críticos para los que un tiempo excesivo de recuperación no supone un problema.

3 DISPOSITIVOS DE ALMACENAMIENTO

3.1 CINTAS MAGNÉTICAS

3.1.1 INTRODUCCIÓN

Como ya se ha comentado en secciones anteriores, las cintas de datos magnéticas fueron el primer tipo de memoria secundaria, no volátil y de acceso secuencial que se utilizó, no únicamente para el suministro de datos a los computadores, sino también para el almacenamiento de datos.

El acceso secuencial a los datos implica que para poder leer el registro *n* se deben leer necesariamente los *n-1* registros anteriores, este hecho, unido a la imposibilidad material (por la propia naturaleza del dispositivo) de intercalar información adicional, para lo cual es necesario realizar de nuevo la grabación completa de la cinta, hacen que su uso actualmente haya quedado relegado únicamente al de almacenamiento de copias de seguridad.

3.1.2 ESTRUCTURA FÍSICA

La estructura estándar de las cintas magnéticas consiste en una banda de material sintético de aproximadamente 0.5 pulgadas de anchura y 3 centésimas de milímetro de grosor. Típicamente consta de cuatro capas (SNIA, 2012):

- **Base**: es la superficie plástica, generalmente de un material no magnetizable sobre la que se apoyan todas las demás capas y es la que le da sus características de flexibilidad y firmeza. Como añadidura proporciona el aislamiento magnético entre capas necesario al estar la cinta enrollada sobre un eje central.
- **Material magnetizable**: compuesto por partículas de óxido de hierro, dióxido de cromo u otro tipo de material sensible a los campos magnéticos. Es la capa responsable del almacenamiento de los datos registrados en la cinta.
- **Aglutinante**: compuesto por un polímero responsable de mantener en suspensión las partículas magnetizables así como de fijarlas a la base.
- **Revestimiento**: recubre la cinta y proporciona una superficie lisa de poco rozamiento que facilita su movimiento por los cabezales de grabación o lectura.

3.1.3 ESTRUCTURA LÓGICA

La estructura lógica de las cintas magnéticas de datos se entiende de una manera más adecuada si con anterioridad se fijan tres conceptos básicos (TextosCientíficos.com, 2006):

- **Pista**: una cinta magnética estándar tiene su superficie dividida lógicamente en varias[1] pistas horizontales, posibilitando la grabación de un dato en cada una de ellas de una manera simultánea.
- **Densidad de grabación (δ)**: en cada pista horizontal, los datos se almacenan en columnas. La densidad de grabación se define como la relación entre la cantidad de información y el espacio que ésta ocupa. Se mide en Bytes por pulgada.
- **Registro**: Es una unidad lógica de información. Corresponde al conjunto de datos correspondientes a una determinada entidad.

La grabación o lectura de datos en una cinta magnética se realiza mediante una cabeza escritora o lectora (según el caso) y únicamente lo puede realizar cuando la cinta está colocada bajo ella. Las cabezas están construidas de tal manera que para efectuar la operación solicitada de una manera eficiente necesitan que la cinta se mueva a una determinada velocidad bajo ellas, lo cual supone que la unidad de lectura o grabación invierte un determinado lapso de tiempo en alcanzar dicha velocidad.

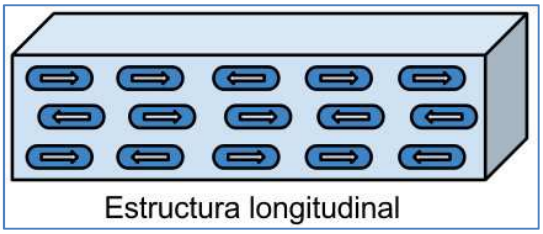
El proceso de grabación se realiza registro a registro; tras acabar de grabar un registro la cinta se detiene (con lo que también invierte tiempo en frenar hasta detenerse por completo) y necesita volver a alcanzar la velocidad adecuada para grabar el siguiente. Los continuos frenados y arranques de la cinta originan un espacio entre registros en los que no hay ningún tipo de datos con lo que se produce cierto desperdicio de cinta.

En orden a minimizar dicho problema, usualmente se procede a grabar la información agrupaciones de registros o bloques, de tal manera que el espacio no utilizado debido a las imposiciones mecánicas se minimiza al estar la información más concentrada.

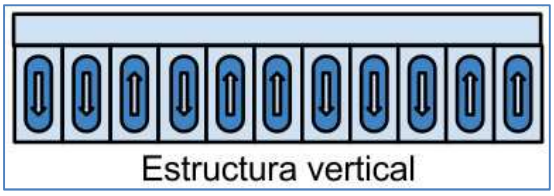
Como se ha comentado, la superficie grabable de la cinta está compuesta por pigmentos de un material magnetizable. Tradicionalmente se ha realizado la grabación de datos variando la orientación de la polaridad magnética de dichos pigmentos longitudinalmente (de izquierda a derecha o de derecha a izquierda), significando una orientación a la izquierda del pigmento por ejemplo un 1 digital (binario) y una orientación contraria un 0. En este tipo de estructura, la única opción para conseguir

[1] El número de pistas ha variado a lo largo de la historia. Actualmente varía entre marcas y tipos de cintas, siendo 9 una medida estándar.

un aumento de cantidad de datos grabados (manteniendo las dimensiones de la cinta) consiste en el desarrollo de nuevos pigmentos más pequeños.


Estructura longitudinal

En mayo de 2010 *Hitachi Maxell, Ltd* y el *Instituto de Tecnología de Tokio* anunciaron el desarrollo de una nueva tecnología consistente en un sistema de pulverización catódica del pigmento ferroso magnetizable, con lo que se pudo reducir drásticamente el tamaño del elemento orientable (Maxell, 2010). Este adelanto se unió a la posibilidad de posicionar los pigmentos verticalmente (y por lo tanto también de alterar su polaridad magnética verticalmente), lo que posibilitó por un lado la utilización de pigmentos de dimensiones mucho menores y por otro el uso de más cantidad de ellos sin la necesidad de aumentar las dimensiones de la cinta.


Estructura vertical

3.1.4 MÉTODOS DE GRABACIÓN DIGITAL

Los distintos tipos y tecnologías de cintas magnéticas se pueden clasificar, además de por sus dimensiones, por el método de grabación digital que se utiliza. Existen básicamente dos métodos distintos de grabación: lineal y transversal.

3.1.4.1 GRABACIÓN LINEAL

La grabación lineal es el primer método que se utilizó y el más sencillo. Consiste en la grabación de los datos en cada una de las pistas de la cinta de una manera longitudinal

(a todo lo largo de la cinta) y simultáneamente, utilizando una cabeza escritora / lectora por pista.

Existen principalmente dos tecnologías competidoras de este tipo de grabación:

- **SDLT (Super Digital Linear Tape)**. Desarrollada en un principio por *Digital Equipment Corporation* en los años 1980 para su línea *VAX* de ordenadores.
- **LTO (Linear Tape Open)**. Creada a finales de los años 1990 conjuntamente por *IBM, HP* y *Seagate*.

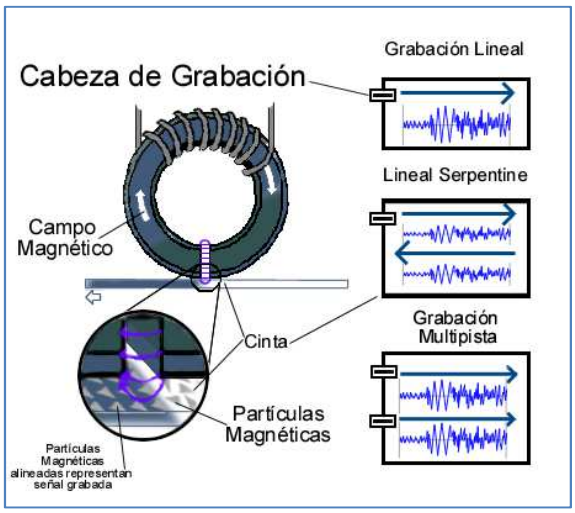


Ilustración 12. Grabación lineal.

Un método especial de grabación lineal es el denominado **serpentina**, consistente en el uso de más pistas de grabación (y lectura) que cabezas escritoras / lectoras. La cinta en este método avanza en un sentido realizándose la grabación en tantas pistas como cabezas disponga el dispositivo para, una vez alcanzado el final de la cinta, avanzar en sentido contrario y comenzar a grabar en el resto de pistas. Por lo tanto al grabar mediante el método de serpentina se consigue que se puedan utilizar más pistas que cabezas, aumentando de una manera sustancial la cantidad de información almacenada.

3.1.4.2 GRABACIÓN TRANSVERSAL

La de grabación transversal de cintas magnéticas se utilizó en un comienzo, principalmente, para la el almacenamiento de vídeo.

En este método de grabación la información es escrita en densas líneas ligeramente inclinadas. Para ello se diseñó un tambor giratorio con cuatro cabezas grabadoras que escriben la información en la cinta, que está continuamente en movimiento.

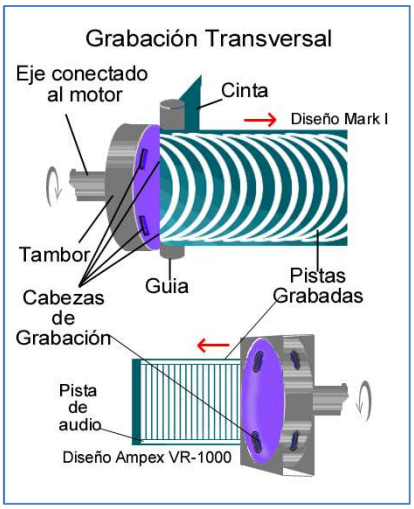


Ilustración 13. Grabación transversal.

Un método derivado de la grabación transversal, y que trataba de mejorar algunos aspectos de ésta, es el de grabación **helicoidal** o helical. En el método helicoidal el número de cabezas grabadoras se ha reducido de las cuatro utilizadas en el método transversal a dos que rotan en diferentes ángulos y en la dirección en la que la cinta es transportada, con lo que se ha logrado una mayor superficie de cinta aprovechada además de una secuencia de grabación más continua.

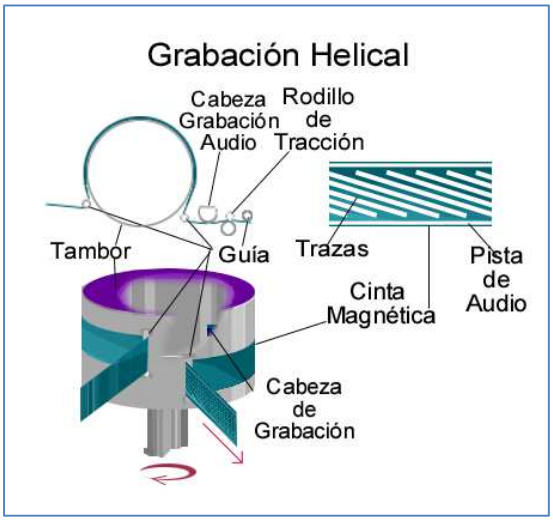


Ilustración 14. Grabación helicoidal.

En general las cintas con las que se utiliza la grabación helicoidal son más pequeñas que las usadas con el método de grabación lineal. La densidad de datos es como norma general mejor aunque normalmente las cintas de este tipo tienen una menor capacidad.

Principalmente existen dos tipos de tecnologías que utilizan este tipo de grabación:

- **Mammoth-2**: Desarrollada por *Exabyte Corporation* a mediados de los años 1990 como respuesta al crecimiento en popularidad de las cintas DLT.

- **AIT-3**: *Sony* puso en circulación esta tecnología a mediados de los años 1990 como respuesta a la necesidad de un tipo de cintas que resultaran más fiables, con mejores resultados y mayor capacidad. Incluyó innovaciones como la inclusión en el propio cartucho de la cinta de un chip de memoria que podía ser utilizado por el software de almacenamiento.

3.1.5 FORMATOS DE CINTAS MAGNÉTICAS

En mercado de cintas magnéticas de datos está en constante movimiento fruto de las investigaciones que desde su origen se están llevando a cabo en orden a conseguir mejores prestaciones, densidades de grabación y capacidad. Fruto de este continuo flujo es la oferta tan amplia que existe tanto de dispositivos de grabación como de cartuchos de almacenamiento.

Las principales empresas especializadas en el sector han desarrollado tecnologías propias para mejorar y potenciar sus productos con la lícita intención de alcanzar la mayor cuota de mercado posible.

Seguidamente se expondrán los principales tipos de formatos de cintas magnéticas que, para el almacenamiento de datos, existen actualmente en el mercado, junto con una breve explicación de cada uno de ellos.

- **8mm**: el formato de 8mm fue desarrollado inicialmente por *Exabyte Corporation*. Hasta la llegada de AIT, *Exabyte* fue la única que lo comercializaba. Los cartuchos de 8mm fueron los primeros que utilizaron el método de grabación helicoidal (Christenson, 2004).

  En la actualidad pueden almacenar desde 40 Gb en los cartuchos de 170m de largo como el *QGD-170* de *Sony* hasta 150 Gb en los de 225m como el *00558* de *Exabyte.*

- **AIT**: ante el avance en cuota de mercado de los formatos DLT, LTO, DAT/DSS y VXA, Sony reaccionó desarrollando en 1996 el Advanced Intelligent Tape (AIT).

  Incorporan la tecnología SCSI que les permite maximizar la transferencia de datos desde el host a una velocidad de hasta 160Mb/Seg y hacia el host a 24 Mb/seg.

  Tienen una capacidad de hasta 1040 Gb.

- **DDS**: El Digital Data Storage (DDS) es un formato evolucionado procedente de la tecnología DAT (Digital Audio Tape) introducido en 1986 por *Sony y Philips* (Schoenher, 2002) y Se utiliza principalmente para el almacenamiento de copias de seguridad.

  Fue desarrollado conjuntamente por *Sony, Maxell* y *Hewlett Packard* en 1989. La principal característica reside en que un una cartucho que ha sido grabado por el dispositivo de un determinado fabricante puede ser leído por el de otro.

  Utilizan un ancho de 3.8 mm, y en la actualidad se capacidad puede llegar a los 320 Gb.

- **DLT**: la tecnología DLT fue originariamente desarrollada por *Digital Equipment Corporation* a principio de los años 1980, posteriormente *Quanum Corporation* adquirió las divisiones de disco y cinta, junto con los derechos de la tecnología DLT en 1994.Actualmente es comercializado por multitud de marcas.

  Su rango de capacidad abarca desde los 10 a los 800 Gb en las versiones mejoradas SDLT.

- **DTF**: el Digital Tape Format, desarrollado por *Sony* utiliza tecnología de grabación helicoidal.

  Puede llegar a albergar hasta 42 b de información.

- **LTO**: en 1997 *IBM, HP* y *Seagate* formaron el consorcio LTO (*http://www.lto.org/index.html*) para desarrollar conjuntamente la tecnología Linear Tape-Open, publicando las especificaciones del nuevo formato abierto con el fin de simplificar el complejo panorama comercial que se estaba produciendo en el mundo de los dispositivos de almacenamiento. La naturaleza abierta de la tecnología LTO proporciona compatibilidad real entre la oferta de los distintos fabricantes.

  Suele ser el formato más utilizado cuando en el proceso de copia de seguridad se hacen relevantes tanto la cantidad de datos a respaldar como el índice de transferencia del proceso de creación de la copia.

  Permite almacenamientos de más de 3Tb (con compresión 2:1), pudiéndose llegar a alcanzar los 32 Tb.

- **T10000**: desarrollada por *Storage Tek*. Es típicamente utilizada en sistemas de computadores de gran formato en conjunción con librerías robotizadas de cintas.

  El T10000 tiene su base en la serie T, con la capacidad de permitir el acceso rápido a grandes cantidades de información para copias de seguridad intensivas.

Con una capacidad nativa de 500Gb, puede llegar a transferir datos a una velocidad de 120Mb/seg.

- **QIC**: el Quarter-Inch Cartridge fue desarrollado inicialmente por *3M* en 1972. Se utiliza principalmente para copias de seguridad e ordenadores personales y portátiles.

  Las cintas QIC más modernas se basan en tecnología Travan y tienen una capacidad de hasta 200Gb.

- **Travan**: desarrollado por *3M*, puede llegar a albergar hasta 20 Gb de capacidad con una tasa de transferencia de 4 Mb/seg.

  El formato Travan fue estandarizado por el consorcio QIC[2] y es compatible con los estándares QIC antiguos.

  Actualmente es comercializada por *Sony, HP, Travan, Imation* e *IBM.*

- **VXA**: formato de copias de seguridad creado originariamente por *Ecrix* y ahora en posesión de *Tanderg Data*.

  Permite leer y escribir los datos en paquetes de información (al igual que ocurre con la transferencia de datos en Internet). Procuran un nivel muy alto de integridad en las operaciones de volcado de datos consiguiendo velocidades de transferencia muy elevadas.

  Su capacidad puede llegar a los 200 Gb.

[2] Los diversos estándares QIC son controlados por un consorcio de fabricantes denominado Quarter-Inch Cardrigge Drive Standards, inc.

3.2 DISCOS DUROS

3.2.1 INTRODUCCIÓN

Existen multitud de fabricantes de discos duros con diferentes prestaciones que hacen difícil la elección de cuál utilizar en cada situación.

El conjunto de prestaciones comunes a todos los discos duros y que a su vez distingue a unos de otros se pueden resumir en las siguientes:

- **Capacidad de almacenamiento**: cantidad de datos que puede almacenar el disco duro.
- **Tiempo medio de búsqueda**: tiempo medio que emplea el cabezal en situarse en la pista deseada. Es la mitad del tiempo empleado que tarda el cabezal en desplazarse desde la pista más exterior hasta la que ocupa el lugar central.
- **Latencia media**: cantidad de tiempo medio que tarda el cabezal en situarse sobre el sector deseado. Es la mitad del tiempo que necesitan los platos en efectuar una rotación completa.
- **Tiempo medio de acceso**: tiempo medio que emplea el cabezal en situarse en la pista y sector deseados. Resulta de la suma de los tiempos medios de búsqueda y latencia.
- **Velocidad de rotación**: se mide en las revoluciones por minuto de los platos del disco duro.
- **Tasa de transferencia**: velocidad a la que el disco duro puede transferir la información leída al sistema operativo de la computadora una vez que el cabezal se encuentra en la pista y sector adecuados.
- **Memoria caché**: memoria incluida en la controladora del disco duro y que hace de puente entra las lecturas / escrituras y el sistema operativo del ordenador y el disco duro.

3.2.2 ESTRUCTURA FÍSICA

La estructura básica de los discos duros actuales no difiere en gran medida de la que tenían a principio de los años 1980 los modelos de 10 Mb que se instalaban en los primeros PC/TX de IBM. Por otro lado, en términos de capacidad, velocidad, fiabilidad

y otras características, comparativamente han avanzado más que otros dispositivos que componen los ordenadores.

Su estructura básica consta de los siguientes elementos:

- **Plato**: también llamados discos, son donde se guardará la información. Suelen estar fabricados con una base de aluminio, vidrio o cerámica, sobre la que se deposita una fina capa de cobertura en ambas caras en un proceso denominado deposición por pulverización catódica.

  Esta capa está compuesta a su vez por varias subcapas de aleaciones metálicas no magnéticas sobre las que se ubica la capa magnética compuesta por gránulos de material magnetizable. Finalmente sobre todas ellas se sitúa una final de protección fabricada en un material con base de carbón.

  Giran a alta velocidad concéntricamente, alrededor de un eje común.

- **Cara**: cada una de los dos lados de cada plato.

- **Cabezal**: el cabezal de lectura y escritura es el dispositivo encargado de leer y escribir los datos en las caras de los platos.

  Normalmente hay un cabezal por cara, aunque algunos modelos de discos duros incluyen más de uno, disminuyendo de esta manera la distancia media que han de desplazarse para acceder a los datos, aumentando por tanto la velocidad de escritura y lectura del disco duro.

  El cabezal reposa sobre un brazo que se introduce entre los discos y puede moverse hacia dentro o fuera de estos gracias a un impulsor que dispone de un motor.

- **Impulsor y brazo**: dispositivo compuesto por un motor y un brazo que alberga los cabezales. El brazo que gira alrededor de un eje, se introduce entre los platos para alcanzar las distintas pistas y sectores de datos.

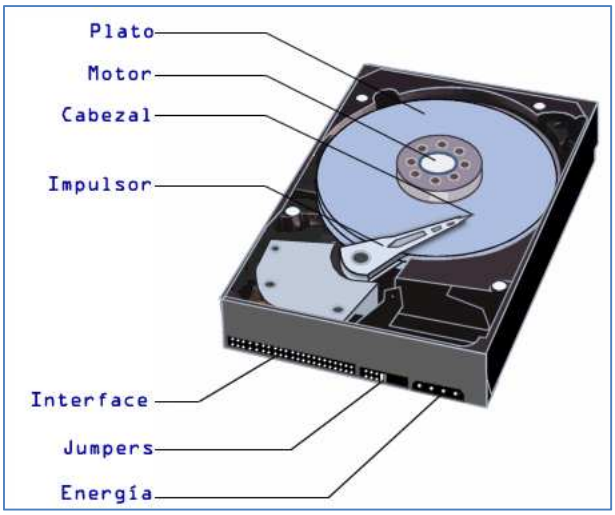


Ilustración 15. Estructura básica de un disco duro.

- **Pista**: cada una de las caras de los platos está dividida en pistas concéntricas donde se almacena la información. Están numeradas ascendentemente desde el exterior del plato hacia su interior, siendo la pista cero la más externa.

- **Cilindro**: el conjunto de pistas concéntricas de cada cara de los platos situados en el mismo plano vertical, apiladas unas encima de las otras.

  Debido a que los cabezales de lectura y escritura se encuentran alineados verticalmente, y que los platos giran concéntricos, la lectura o escritura de las pistas de un cilindro determinado se puede efectuar de un modo simultáneo sin necesidad de mover los brazos del impulsor.

- **Sector**: cada una de las divisiones de una pista y la unidad mínima de información que puede leer o escribir un disco duro.

  El tamaño de cada sector no es fijo[3]. Como norma general la controladora del disco duro es quien, en el momento de ser formateado, determina el tamaño de un sector, por otro lado en determinados modelos de discos duros se permite especificar su tamaño.

  En modelos antiguos de discos duros el número de sectores por pista era fijo, lo cual implicaba un desaprovechamiento de las pistas exteriores, capaces de albergar mayor número de sectores. Con el fin de mitigar este problema se ideó la tecnología ZBR[4] (Zone-Bit, Recording).

[3] Actualmente el tamaño estándar de los sectores es de 512 bytes.
[4] La tecnología ZBR es un método de optimización consistente en colocar más sectores en las pistas exteriores de los platos del disco duro que en las interiores (Rouse, 2005).

- **Cluster**: agrupación de varios sectores del disco. Su tamaño depende de la capacidad del disco duro.

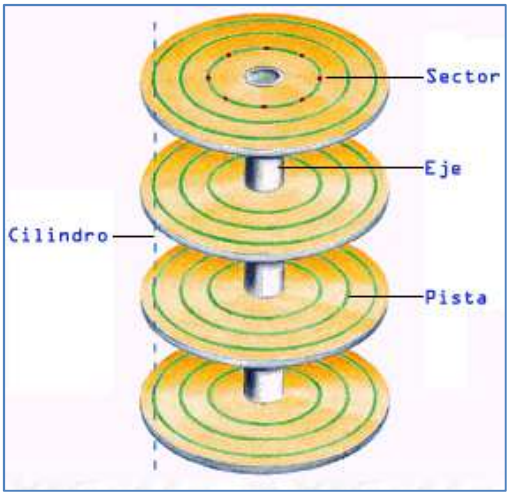


Ilustración 16. Cilindro, pista y sector de un disco duro. Fuente Partition-table.com

3.2.3 ESTRUCTURA LÓGICA

A un nivel básico la estructura lógica de cualquier disco duro está formada por el sector de arranque, el espacio particionado y el espacio sin particionar.

- **Sector de arranque**: también denominado Registro Maestro de Arranque o MBR, tradicionalmente identificado por el cabezal cero, en la pista cero y el sector cero, se almacena la tabla de particiones y un pequeño programa maestro de inicialización llamado Master Boot. Dicho programa es el encargado de leer la tabla de particiones t ceder el control al sector de arranque de la partición activa.

- **Espacio particionado**: es el espacio del disco que ha sido asignado a alguna partición, de forma que el sistema operativo lo considera como una unidad totalmente independiente.

- **Espacio no particionado**: espacio no accesible del disco duro que no ha sido asignado a ninguna partición y está sin formatear.

3.2.4 FUNCIONAMIENTO BÁSICO

El proceso de grabación de datos no difiere en gran medida al descrito para las cintas magnéticas. Siendo su base la misma difiere en los componentes que actúan y los materiales que se utilizan, por lo que no se añadirá nada al respecto.

El proceso de lectura de un determinado dato es complejo e intervienen en él multitud de componentes y sistemas del ordenador, no obstante su estructura básica, en la que no se tienen en cuenta aspectos como el funcionamiento de la caché del disco, la corrección de errores y otros muchos, es la que a continuación se expone de una manera secuencial (Kozierok, Abril):

1. Una vez que el sistema operativo desea leer una determinada información del disco duro, el primer paso consiste en averiguar en qué lugar del disco se encuentra dicha información. De dicho trabajo se ocupa el sistema operativo junto con la BIOS.

2. La información obtenida en el primer paso, generalmente en términos de qué cilindro, cabeza y sector quiere leer el sistema operativo, se manda a la controladora del disco duro.

3. El controlador del disco duro en primer lugar averigua si dicha información requerida se encuentra aún en su memoria caché. Si es así la devuelve al sistema operativo sin la necesidad de efectuar la búsqueda en el disco duro.

4. Si no se encuentra en la memoria caché, el controlador da la orden para que los platos del disco duro comiencen a girar, en el caso de que no estuvieran haciéndolo ya, y alcancen la velocidad adecuada de giro.

5. La controladora interpreta la dirección que recibió del sistema operativo para ser leída y la formatea en una dirección entendible por el disco duro. El valor resultante es pasado al programa interno del disco duro y éste mira el número de cilindro al que se necesita acceder. El número de cilindro le informa de qué pista es la que se va a leer y mueve el cabezal a hasta dicha pista.

6. Cuando el cabezal está situado sobre la pista correcta comienza a leerla en búsqueda del sector adecuado, y cuando esta pasa por debajo lee su contenido.

7. El controlador del disco coordina el flujo de datos entre el disco hacia el sistema operativo por medio de un *buffer* temporal, del que parte la información hasta el sistema operativo satisfaciendo la petición de información de este.

3.2.5 TIPOS DE DISCOS DUROS

Una primera clasificación de los distintos tipos de disco duro se puede realizar dividiéndoles según se encuentren en el interior de la carcasa de la computadora (internos) o no (externos), es decir, los discos duros se pueden dividir atendiendo a su ubicación en discos duros externos y discos duros internos.

Una de las características de una buena política de copias de seguridad es la del aislamiento físico de los datos, es decir, la ubicación de las copias de respaldo en lugares separados del sistema al que respaldan. Este hecho implica la utilización de discos externos es la opción más adecuada para tal tarea. Por ese motivo en la presente sección se abordará únicamente la cuestión de los distintos tipos de discos duros existentes en la actualidad.

Actualmente existen básicamente tres tipos de discos duros externos: discos duros portátiles, de sobremesa y mini discos duros externos.

Se tratan de discos que se conectan al ordenador, mediante un cable, a los puertos USB, Fireware, Lan RJ45, conector eSata o inclusive vía inalámbrica. Una característica de este tipo de discos es que sus platos se encuentran girando constantemente mientras el disco se encuentre encendido.

3.2.5.1 DISCOS DUROS EXTERNOS PORTÁTILES

Son de un tamaño reducido (unas 2.5 pulgadas) que posibilita su transporte. Debido a su naturaleza transportable cuentan con sistemas de protección contra golpes y vibraciones. Actualmente pueden llegar a albergar varios TeraBytes de información.

Por lo general cuentan con conectores USB 2.0/USB 3.0 y eSata (o ambos dependiendo del fabricante).

3.2.5.2 DISCOS DUROS EXTERNOS DE SOBREMESA

Son de mayor tamaño que los portátiles (3.5pulgadas de diámetro), por lo que suelen disponer de una base que les permite mantenerse situados de una manera segura en una superficie plana.

Suelen contar con conectores USB 2.0/USB 3.0, eSata, FireWare, Lan Rj45 1Gb, WirelessG o alguna combinación de los anteriores.

En la actualidad su rango de almacenamiento abarca desde los 80 Gb a los 4 TeraBytes.

3.2.5.3 MINI DISCOS DUROS EXTERNOS

Son de un tamaño menor que los anteriores similar al de las memorias flash y se conectan a los equipos a través de puertos USB.

Su capacidad de almacenamiento puede llegar a los 16 Gb. Debido a la alta popularidad de las memorias USB no tuvieron mucho éxito comercial por lo que en la actualidad es difícil encontrarlos en el mercado.

A parte de los distintos tipos duros externos que se han comentado, existen en el mercado carcasas que permiten conectar discos duros internos como los IDE o SATA/SATA II como si de discos duros externos se trataran. La conexión con el equipo se realiza mediante el puerto USB.

3.3 DISCOS ÓPTICOS

3.3.1 INTRODUCCIÓN

El principal uso de los discos ópticos (CD-R, CD-RW, DVD, DVD-R y BLU-RAY) en cuanto a copias de seguridad se refiere, es el de almacenamiento de copias de respaldo de las propias copias de seguridad efectuadas en otros dispositivos.

La estructura y funcionamiento de las distintos tipos de discos ópticos es básicamente la misma, siendo la más llamativa el tipo de láser utilizado por el disco Blu-Ray que es de color azul a diferencia del rojo utilizado por el resto de discos (CD y DVD).

3.3.2 ESTRUCTURA

Los discos ópticos tienen un grosos aproximado de 1.2 mm.

Están formados por una base de policarbonato plástico. Durante la fabricación a dicha base se le practican hendiduras microscópicas mediante un láser en una trayectoria continua y en espiral, debido al pequeño tamaño de las perforaciones la longitud de la espiral es elevada y compacta, y es lo que, básicamente, diferencia unos discos de otros (Brain, 2011).

Por ejemplo en la fabricación de los discos Blu-Ray se utiliza un láser de color azul, a diferencia del rojo utilizado en el resto de discos. Esto permite concentrar mucho más el haz de luz, lo que da la posibilidad de practicar las hendiduras de un tamaño sensiblemente menor que con el rojo. Al realizar las hendiduras más pequeñas se loga aumentar la densidad de las mismas produciendo una espiral mucho más compacta y de mayor longitud, lo que revierte directamente en un aumento de la capacidad de almacenamiento de datos.

Una vez completada la capa de policarbonato se coloca una delgada de aluminio reflectante cubriendo las hendiduras y sobre ésta un material acrílico como protección.

Sobre todas ellas se sitúa la capa sobre la que se realizará la impresión de la etiqueta del disco.

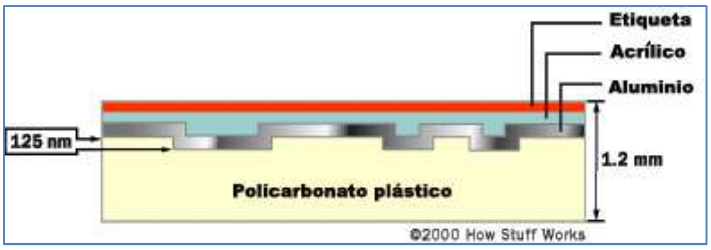


Ilustración 17. Sección (no a escala) de un disco óptico. Fuente www.electronics. Howstuffworks.com.

3.3.3 PROCESO DE LECTURA

El proceso de lectura de este tipo de discos se puede resumir en la siguiente secuencia.

El motor del dispositivo hace que el disco comience a rotar sobre su eje y un brazo mecánico hace que el láser comience a moverse, ajustando su trayectoria de una forma rectilínea de manera que en ningún momento se salga de la espiral, que pasa bajo él.

El haz del láser pasa a través de la capa de policarbonato e incide sobre las hendiduras recubiertas del aluminio reflectante. Éste refleja el haz que incide sobre un dispositivo electrónico capaz de detectar cambios en la luz.

Las hendiduras reflejan la luz de manera diferente a como lo hace la superficie lisa y el dispositivo electrónico detecta los cambios de la reflexión.

Los componentes electrónicos asociados al detector interpretan los cambios producidos en la reflexión y los traducen a información binaria, esto es bits.

3.3.4 PROCESO DE GRABACIÓN

En el proceso de grabación de los discos ópticos intervienen multitud de sistemas y tecnologías, tanto del dispositivo de grabación como del ordenador en el que se encuentra y no es intención del presente trabajo entrar en profundidad a explicar su detallado proceso, no obstante seguidamente se expone un breve resumen del mismo.

Los discos manufacturados contienen la espiral anteriormente citada pregrabada de fábrica. Dicha espiral ha sido tratada con una capa orgánica translúcida que contiene un pigmento que reacciona al láser.

Cuando el láser incide en una determinada posición sobre el pigmento lo calienta decolorándolo y dejando expuesta la capa inferior en la que se encuentran las hendiduras recubiertas de la capa reflectante, con lo que el disco queda preparado para ser leído.

3.4 DISPOSITIVOS DE MEMORIA FLASH

3.4.1 INTRODUCCIÓN

El uso de dispositivos de memoria flash para el almacenamiento de copias de seguridad no se encuentra en la actualidad muy extendido y prácticamente queda enmarcado en el seno de los usuarios domésticos o como copia de seguridad a nivel personal de los trabajadores de las empresas. No obstante los nuevos avances tecnológicos en el sector, reflejados en los nuevos dispositivos que utilizan puertos USB 3.0 pueden hace cambiar esta tendencia.

Existen en el mercado dos tipos de memorias flash USB dependiendo del tipo de puerto que utilicen para el trasiego de datos entre ellas y el ordenador:

- Memorias flash USB 2.0, 3.0. Son las más comunes.
- Memorias flash con interfaz FireWare. Aunque tienen un mayor coste que las que utilizan un puerto USB normal, la tasa de transferencia es mucho más elevada.

3.4.2 ESTRUCTURA

La estructura básica de una memoria flash de puerto USB está formada por los siguientes componentes:

- Un conector USB macho tipo A, que proveerá la interfaz física con el ordenador al que se conecta.
- Un dispositivo de controlador de almacenamiento masivo USB. Implementa el controlador USB y provee la interfaz homogénea y lineal para dispositivos USB seriales orientados a bloques. Posee un pequeño microprocesador RISC[5] y un pequeño número de circuitos de memoria RAM y ROM.
- Un circuito de memoria flash NAND para el almacenamiento de datos.
- Un oscilador de cristal que produce la señal de reloj principal del dispositivo a 12 MHz y controla la salida de datos a través de un bucle de fase cerrado.

[5] La arquitectura computacional RISC ("Reduced Instruction Set Computer", traducido "Computador de Set de Instrucciones Reducidas) tiene como principales características que las instrucciones son de formato fijo, presentadas en un número reducido de formatos y en la que sólo las instrucciones de carga y almacenamiento acceden a la memoria de datos.

Adicionalmente estos dispositivos incluyen normalmente los siguientes componentes:

- Jumpers y puntos de prueba que se utilizan durante el proceso de fabricación del dispositivo para comprobar su correcto funcionamiento.
- Leds para indicar la transferencia de datos entre el dispositivo y el ordenador al que está conectado.
- Espacio libre. Proporciona espacio físico para incluir un segundo chip de memoria, lo que permite a los fabricantes utilizar el mismo circuito impreso para dispositivos de distintos tamaños de almacenamiento.
- Tapa protectora para el conector USB.
- Diseño con algún tipo de ayuda para el transporte.

3.4.3 MÉTODO DE GRABACIÓN

Las memorias USB utilizan tecnología de estado sólido (Aaronson, 2008).

Mientras que la mayoría de los componentes de los ordenadores utilizan tecnología que aprovecha las propiedades del magnetismo, lo que les hace sensibles a los cambios en los campos magnéticos, las unidades de almacenamiento en estado sólido escriben los datos electrónicamente en los dispositivos.

Los valores cero y uno se almacenan en millones de transistores en miniatura. Si el transistor conduce la corriente el chip lee un uno y en caso contrario, esto es, si no la conduce, lee un cero. La corriente fluye bajo los transistores a lo largo de la base del chip.

Cada unidad de almacenamiento está seccionad en bloques de muy pequeño tamaño cargados eléctricamente. Cuando se producen cambios en los archivos del dispositivo, los datos son electrónicamente almacenados en dichos bloques[6] y permanecen incluso si el dispositivo está separado de la fuente de alimentación eléctrica.

[6] Dichos bloques contienen millones de transistores que guardan los valores cero y uno. Si el transistor conduce la corriente el chip lee un uno y en caso contrario, esto es, si no la conduce, lee un cero. La corriente fluye bajo los transistores a lo largo de la base del chip.

4 LAS COPIAS DE SEGURIDAD Y EL ESTÁNDAR ISO

4.1 INTRODUCCIÓN

Existen numerosas definiciones acerca de lo que es un estándar, la guía 2 de 1996 de ISO/IEC define un estándar como "un documento establecido por consenso y aprobado por un cuerpo reconocido que provee, para uso común y repetido, reglas, directivas y características para actividades o sus resultados, encaminadas a la consecución de un óptimo grado de orden en un contexto dado", y la Real Academia española, en su Diccionario de la Lengua Española (Vigésima segunda edición) lo define como "tipo, modelo, patrón, nivel".

Los estándares son diseñados voluntariamente y no imponen ningún tipo de regulación, sin embargo, las leyes promulgadas por los países y regulaciones oficiales pueden hacer referencia a ellos y convertir su inicial cumplimiento voluntario en obligatorio.

Los estándares se pueden dividir, según su alcance, en tres grupos:

- Oficiales: son estándares respaldados por organismos oficiales dedicados a la labor de definir estándares.
- De facto: estándares no oficiales, pero su nivel de popularidad e inclusión en el mercado es grande y aceptada.
- De jure: estándares que se establece por convenio en contraposición a un establecimiento por hecho o costumbre. Son definidos por organizaciones comerciales.

Así mismo, las organizaciones que definen estándares se pueden dividir en dos grandes grupos atendiendo a su composición, el primero aquellas que están formadas por consultores independientes, integrantes de departamentos o Secretarías del Estado, ejemplos de este tipo son la **ITU** (Organización de las Naciones Unidas para las tecnologías de la información y la comunicación), **ISO** (International Organization for Standarization), **ANSI** (American National Standards Institute), etc. El segundo tipo lo forman aquellas organizaciones integradas por compañías fabricantes que de una manera conjunta deciden y proponen estándares para entrar en el mercado.

Las dos organizaciones más importantes y que de hecho absorben y auspician a la mayoría del resto son la **ITU** e **ISO**.

ITU (http://www.itu.int/en/Pages/default.aspx) fue fundada en París en 1865 como la Unión Internacional de Telégrafos. Su nombre actual data de 1934, y en 1947 se convirtió en una agencia especializada de Naciones Unidas.

Aunque su área original se cernía al telégrafo y su problemática su trabajo actual abarca todo el panorama de las telecomunicaciones, desde internet a las emisiones de televisión, pasando por la telefonía móvil.

Actualmente goza de una membresía de 193 países y más de 700 entidades del sector privado. Tiene su sede en Ginebra, Suiza.

ISO (http://www.iso.org/iso/home.htm), por su parte, es una red formada por los institutos de estandarización de 163 países[18], con una Secretaría General en Ginebra, Suiza, que coordina todo el sistema.

Se trata de una organización no gubernamental que hace de puente entre el público y los sectores privados.

ISO comenzó oficialmente sus operaciones el 23 de Febrero de 1947, en Ginebra, Suiza. Se formó en 1946, cuando delegados de 25 países se reunieron en Londres y decidieron crear una nueva organización internacional que tuviera como objetivo facilitar la coordinación internacional y la unificación de estándares industriales.

[18] La Organización ISO, únicamente permite un miembro por país.

4.2 EL ESTÁNDAR ISO/IEC 27002

La seguridad de la información tiene asignada la serie 2700 dentro de los estándares ISO/IEC (International Organization for Standarization / International Electrotechnical Commision).

Dentro de la serie 2700, se encuentra la norma ISO 27002, anteriormente denominada ISO17799 que refleja la guía de buenas prácticas y describe los objetivos de control y controles recomendables en cuanto a seguridad de la información (con 11 dominios y 133 controles) y en su sección 10.5, aborda la cuestión de las copias de seguridad.

La sección 10.5, relativa al respaldo o *backup*, abarca desde la página 73 a la 75, de la segunda edición (en español) de la ISO/IEC 27002, con fecha 15 de Junio de 2005. Debido a la importancia del tema en el contexto del presente trabajo, a continuación se reproduce textualmente su contenido.

Extracto perteneciente al ESTÁNDAR ISO/IEC. INTERNACIONAL 17799. "Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información". Segunda Edición. 2005-06-15.

10.5 Respaldo o Back-Up

Objetivo: Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información. Se debieran establecer los procedimientos de rutina para implementar la política de respaldo acordada y la estrategia (ver también 14.1) para tomar copias de respaldo de la data y practicar su restauración oportuna.

Control

Se debieran hacer copias de respaldo de la información y software y se debieran probar regularmente en concordancia con la política de copias de respaldo acordada.

Lineamiento de implementación

Se debiera proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y software se pueda recuperar después de un desastre o falla de medios:

Se debieran considerar los siguientes ítems para el respaldo de la información:

a) se debiera definir el nivel necesario de respaldo de la información;

b) se debieran producir registros exactos y completos de las copias de respaldo y procedimientos documentados de la restauración;

c) la extensión (por ejemplo, respaldo completo o diferencial) y la frecuencia de los respaldos debiera reflejar los requerimientos comerciales de la organización, los requerimientos de seguridad de la información involucrada, y el grado crítico de la información para la operación continua de la organización;

d) las copias de respaldo se debieran almacenar en un lugar apartado, a la distancia suficiente como para escapar de cualquier daño por un desastre en el local principal;

e) a la información de respaldo se le debiera dar el nivel de protección física y ambiental apropiado (ver cláusula 9) consistente con los estándares aplicados en el local principal; los controles aplicados a los medios en el local principal se debiera extender para cubrir la ubicación de la copia de respaldo;

f) los medios de respaldo se debieran probar regularmente para asegurar que se puedan confiar en ellos para usarlos cuando sea necesaria en caso de emergencia;

g) los procedimientos de restauración se debieran chequear y probar regularmente para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación;

h) en situaciones cuando la confidencialidad es de importancia, las copias de respaldo debieran ser protegidas por medios de una codificación.

Los procedimientos de respaldo para los sistemas individuales debieran ser probados regularmente para asegurar que cumplan con los requerimientos de los

> planes de continuidad del negocio (ver cláusula 14). Para sistemas críticos, los procedimientos de respaldo debieran abarcar toda la información, aplicaciones y data de todos los sistemas, necesarios para recuperar el sistema completo en caso de un desastre.
>
> Se debiera determinar el período de retención para la información comercial esencial, y también cualquier requerimiento para que las copias de archivo se mantengan permanentemente (ver 15.1.3).
>
> Otra información
>
> Los procedimientos de respaldo pueden ser automatizados para facilitar el proceso de respaldo y restauración. Estas soluciones automatizadas debieran ser probadas suficientemente antes de su implementación y también a intervalos regulares.

Como se puede observar, la norma transcrita abarca todos los aspectos a tener en cuenta al planificar una política correcta de copias de seguridad y se convierte en la guía a seguir en el momento de afrontar dicha tarea.

5 MODELOS DE COPIAS DE SEGURIDAD

5.1 INTRODUCCIÓN

Desde los primeros años de uso de copias de seguridad, se han desarrollado nuevas tecnologías que han intentado minimizar en la medida de lo posible el tamaño de los datos almacenados, el tiempo de copia y el tiempo de restauración de los mismos. Fruto de estas investigaciones son los cuatro modelos básicos que hoy día se utilizan en los procesos de generación de copias de seguridad:

- Copia total o completa (full backup).
- Copia diferencial.
- Copia incremental.
- Copia espejo.

Existen otros modelos que en los últimos tiempos se han ido consolidando en el panorama del software de respaldo de datos. Impulsados sobre todo por la necesidad de responder a las exigencias de las nuevas tecnologías emergentes en el ámbito de las redes de datos, técnicas como las copias a nivel de bloque (delta), "parcheados" binarios o copias sintéticas, cada vez son más utilizadas en políticas integrales de copias de seguridad.

La decisión de cuál de los métodos anteriormente citados se ha de utilizar cambia con las circunstancias particulares de cada situación y en la mayoría de los casos depende fundamentalmente de cuatro factores:

- La capacidad de los soportes sobre los que se va a gravar la información.
- El período de tiempo disponible para hacer la copia.
- El medio en el que se desarrolla el trabajo (local, intranet, internet, etc.).
- El nivel de urgencia a la hora de necesitar restaurar los datos.

Independientemente de los factores que determinen el tipo de copia a realizar, en la práctica, una buena política de gestión de copias de seguridad incluirá la conjunción de varios de los modelos expuestos. Una buena política de cooperación entre modelos de copias de seguridad garantizará un buen resultado final y la obtención de un respaldo de datos fiable, robusto y rápido.

5.2 COPIA TOTAL O COMPLETA

Es el tipo básico e ideal de copia de seguridad ya que es el más exhaustivo y autónomo, y en el que se basan el resto de modalidades.

Una copia total incluye todos y cada uno de los archivos seleccionados para ser incluidos en la tarea programada de copia, sin importar si han sufrido cambio o no desde la última vez que se realizó la anterior. Usualmente se genera un único archivo que se comprime con contraseña para ahorrar espacio de almacenamiento y aumentar la seguridad.

La copia total adolece de un inconveniente manifiesto; si la misma está programada para realizarse cada poco tiempo y no ha habido muchos cambios en los archivos a copiar, al realizarse una copia íntegra de todos los archivos de nuevo, en muchos de los casos las copias serán redundantes existiendo pocas diferencias entre ellas, lo cual supone un desperdicio de tiempo y espacio. Para solucionar este problema lo más adecuado consiste en programar copias totales, por ejemplo, semanales, en conjunción con copias incrementales (de las que más tarde se hablará) entre las anteriores.

La principal ventaja que ofrece este tipo de copias de seguridad reside en que el más rápido y seguro (en ámbitos donde el volumen de datos lo permite es, sin duda, la elección más aconsejable a la hora de decidir la política de copias de seguridad a seguir) si es necesario realizar una restauración total de los archivos copiados; como contrapartida es el que más recursos y tiempo de copia consume, por lo que hay que tenerlo en cuenta a la hora de programarlas.

Un aspecto importante que se debe tener en cuenta al decidirse por este tipo de copias es el de la confidencialidad y la seguridad. Como ya se ha comentado anteriormente, el modo de copia completa implica que se copiarán la totalidad de los archivos seleccionados, lo que implica que si se produce algún tipo de acceso no autorizado a la misma o incluso un robo, el intruso dispondrá de toda la información. Por lo tanto se deberá salvaguardar tanto la integridad física de las copias como su nivel de consulta por parte de personal no autorizado, estableciendo las medidas de seguridad adecuadas en cada caso.

5.3 COPIA DIFERENCIAL

Normalmente las aplicaciones de copias de seguridad mantienen un registro del día y hora en el que se realizan las copia. La fecha de modificación o creación de archivos es comparada con la marca de la última copia de seguridad y dependiendo de la modalidad de copia actúa en consecuencia.

La copia diferencial contiene todos los archivos que han cambiado desde la última copia completa. Las copias diferenciales son acumulativas entre sí, es decir, si se tienen programadas varias copias diferenciales entre copias totales, cada una de ellas no tendrá en cuenta la anterior e irá acumulando los cambios desde la última total (Backup4all, 2011).

La siguiente imagen ilustra el funcionamiento de este tipo de copias.

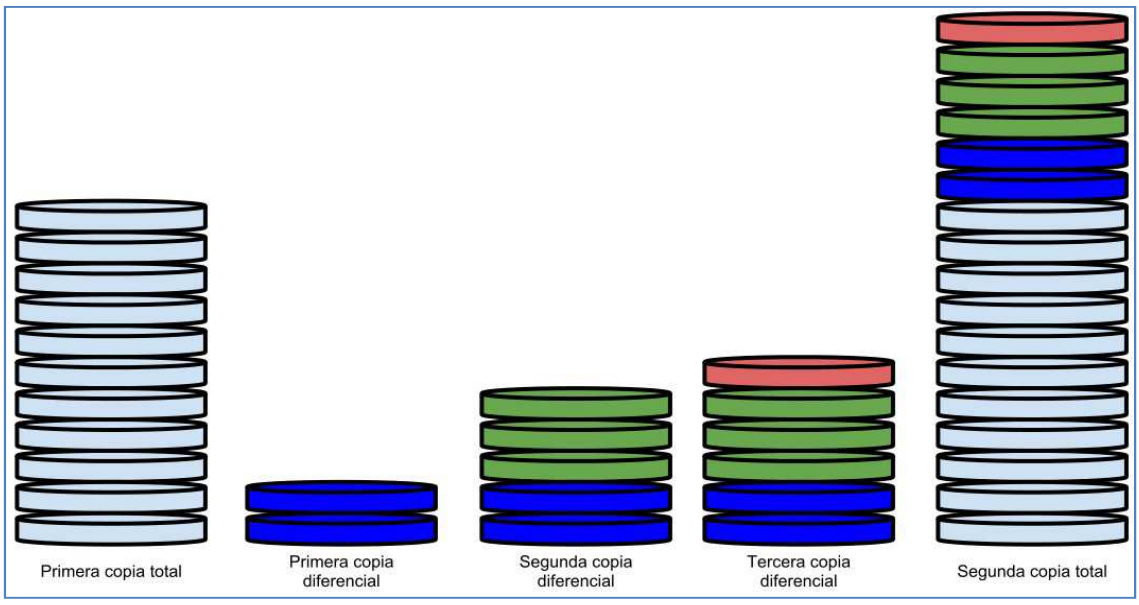


Ilustración 18. Copias diferenciales.

Las copias diferenciales tienen la ventaja de que su tiempo de restauración es menor que el de otros modelos; al restaurar los archivos únicamente hace falta restaurar la última copia total y la última diferencial. Como contrapartida el espacio de almacenamiento que se utiliza es mayor que el de otros tipos, como por ejemplo el diferencial, ya que cada copia contiene los nuevos archivos modificados o creados más la totalidad de la última diferencial, si no es la primera, incrementando progresivamente el espacio utilizado para su almacenamiento.

El tiempo de creación de la copia dependerá, como en todos los casos, del volumen de datos modificados o creados. Comparativamente es mayor que el de las copias incrementales y mayor que el de las totales.

Como ya se ha comentado anteriormente, la modalidad de copia diferencial normalmente se utiliza en conjunción con las totales. Una configuración estándar de copias de seguridad comprende la programación de una copia total a la semana junto con copias diferenciales (o incrementales, de las que se hablará seguidamente) diarias hasta la siguiente total.

5.4 COPIA INCREMENTAL

Las copias de tipo incremental contienen únicamente los archivos que fueron modificados o creados desde la última copia total, o incremental. La diferencia fundamental respecto a las copias diferenciales, es que no son redundantes (la información no se repite de una copia a la siguiente).

La siguiente imagen muestra el funcionamiento de la modalidad de copia incremental.

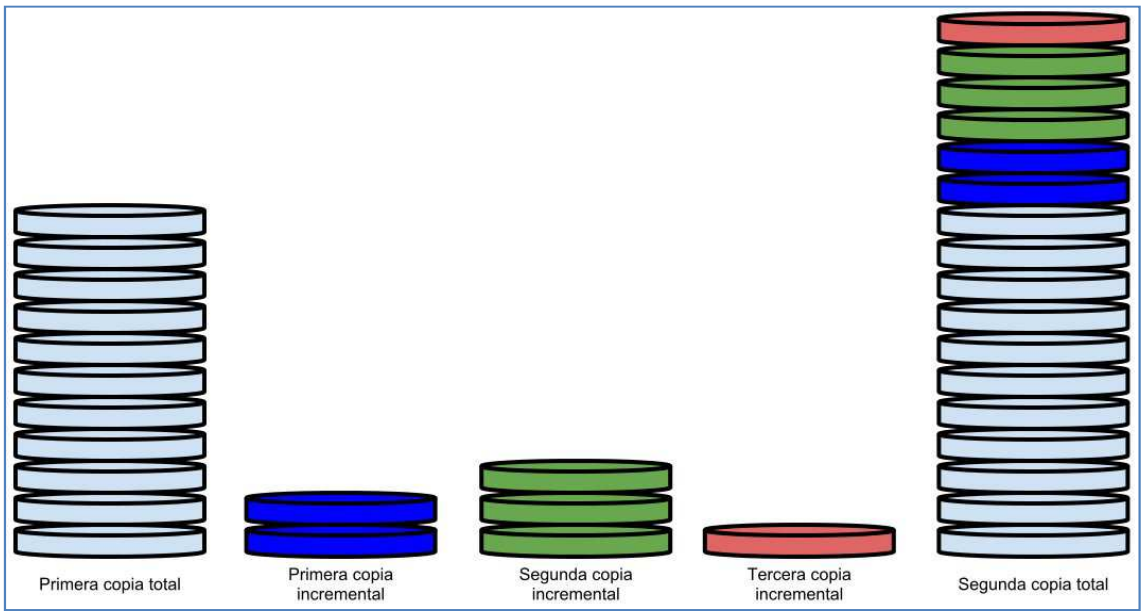


Ilustración 19. Copias incrementales.

La principal ventaja de este tipo de copias es, por regla general, su menor tiempo de creación. Al copiarse únicamente los archivos modificados o creados desde la última copia diferencial, el volumen de datos es manejable y requiere menor espacio de almacenamiento, posibilitando reducir el periodo de tiempo programado entre copia y copia.

Como contrapartida, el tiempo de restauración es mayor, ya que en el caso de un volcado total de archivos, se deberá restaurar en primer lugar la última copia total y cada una de las copias incrementales existentes hasta la fecha. Por otro lado, si la necesidad de restauración consiste en determinados archivos dispersos, se necesitará buscarlos, hasta encontrarlos, en todos los archivos de copia.

5.5 COPIA ESPEJO (MIRROR BACKUP)

Una copia espejo es básicamente una copia total a la que no se le ha aplicado ningún tipo de compresión. Algunos autores mantienen que este tipo de copia de seguridad en realidad no responde a las características propias de funciones de respaldo de datos, sino que se trata más bien de un mero proceso de "copiar y pegar".

Las copias en espejo están especialmente recomendadas en sistemas de datos que ya se encuentran comprimidos de por sí: archivos de música en mp3 o wma, imágenes en jpg o png, vídeos en divx o mov o archivos de instalación ya comprimidos.

Tienen principalmente dos ventajas frente al resto de modelos: son las más rápidas trabajando con archivos comprimidos y al no estar la información contenida en un solo archivo, el riesgo de perder datos producido por corrupción de archivos se minimiza, ya que de producirse sólo afectaría al archivo, o archivos, en cuestión y no a la totalidad de la copia.

Su inconveniente manifiesto es, generalmente, que al no encontrarse comprimida, el volumen de espacio necesitado es mayor que una copia de los mismos datos comprimida.

5.6 OTROS MODELOS

5.6.1 COPIA A NIVEL DE BLOQUES (DELTA)

Las copias de respaldo a nivel de archivo copiarán el archivo completo incluso si únicamente una parte mínima del mismo ha sido modificada. Este hecho no supone mayor problema si se trata de archivos de tamaño relativamente pequeño, el problema se origina cuando se trata de archivos de gran tamaño como pueden ser los de bases de datos. Aplicando este tipo de modelos de copias de seguridad un cambio, por mínimo que sea, en la base de datos origina una copia completa de la misma al encontrarse contenida en un único archivo, lo cual supone un desaprovechamiento excesivo de recursos. El modelo de copia a nivel de bloques soluciona este inconveniente.

En esencia este proceso evalúa los datos que han cambiado rompiendo los archivos en pequeños bloque de información. Típicamente los bloques son de entre 1 a 32 kilobytes de tamaño. A través de uso de algoritmos de chequeo redundante, se compara cada bloque de un archivo modificado con su correspondiente bloque en la versión anterior. Cuando se detecta una diferencia se crea una copia de ese bloque en particular. Al final del proceso se habrán obtenido un conjunto de bloques cuyo tamaño suele ser inferior al conjunto de archivos modificados.

Ilustración 20. Copia a nivel de bloque.

El archivo de respaldo resultante es, no obstante, de mayor tamaño del que se cabría esperar si se computan los tamaños de los cambios, esto es debido a la naturaleza discreta de los bloques, ya que se copiarán los bloques enteros, incluso si lo modificado no afecta al bloque en su totalidad.

Es importante reseñar que las técnicas delta sólo se aplican a archivos modificados, no a los creados, que deben ser respaldados por otro método.

Existen copias a nivel de bloque tanto incrementales como diferenciales, que a parte de la naturaleza granular del modelo, funcionan bajo los mismos principios que las copias incrementales y diferenciales ordinarias.

El modelo Delta de copias de seguridad está especialmente indicado para ser usado en situaciones en las que los archivos han de ser respaldados inmediatamente de su modificación o creación (este fenómeno es conocido como copia de seguridad en tiempo real o protección de datos continua), o en el caso de respaldos den redes con poco ancho de banda o mediante servidores remotos.

Las principales ventajas que se pueden deducir de lo anteriormente descrito son su extrema velocidad y poco uso de espacio de almacenamiento. Por otro lado adolecen del inconveniente, en algunos casos inaceptable, de largo tiempo que requiere la recuperación de la información ya que los archivos han de ser reconstruidos a partir de los bloques en los que han sido divididos.

5.6.2 PARCHES BINARIOS (BINARY PATCH - FASTBIT)

La tecnología de parches binarios originariamente fue desarrollada como método de actualización de software. Para reducir costes y tiempo, los fabricantes distribuyen sus actualizaciones por medio de pequeños archivos o "parches" que contienen únicamente la diferencia binaria entre su software antiguo y la nueva versión. Una vez que el cliente lo ha recibido, estos parches son aplicados sobre los archivos existentes actualizándolos a la última versión. La ventaja obvia radica en el hecho de que el tamaño de la actualización se reduce significativamente. Recientemente se ha comenzado a adaptar esta tecnología al sector de copias de seguridad.

Aunque el la aplicación de "parches" pueda en un principio ser confundida con la tecnología de bloques, explicada anteriormente, se diferencian en un aspecto significativo: la técnica de parches binarios no evalúa un archivo como una colección de bloques discretos sino que lo hace a nivel de bits, es decir, como una cadena continua de datos binarios.

Utilizando un complejo algoritmo y un gestor de memoria especial, es capaz de comparar archivos y extraer "parches" de datos binarios que representan específicamente las diferencias entre las dos versiones del archivo. Consecuentemente se crea una archivo con exactamente el tamaño que ocupan los datos modificados, lo cual elimina el espacio no aprovechado que impone e método de bloques.

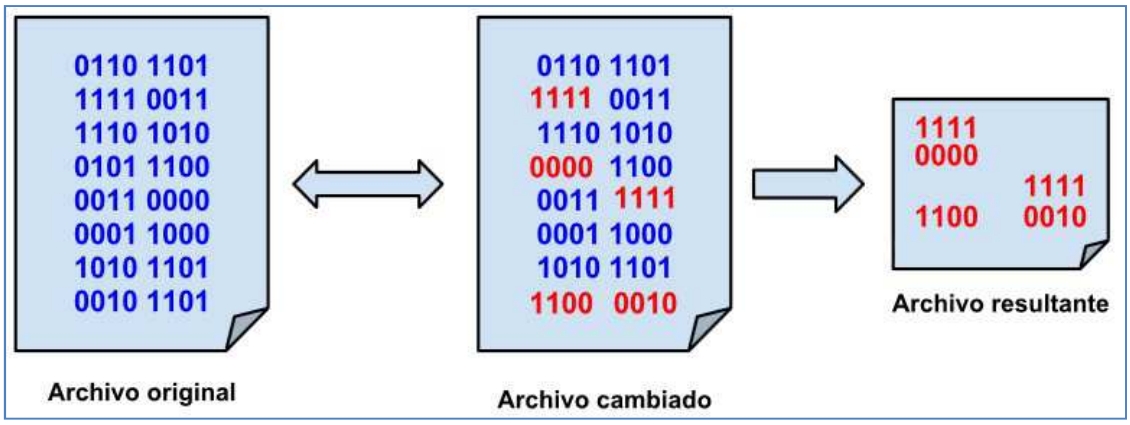


Ilustración 21. Proceso de "parcheado" binario.

Observando el proceso de "parcheado" binario se puede concluir que supone un descenso significativo en el tamaño del archivo de respaldo comparándolo con el mismo proceso realizado mediante el modelo de bloques.

5.6.3 COPIAS COMPLETAS SINTÉTICAS (SYNTHETIC FULL BACKUPS)

El modelo de copias sintéticas o sintetizadas (el término sintético se utiliza debido a que no se crean a partir de datos originales) más que un tipo de copias se debe entender como una tecnología de apoyo que debe ser aplicada a alguno de los métodos tradicionales de copias con el objetivo de conseguir respaldos y volcados más eficientes y rápidos (Comvault Systems).

Como norma general, esta tecnología solo se aplica en copias de seguridad del tipo cliente - servidor. Básicamente funciona de la siguiente manera:

- Los equipos clientes cliente realizan una copia mediante cualquiera de los métodos tradicionales.
- Las copias generadas son transferidas al servidor.
- El servidor en algún momento combina varias de esas copias individuales para conformar una copia completa sintética.

Tras la creación de esta copia total, los ordenadores clientes solamente necesitan realizar copias de los archivos nuevos o modificados, es decir, ya no será necesaria ninguna copia completa más.

El beneficio de configurar políticas de copias de seguridad con este tipo de copias es doble:

- La velocidad de generación de copias mediante modelos como el diferencial no se degradará en el tiempo debido al incremento producido por la acumulación de archivos, puesto que la copia sintética se estará actualizando constantemente y para el cliente siempre será como si de la primera copia diferencial se tratara.
- Cuando sea necesaria una restauración completa en alguno de los clientes, no hará falta reconstruir ningún archivo no partes de estos ya que la reconstrucción ya se ha realizado en el servidor permitiendo así la más rápida velocidad posible de recuperación.

6 GESTIÓN DE COPIAS DE SEGURIDAD

6.1 INTRODUCCIÓN

En el presente capítulo se estudiarán los distintos métodos que existen para la gestión de copias de seguridad. Independientemente del modelo que se haya decidido utilizar para su realización se ha de elegir un modo de gestionarlas.

Existen diversos métodos para realizar dicha tarea y, como al igual que ocurría con la elección de los modelos de copias, no son excluyentes entre sí, por lo que es importante que antes de decirse por uno u otro (o por una combinación de varios), se realice un exhaustivo estudio de viabilidad en el que se sopesen todas aquellas cuestiones relativas a la accesibilidad al sistema, y por lo tanto a los datos, la seguridad de los mismos y el coste de la gestión.

La gestión de copias de seguridad básicamente se puede realizar mediante cuatro métodos:

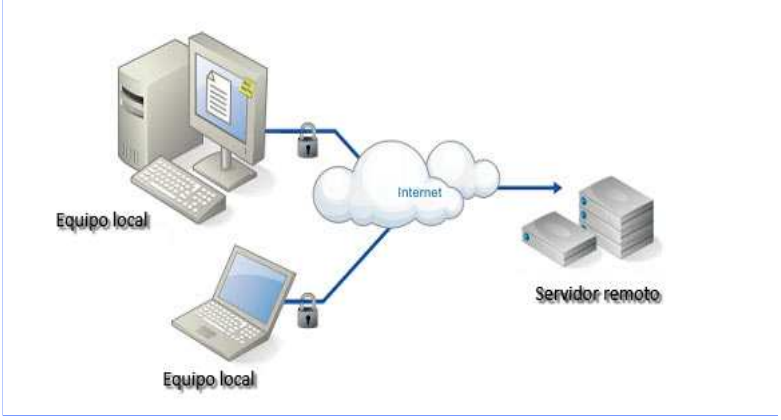
- Online.
- Nearline.
- Offline.
- Backup site o DCR (Disaster Recovery Center).

6.2 COPIAS DE SEGURIDAD ONLINE (CLOUD BACKUPS)

Las copias de seguridad online o *cloud backups* pueden ser definidas como un servicio basado en la web que permite a los clientes hacer copias de seguridad de sus datos y enviarlas a contenedores remotos protegidos.

Actualmente existen en el mercado tres tipos de figuras que ofertan este tipo de servicio (Clapperton, 2000): intermediarios, almacenes de datos y proveedores de servicios. Los intermediarios únicamente hacen de puente entre los clientes y otras compañías de software de copias de datos y los almacenes de datos alquilan espacio en sus servidores, permitiendo a sus clientes almacenar allí sus datos.

Los proveedores de servicios se ocupan de la gestión integra de las copias de seguridad. Por norma general instalan en el equipo un software cliente que ejecuta una tarea periódica programada. Dicha tarea se ocupa de recopilar, comprimir, cifrar y enviar los datos, mediante conexiones seguras, que conforman la copia de seguridad a un equipo remoto.



La utilización de sistemas de copia de seguridad online ofrece varias ventajas frente a otros sistemas que le hacen ser la opción ideal para tanto para el consumidor particular como para la pequeña y mediana empresa:

- El nivel de seguridad suele ser alto (aunque algunos proveedores no garantizan la seguridad de los datos obligando al cliente a realizar él mismo el encriptado), llegando en algunos casos a utilizar encriptados de hasta 128 bits, seguridad comparable a la de los sistemas militares y a la utilizada en las entidades bancarias. A demás la compresión y el encriptado se realiza en la máquina cliente antes de ser enviada al servidor remoto, lo cual aumenta la seguridad del envío.

- Los datos de respaldo son físicamente separados de los originales, evitando de esta manera los posibles perjuicios que pudieran ocasionar el robo o los desastres naturales.

- La mayoría de los servicios permiten el uso del modelo por bloques (delta) de copia, con lo que se tiene seguridad de que solo los cambios con copiados, reduciendo el tamaño de los paquetes a mandar por la red.

- Es virtualmente imposible que un usuario, tanto por descuido o malintencionadamente, dañe las copias de seguridad.

- Por norma general, las aplicaciones de los proveedores de servicios son capaces de soportar cualquier sistema operativo (Linux, Windows, Solaris, Unix) y sistema de archivos (NTFS, FAT, Linux, etc.).

- La capacidad de almacenamiento suele ser ampliable.

- El acceso a los datos únicamente lo puede realizar el cliente y generalmente de una manera amigable y apta para cualquier tipo de usuario.

- En la actualidad existen servicios que ofrecen acceso a los datos almacenados vía teléfono móvil.

Como ya se ha comentado al comienzo de esta sección, la tecnología de copias de seguridad online está basada en la web, es decir, los datos son transmitidos a través de internet hasta llegar a los servidores remotos que los albergarán. Por este motivo los inconvenientes que pueden llegar a surgir al utilizar esta tecnología tienen su raíz precisamente en el medio en el que se desarrolla: la red.

Los principales inconvenientes pueden ser:

- Caídas de red.

- Saturación del ancho de banda.

- El tamaño del ancho de banda puede originar que en determinadas circunstancias el revolcado de datos sea excesivamente lento, llegándose incluso, en casos extremos, a imposibilitarlo.

- Un excesivo tiempo de conexión a la hora de realizar la copia o restaurarla puede elevar los costes finales.

Tras lo expuesto, se llega a la conclusión de que, si bien las copias de seguridad son una opción sencilla y funcional de realizar copias de seguridad, también es cierto que no están carentes de inconvenientes, por lo que es necesario sopesar los pros y los contras antes de tomar la decisión de si utilizar o no este tipo de copias, en ese sentido

Russ Fellows[19] ha ideado la siguiente tabla en la que ilustra cuando los respaldos en la nube deberían ser considerados como una opción viable.

Factor Respaldo	Almacenamiento en la nube	Copia tradicional
Cantidad de datos	Mejor cuando la cantidad total a proteger es menor de 1GB por cada 1 MB e ancho de banda.	Para cantidades grandes de datos, o para entornos con limitada conectividad de red, son más apropiadas las técnicas tradicionales de respaldo.
Porcentaje de cambios	Mejor cuando el porcentaje de cambio por mes es menor al 10% del total de los datos.	En caso de datos que cambian frecuentemente, las copias de seguridad tradicionales, que utilizan discos o cintas, los cuales son separados del sistema, son más adecuadas.

Fuente: http://searchdatabackup.techtarget.com/definition/cloud-backup.

[19] Russ Fellows es analista sénior en Evaluator Group.

6.3 COPIAS DE SEGURIDAD OFFLINE

El almacenamiento de datos *offline*, permite a un usuario acceder a ellos incluso cuando no esté conectado a la red en cuestión.

En cuanto a copias de seguridad, el término se utiliza para referirse a un tipo de copia que se realiza cuando el sistema se encuentra "desconectado" y por lo tanto no son accesibles para ser modificados. El resultado es una "instantánea" de los datos que no puede ser modificada. Se utiliza sobre todo en el ámbito de bases de datos y debido a la desconexión forzada de esta, previenen el riesgo de copiar datos que se encuentren actualizándose o en proceso de creación.

La copia *offline*, también llamada *fría* implica tiempo de inactividad, ya que los usuarios no pueden acceder a los datos mientras se está realizando.

6.4 COPIAS DE SEGURIDAD NEARLINE

El término *nearline backups* hace referencia a copias de seguridad que se encuentran almacenadas en dispositivos estáticos o dinámicos separados físicamente del sistema y a los que se debe acceder de una manera mecánica (ya sea manualmente o mediante la utilización de robots).

En la actualidad existen principalmente dos métodos mecanizados utilizados para el almacenamiento o acceso a los datos guardados mediante este modelo de gestión: la librería de cintas magnéticas (Tape library) y la máquina de discos ópticos (Optical jukebox).

La librería de cintas magnéticas es un dispositivo de almacenamiento compuesto por un número indeterminado de slots o ranuras que albergan cintas magnéticas, cada una de ellas identificada por un código de barras único. A demás dispone de un lector de códigos de barras y un robot de carga.

El sistema solicita la información de una determinada cinta que es buscada por el lector de códigos de barra. Este comunica al robot la cinta en cuestión que se encarga de transportarla al dispositivo de lectura / escritura instalado en la máquina.

La cantidad de información que se puede llegar a almacenar en este tipo de dispositivos es virtualmente ilimitada. Este hecho, unido a su bajo índice de velocidad, debido principalmente a su parte mecánica, lo convierte en un dispositivo típico de almacenamiento de copias de seguridad.

La máquina de discos ópticos dispone de una funcionalidad básicamente idéntica a la librería de cintas magnéticas. Su principal diferencia reside en el hecho de almacenar la información en distintos soportes ópticos (cd, dvd, blu-ray, etc.), y al igual que en caso de esta, su capacidad de almacenamiento es casi ilimitada, llegándose en determinados dispositivos a almacenar un volumen de datos del orden de los petabytes (1 Petabyte = 1.000 Terabytes).

6.5 UNA NUEVA INTERPRETACIÓN DE LOS TÉRMINOS OFFLINE Y NEARLINE

Llegados a este punto cabe destacar que determinados autores, como es el caso de Steven Nelson en su libro "*Pro Data Backup and Recovery*", mantienen que los términos *offline* y *nearline*, no pueden ser referidos en el ámbito de las copias de seguridad directamente.

Nelson utiliza el concepto de *archivo (archive)*. Postula una situación en la que una empresa necesita mantener una copias de datos (obsérvese que en ningún momento se hace referencia a que la empresa necesite mantener una copia de seguridad de dichos datos) durante un periodo de diez años, con la peculiaridad de que dichos datos son estáticos, es decir, no van a cambiar a lo largo del tiempo. En este escenario una política estándar de copias de seguridad basada en una copia completa semanal y las correspondientes copias incrementales o diferenciales diarias, originaría al final de esos diez años un volumen de datos elevado y posiblemente inmanejable y cuyos ficheros de respaldo contendrían (al ser los datos estáticos) todos la misma información.

La solución a este desperdicio de espacio pasa por la creación del archivo[20]. El archivo no está compuesto por las copias de los datos estáticos, sino por los originales movidos a una localización distinta.

A los datos archivados se les hace un seguimiento a lo largo del tiempo pero nunca cambian. Si es necesario modificar alguno, el software encargado de la gestión del archivo puede eliminar el archivo original o como si de un nuevo dato se tratara añadiéndolo al archivo.

La potencia de separar los daos estáticos de los dinámicos reside en la disminución, drástica según el caso, del volumen de la copia de seguridad, por ejemplo de en un sistema en el que los datos ocuparan 20 T y de ellos 5TB fueran estáticos, la copia de seguridades reduciría en un 25%.

Se puede tener acceso a los datos originales de dos maneras distintas dependiendo del método de creación del archivo: *offline* y *nearline*.

El método *offline* crea una copia de los datos en un dispositivo estático y elimina la copia original de los mismos. Si es necesario el acceso a alguno de los datos se realiza a través de peticiones específicas al software de gestión que creó los archivos, este lo

[20] El término *archivo* se utiliza con la acepción de la Real Academia Española como el lugar donde se custodian uno a varios archivos.

demanda al dispositivo de almacenamiento y lo ubica en el contenedor de datos principal.

El método *nearline* o *archivo activo* difiere con el anterior principalmente en que su existencia es transparente al usuario final. Los sistemas de archivo activo normalmente interactúan con el sistema de archivos o las estructuras de datos que están gestionando, migrando datos a varios dispositivos (estáticos o dinámicos). En orden a tener control de los cambios de ubicación que realizan en los datos dejan marcas en el sistema de archivos que representan los daos migrados. Cuando un usuario necesita acceder a alguno de los datos migrados el software de archivado intercepta la petición y se hace cargo de la misma. Interpreta qué archivos son los solicitados y busca en los índices dónde se encuentran ubicados actualmente, comunicándoselo al sistema operativo, el cual puede finalizar la operación de una manera segura.

La separación de datos estáticos en archivos no implica de modo alguno que no sea necesario realizar copia de seguridad de estos. Todo lo contrario, como ya se ha comentado anteriormente, se trata de los datos originales separados del resto, por lo que es muy importante planificar una buena política de copias de seguridad de los mismos que tenga en cuenta su carácter estático.

6.6 BACKUP SITE O DCR (DISASTER RECOVERY CENTER)

El concepto de Cetro de Recuperación de Desastre, también llamado *backup site* o DCR, tiene su punto de partida a mediados de los años 1970, cuando el ser humano se hace consciente de su estrecha dependencia en todos los ámbitos de la vida de los sistemas informáticos y del colapso que podría suponer la repentina ausencia de estos.

Como resultado de esta preocupación surgen los primeros DCR, en los que tanto las empresas como las organizaciones gubernamentales vuelcan sus datos e infraestructuras informáticas tratando de asegurar así la continuidad de sus actividades ante posibles "apagones informáticos" o desastres naturales.

En principio el uso o mantenimiento de un DCR no implica intrínsecamente la creación y gestión de las copias de seguridad de los datos, sin embargo es práctica habitual que las empresas que ofertan los servicios de un centro de recuperación de desastre lo ofrezcan.

Existen básicamente tres tipos de DCR: calientes (*hot sites*), fríos (*cold sites*) y templados (*warm sites*).

6.6.1 SITIOS FRÍOS (*COLD SITES*)

Los sitios fríos por lo general no incluyen la gestión de las copias de seguridad, la instalación de los datos originales ni la instalación de la infraestructura ni el hardware. Tan solo ofrecen un espacio de "oficina".

Es la opción más económica pero implica por un lado tener una buena política de copias de seguridad y por otro, ante un desastre, es necesario tiempo para volcar los datos, instalar la infraestructura y reanudar la actividad normal.

6.6.2 SITIOS CALIENTES (HOT SITES)

Los sitios calientes ofrecen un duplicado exacto del lugar habitual de trabajo de la empresa u organización. Por norma general ofrecen sincronización en tiempo real con los datos originales y la creación, gestión y seguimiento de las copias de seguridad de los datos.

En teoría, ante un desastre, el tiempo de reacción sería mínimo, con una pérdida virtualmente nula de información al estar el sistema constantemente actualizándose. Por todas estas ventajas se convierte en la opción más cara de todas.

6.6.3 SITIOS TEMPLADOS (WARM SITES)

Se trata de una mezcla de los dos anteriores (sitios fríos y calientes). Opera a una escala intermedia, es decir, si bien se encuentran conectados, configurados y con políticas de copias de seguridad de datos, no gozan de la ventaja de la sincronización en tiempo real.

Al no encontrarse sincronizados, los dos sitios, el normal de trabajo y el DCR, tienen un desfase de datos, por lo que estos no se encuentran actualizados. Ante un desastre, si bien el sitio podría comenzar a operar de inmediato, lo haría con datos obsoletos y sería necesario, si fuera posible, una actualización de los mismos, por lo que el tiempo de respuesta se ampliaría y paralelamente aumentaría el riesgo de pérdida de información.

7 METODOLOGÍA DE COPIAS DE SEGURIDAD

7.1 INTRODUCCIÓN

En el diseño de una adecuada política de copias de seguridad se han de tener en consideración numerosos aspectos que, en conjunción, hagan de ella un medio seguro, eficaz y ágil de respaldo de datos.

Aspectos básicos como qué datos incluir en la copia de respaldo, con qué periodicidad realizarla o qué tipo de copia hacer, son de una importancia tal que por norma general se tienen en cuenta de una manera automática. Esto sucede, bien conscientemente por parte de la persona encargada de programar las copias, o bien por exigencia de la mayoría del software especializado en este tipo de tareas, que obliga a definir de una manera explícita dichos parámetros.

Sin embargo, existen otras facetas que, no siendo tan obvias ni directas, son de igual importancia para conseguir copias de seguridad fiables. Cuestiones como la separación física de las copias del lugar de origen; la realización de pruebas de verificación, tanto de la correcta generación de los archivos de respaldo, como de la integridad de los datos que contienen; o el mantenimiento de un historial de las copias generadas, aseguran que los archivos que se han generado como copias de seguridad, no sólo contienen los datos correctos, sino que en caso de desastre van a servir a su fin último, esto es, devolver al sistema su estado original.

Teniendo en consideración que cada caso es distinto, con su propia problemática, por lo que, en las siguientes secciones se ofrecerá una visión general de cada uno de los temas que es necesario tener en cuenta en orden a planificar la política de copias de seguridad.

7.2 QUÉ DATOS COPIAR

7.2.1 INTRODUCCIÓN

La primera tarea a realizar en el momento de planificar una buena política de copias de seguridad, consiste en la identificación de una manera exhaustiva de todos aquellos datos que deben ser respaldados. Una regla básica al respecto determina que se deberían respaldar todos aquellos datos que se necesitarían para efectuar la total recuperación de los sistemas, o que fueran necesarios en orden a consideraciones legales o financieras (De Guise, 2009, pág. 97).

La identificación de dichos datos no es una tarea sencilla. Desde el punto de vista de la ingeniería del software requiere un profundo conocimiento del entorno de trabajo de la organización para la que se diseñará la política de copias de seguridad, y tal fin no se conseguirá, sino la consecución de tres pasos secuenciales:

- Recopilación de la información: en este primer paso se recabará toda la información necesaria del entorno de trabajo objeto de las futuras copias de seguridad.
- Realización de inventario: en el que se aunará la información anteriormente conseguida y los medios físicos de los que se dispone.
- Decisión sobre los datos a respaldar: finalmente teniendo en cuenta los pasos anteriores se procederá a decidir qué datos respaldar.

7.2.2 RECOPILACIÓN DE INFORMACIÓN

La recopilación de información se puede realizar mediante tres vías: entrevistas con usuarios del sistema, conocimiento del software utilizado y observación sobre el terreno. La conjunción de la información obtenida por cada una de ellas ofrecerá una visión de conjunto necesaria para la toma de decisiones finales.

Mediante entrevistas con los usuarios del sistema, y utilizando técnicas propias de la ingeniería del software, será necesario identificar qué tareas realizan en su habitual modo de trabajo. Dicha información permitirá conocer qué tipo de software utilizan normalmente y cómo hacen uso del mismo, posibilitando la identificación del tipo de datos que usualmente manejan.

Así mismo es importante conocer cuál es la política que ha establecido la organización en cuanto a almacenamiento de datos por parte de los usuarios. En este sentido se pueden dar, principalmente dos tipos de situaciones:

- Los usuarios no pueden almacenar ningún tipo de dato en sus equipos, ya sean ordenadores portátiles o personales. Toda la información generada por el usuario es mandada a un servidor central, bien en tiempo real o asincrónicamente.

- Los usuarios pueden almacenar en sus equipos aquella información que consideren necesaria en el desarrollo de su trabajo. En este supuesto se pueden dar a su vez dos casos; que el usuario no mande ningún tipo de información al servidor o que envíe aquella que considera oportuno.

Otro aspecto a tener en cuenta es qué tipo de software es utilizado habitualmente en la organización por parte de los usuarios. Se ha de saber qué tratamiento de datos realiza cada una de las aplicaciones utilizadas. Toda información relativa a qué tipo de datos genera, dónde los almacena o en que formato es fundamental a la hora de diseñar una planificación del respaldo de dichos datos.

En el caso de tratarse de software de código abierto o privado pero de pública distribución, dicha información se puede obtener de manera relativamente fácil, ya que normalmente se encuentra publicada y accesible a través de distintos medios (internet, libros, manuales).

Si por el contrario se trata de software específico para el tipo de actividad desarrollado por la organización, se deberá acudir a las especificaciones del mismo, o en su defecto, a la comunicación directa con la empresa desarrolladora del mismo a fin de que dicha información sea suministrada.

El último paso necesario en la labor de obtención de información consiste en la observación sobre el terreno. Es buena práctica acudir al puesto de trabajo de los usuarios y observar cómo realizan su tarea, ya que por un lado se podrá confirmar la información obtenida mediante las entrevistas realizadas y por otro se podrá detectar determinados hábitos de los usuarios de los cuales, bien por error o por omisión, no han informado.

7.2.3 REALIZACIÓN DEL INVENTARIO

Una vez recabada toda la información posible, el siguiente paso consiste en inventariarla. Esta tarea, además de ayudar a tomar la decisión final sobre qué datos respaldar, servirá de ayuda de referencia ante un posible episodio de desastre y necesidad de revolcado de datos (Preston Curtis, 2007, págs. 21,22).

A la hora de realizar el inventario, se han de tener en cuenta diversos aspectos, que deberán ser recogidos de la manera más exacta posible. Entre otras cuestiones como mínimo se deberá disponer de toda la información relativa a:

- Discos del sistema.
- Particionamiento de los discos.
- Hardware.
- Configuración de bases de datos y contenedores de datos.
- Configuración de DHCP, Active Directory, NFS y CIFS.

7.2.3.1 LISTADO DE DISCOS DEL SISTEMA Y SUS PARTICIONES

Normalmente, dentro de un mismo sistema coexiste más de un disco. Será necesario inventariar tanto la capacidad, como la unidad y el modelo de cada uno de ellos.

En sistemas Unix y Mac OS se graba en el archivo *messages*, y en Microsoft Windows dicha información se almacena en el registro del sistema.

Ilustración 22. Registro de Windows.

La cuestión relativa a de qué manera están particionados los discos duros cobra mayor importancia a la hora de restaurar sistemas operativos o bases de datos. La información acerca de cómo se encuentran divididos los discos no se guarda

explícitamente en ninguna ubicación del sistema, por lo que es necesario extraerla y almacenarla manualmente.

En sistemas Windows se puede acceder a esta información a través de la línea de comandos mediante la instrucción ***diskpart***. Los parámetros que se le pueden pasar son muchos y variados, todos ellos orientados a la gestión de discos y sus particiones. Seguidamente se muestra una imagen en la que se puede apreciar todos los parámetros disponibles.

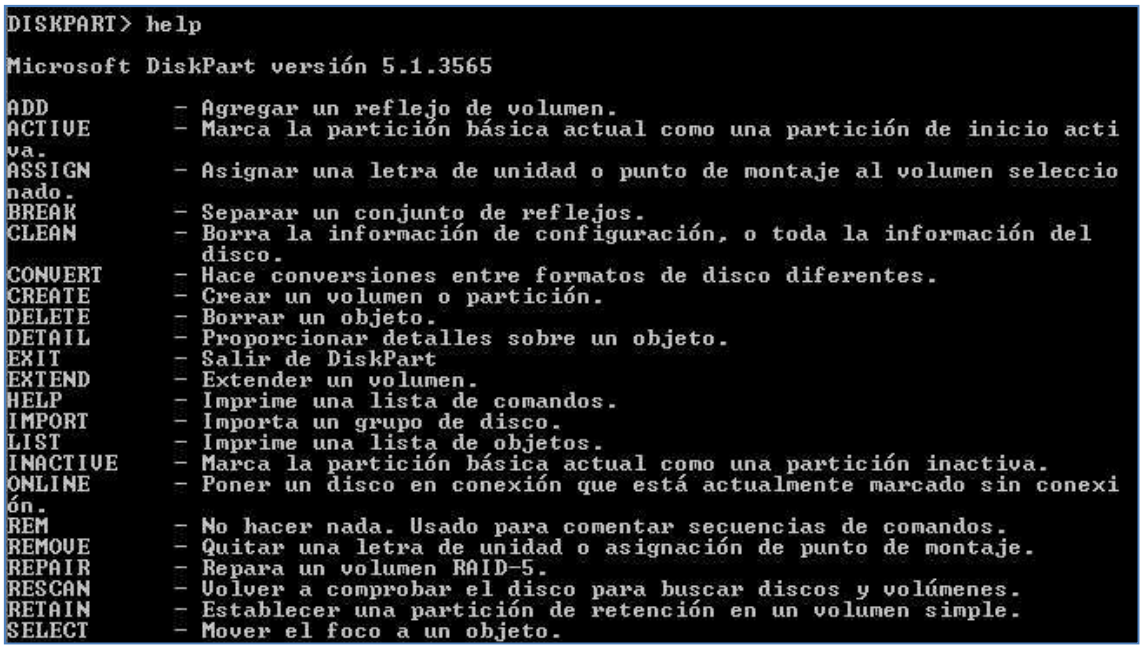


Ilustración 23. El comando *diskpart* y todos sus parámetros.

Mediante dicho comando, y utilizando los parámetros "***select***" y "**list partition**" se puede obtener un listado de las particiones de cualquier disco del sistema. Como ejemplo se muestra una imagen en la que se ha pedido a través de la línea de comandos de Windows, el listado de las particiones del disco 1 del sistema.

```
C:\Documents and Settings\Administrador>diskpart

Microsoft DiskPart versión 5.1.3565

Copyright (C) 1999-2003 Microsoft Corporation.
En el equipo: INTERNET

DISKPART> list disk

  Disco ###  Estado      Tamaño     Libre     Din.  Gpt
  ---------  ----------  -------  --------  ---  ---
  Disco 0    En pantall    77 GB      0 B
  Disco 1    En pantall   190 GB      0 B
  Disco 2    En pantall   932 GB      0 B

DISKPART> select disk 1

El disco 1 es ahora el disco seleccionado.

DISKPART> list partition

  Partición ###  Tipo              Tamaño     Desplazamiento
  -------------  ----------------  -------  -------
  Partición 1    Principal          49 GB    32 KB
  Partición 2    Principal         141 GB    49 GB

DISKPART>
```

Ilustración 24. Uso del comando *diskpart*.

Como se puede observar la secuencia de comandos es la siguiente:

1. Se accede a la utilidad ***diskpart***.
2. Se listan los discos existentes en el sistema con el comando "***list disk***".
3. Se selecciona el disco deseado (en este caso el número 1), con el fin de que adquiera el foco, con el comando "***seleck disk 1***".
4. Se solicita un listado de las particiones de ese disco mediante el comando "***list partition***".

Una vez que se ha obtenido la información de las particiones del disco, se puede obtener un listado con los detalles de cada una de ellas, para ello basta con utilizar el comando "***detail***" una vez que se ha seleccionado la partición deseada. La siguiente imagen muestra un ejemplo.

```
DISKPART> select partition 1

La partición 1 es ahora la partición seleccionada.

DISKPART> detail partition

Partición 1
Tipo: 07
Oculta: No
Activa: Sí

  Volumen ###  Etiqueta  Ltr         Fs     Tipo        Tamaño     Estado     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
* Volumen 3     C                NTFS   Partición     49 GB  Correcto   Inicio

DISKPART> select partition 2

La partición 2 es ahora la partición seleccionada.

DISKPART> detail partition

Partición 2
Tipo: 07
Oculta: No
Activa: No

  Volumen ###  Etiqueta  Ltr         Fs     Tipo        Tamaño     Estado     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
* Volumen 4     G   Datos        NTFS   Partición    141 GB  Correcto

DISKPART>
```

Ilustración 25. Detalle de particiones.

Como se puede observar la secuencia realizada es la siguiente:

1. Se selecciona la partición deseada (en este caso la número 1) con el comando "***select partition 1***", con lo que adquiere el foco.
2. Mediante el comando "***detail partition***" se obtienen los detalles de dicha partición.
3. Se repite el proceso para cada una de las particiones.

Una vez obtenida la pantalla con toda la información necesaria, se puede mediante el botón derecho, seleccionar todo el contenido de la misma, tras lo cual con la secuencia

de combinaciones de teclas Ctrl+C y Ctrl+V pegarlo en un documento de Word o en el block de notas de Windows y guardarlo.

La misma información se puede obtener, de una forma gráfica mediante el administrador de discos.

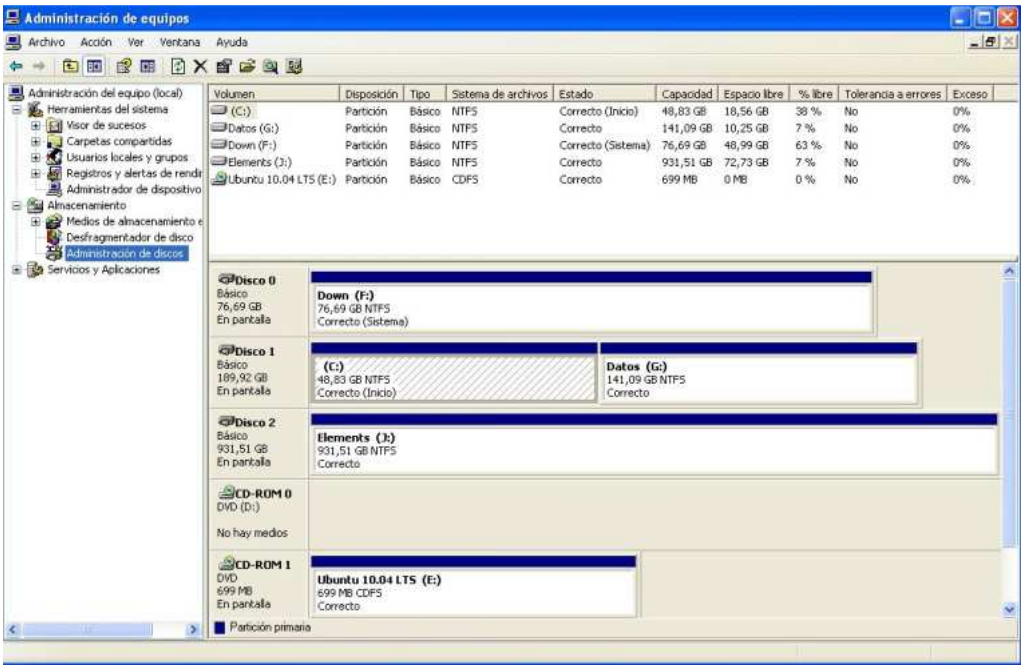


Ilustración 26. Administrador de discos en Windows.

En sistemas *Solaris* existe el comando ***prtvtoc*** cuya función es la de reportar información sobre la geometría y el particionamiento de un disco (Oracle, 2010), por lo que cabe la posibilidad de ir consultando dicha información disco a disco.

Tal y como se recoge en la documentación en línea de *Oracle*, la notación de dicho comando es: *prtvtoc [-fhs] [-t vfstab] [-m mnttab] nombre_dispositivo*. Y dispone de las opciones siguientes:

- -f: informa del espacio libre del disco, incluyendo la dirección del bloque de comienzo del espacio libre, número de bloques y las particiones no utilizadas.
- -h: omite los encabezados.
- -m mnttab: utiliza mnttab como lista de sistemas de archivos montados, en lugar de /etc/mnttab.
- - t vfstab: utiliza vfstab como lista de sistema de archivos por defecto, en lugar de /etc/vfstab.

La siguiente imagen ilustra el uso de dicho comando sobre un disco de aproximadamente 1 TB de capacidad.

```
example# prtvtoc /dev/rdsk/c1t1d0s2
* /dev/rdsk/c1t1d0s2 partition map
*
* Dimensions:
*     512 bytes/sector
* 3187630080 sectors
* 3187630013 accessible sectors
*
* Flags:
*   1: unmountable
*  10: read-only
*
*                          First     Sector    Last
* Partition  Tag  Flags    Sector     Count    Sector  Mount Directory
0      2    00         34    262144    262177
1      3    01     262178    262144    524321
6      4    00     524322 3187089340 3187613661
8     11    00  3187613662     16384 3187630045
```

Ilustración 27. Uso del comando *prtvtoc* de *Linux*.

7.2.3.2 HARDWARE

De la misma manera que es importante disponer de toda la información referente a los discos del sistema y sus pariciones, es necesario conocer los modelos y características de los principales componentes del hardware, tales como el modelo de placa base, el modelo de la tarjeta de red (si es el caso) o el modelo de la tarjeta de video.

Como norma general esta información figura en la documentación de los equipos informáticos o en sus discos de instalación, por lo que será necesario tenerlos controlados y almacenados en lugar seguro y accesible.

Sin embargo en determinadas ocasiones esa información se encuentra extraviada u obsoleta, por ejemplo por cambios realizados en el hardware original del sistema, si este es el caso existen multitud de aplicaciones, tanto de uso comercial como gratuito, las cuales permiten realizar un chequeo del sistema y obtener un informe de todos los componentes de que dispone, y en la mayoría de los casos, ofrecen utilidades para exportarlo a algún tipo de formato almacenable. ***aida64*** (*http://www.aida64.com/downloads/a64xe*), antiguo Everest, ***Speccy*** (*http://www.piriform.com/speccy*) y ***Everest*** (aún descargable en http://majorgeeks.com/download4181.html), son tres ejemplos de aplicaciones de este tipo, la primera de uso comercial y la segunda y tercera de uso libre.

En la siguiente imagen se puede observar una de las pantallas de información, que sobre un determinado equipo, se obtiene con el software ***aida64***, comentado anteriormente, en su edición Extreme de prueba.

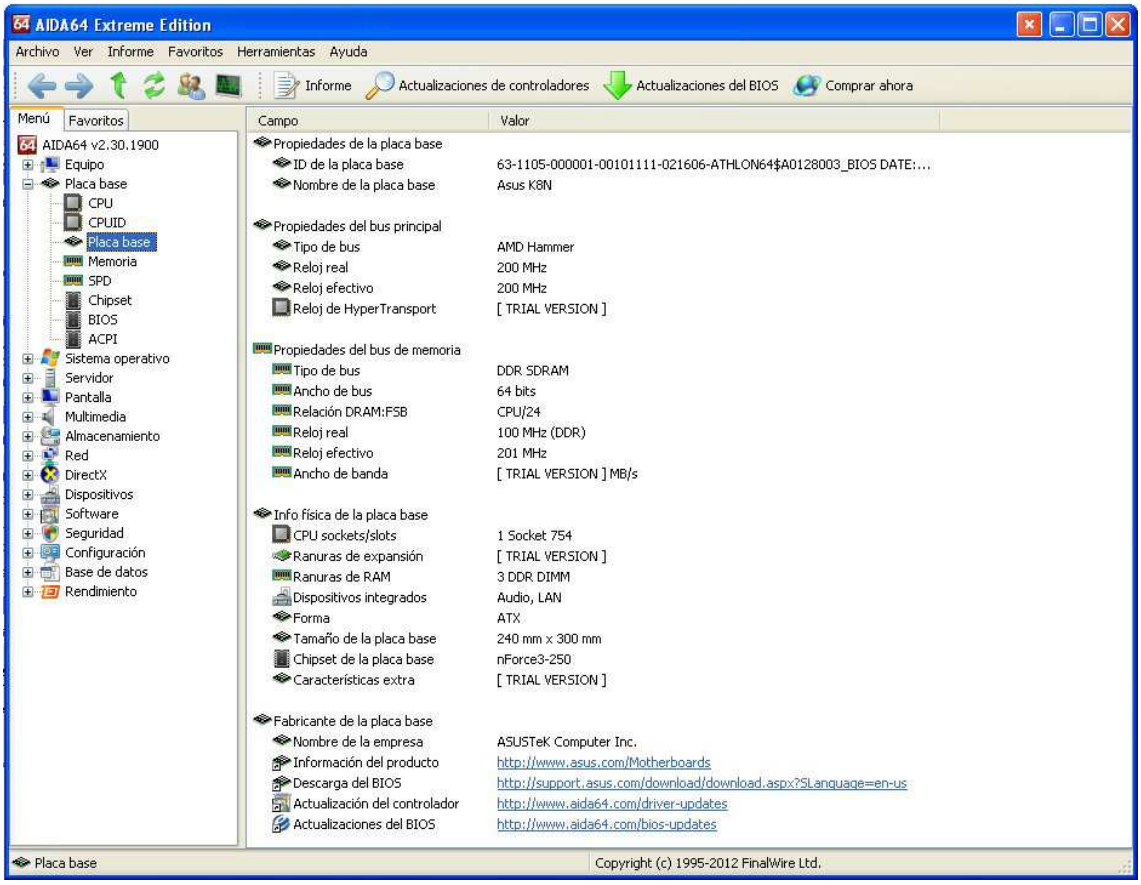


Ilustración 28. Informe de placa base obtenido con el software Aida64.

El informe obtenido por este tipo de aplicaciones deberá ser almacenado e incluido en la rutina de copias de seguridad del sistema.

7.2.3.3 CONFIGURACIÓN DE LAS BASES DE DATOS Y CONTENEDORES DE DATOS

7.2.3.3.1 Breve descripción de las bases de datos

Una base de datos se puede definir como un conjunto de ficheros entre los que se establecen vínculos o interrelaciones y que guardan algún tipo de información.

Para que la base datos sea útil debe recuperar los datos almacenados eficientemente. Esta necesidad de eficiencia ha provocado que los diseñadores recurrieran a estructuras de datos complejas para la representación de los datos, complejidad que es deliberadamente ocultada a los usuarios mediante varios niveles de abstracción que simplifica la interacción entre estos y el sistema.

Los niveles de abstracción son el nivel físico, el lógico y el de vistas, y se pueden definir de la siguiente manera:

- **Nivel físico**: representa el nivel más bajo de abstracción, y define cómo se almacenan realmente los datos. Describe en detalle las estructuras de datos complejas de bajo nivel.

- **Nivel lógico**: nivel inmediatamente superior al físico. Define qué datos se almacenan en la base de datos. Describe toda la base de datos en términos de un número pequeño de estructuras relativamente simples. Los administradores de bases de datos, que deben decidir la información que se guarda en las mismas, utilizan este nivel.

- **Nivel de vistas**: se trata del nivel más elevado de abstracción y sólo describe parte de la base de datos. Existe para simplificar la interacción entre los usuarios y el sistema de base de datos.

Bajo la estructura de las bases de datos se encuentra el modelo de datos, consistente en utilidades conceptuales que sirven para describir los datos, sus relaciones, su semántica y las restricciones de consistencia (Silberschatz, Korth, & Sudarshan, 2006).

Los modelos de bases de datos pueden ser clasificados en cuatro tipos básicos: relacional, entidad - relación, orientado a objetos y de datos semiestructurados, y sus principales características se pueden resumir de la siguiente forma:

- **Relacional**: utiliza una serie de tablas para representar tanto los datos como las relaciones. Cada tabla está formada por una o más columnas y cada una de ellas tiene un nombre único que las distingue de las demás.

  Es un modelo basado en registros, en el que cada tabla de la base de datos contiene registros de un determinado tipo, y cada registro está definido por un conjunto fijo de atributos, denominados *campos*. Las columnas de la tabla se corresponden con los atributos del tipo de registro.

- **Entidad – relación**: consiste en un conjunto de objetos básicos, denominados *entidades*, y las relaciones entre ellos. Una entidad es un objeto del mundo real que es distinguible de otros. Se utiliza fundamentalmente en el diseño de bases de datos.

- **Orientado a objetos**: se puede considerar como una extensión del modelo entidad – relación en el que se han incluido funcionalidades propias de la programación orientada a objetos, tales como la encapsulación, la utilización de métodos y el concepto de entidad de objeto.

- **De datos semiestructurados:** es un modelo que tiene la particularidad de permitir la especificación de datos donde los elementos de datos individuales pertenecientes al mismo tipo pueden poseer diferentes conjuntos de atributos.

7.2.3.3.2 Sistemas de gestión de bases de datos y copias de seguridad

Las primeras bases de datos utilizaban ficheros para el almacenamiento de la información. Esos ficheros contenían datos interrelacionados y eran compartidos por varios procesos de forma simultánea.

A medida que las bases de datos comenzaron a crecer, el software de gestión que las procesaba se mostró demasiado elemental como para poder responder de una manera eficiente a la creciente demanda de operaciones, usuarios y consultas. Por ese motivo, especialmente durante la segunda mitad de los años 1970, comenzaron a ver la luz aplicaciones especializadas en gestionar grandes bases de datos de una manera cada vez más eficiente y con interfaces más amigables, tanto para diseñadores como para los usuarios finales. Se trataba de los sistemas de gestión de bases de datos (SGBD).

En la actualidad existe multitud de SGBD, tanto gratuitas como comerciales, y cada una de ellas gestiona y almacena sus bases de datos de manera diferente, por lo que el proceso de copia de seguridad de las mismas varía entre unas y otras. En la siguiente tabla se puede observar los SGBD más utilizados.

Licencia	Nombre
Gratuita	Postgre SQL
Gratuita	MySQL
Gratuita	DB2-Express C (Edición limitada de DB2 de IBM)
Gratuita	Oracle Express (Edición limitada de Oracle)
Gratuita	SQL Server Express (Edición limitada de Microsoft SQL Server)
Comercial	MySQL (Edición comercial)
Comercial	dBase
Comercial	IBM Informix
Comercial	Microsoft SQL Server
Comercial	Oracle
Comercial	Sybase

Cada base de datos es distinta a las demás y está configurada de una manera única. Es necesario recabar y documentar la configuración de todas las bases de datos de la organización.

A la hora de programar las copias de seguridad hay que tomar las debidas precauciones en orden a obtener una copia de la base de datos viable. Es un error demasiado común el creer que basta con realizar una copia simple de los archivos de las bases de datos, ya que esta operación se debe realizar bajo unas determinadas condiciones, como el que la base de datos se encuentre cerrada, que no existan transacciones pendientes (si se trata de una base de datos transaccional), y otras muchas que hacen que la copia de seguridad las bases de datos de un sistema se deban realizar, preferentemente, con las herramientas propias de la base de datos en cuestión.

En los anexos II y III se pueden encontrar algunos métodos para generar copias de seguridad totalmente viables con PostgreSQL y MySQL respectivamente.

En todo caso, si se opta por la realización de las copias de las bases de datos mediante un software especializado en copias de respaldo, es necesario tener en consideración las recomendaciones que sobre el tema vendrá reflejadas en la documentación del SGBD.

7.2.3.3.3 Configuración de otros contenedores de datos

De la misma manera que se debe obtener información detallada de las bases de datos el sistema, se tendrá que documentar cualquier otro tipo de contenedor de datos que se utilice en la organización. Téngase como ejemplo el caso de una pequeña organización en la que no utilizan ninguna base de datos convencional, sino que sus datos se basan en documentos de Microsoft Word que almacenan en carpetas ubicadas en distintas carpetas del servidor y puestos de trabajo, en ese caso será necesario, entre otras cosas, documentar la ubicación de todas las carpetas contenedoras, en orden a poder definir una copia de respaldo adecuada.

7.2.3.4 CONFIGURACIÓN DE DHCP, ACTIVE DIRECTORY, NFS Y CIFS

En caso de desastre y consecuentemente sea imperativa una reinstalación total, será imprescindible haber documentado y tener actualizado la información acerca de cómo configurar correctamente el protocolo de configuración dinámico del host (DHCP), el directorio activo (AD), el sistema de archivos de red (NFS) y el sistema de archivos común de Internet (CIFS).

7.2.3.4.1 DHCP

El protocolo de configuración dinámica del host (**DHCP**)[21], es un protocolo de red que permite a un servidor asignar automáticamente una dirección IP a un ordenador de entre un rango definido de números configurado para una red de ordenadores dada (Indiana University, 2009).

DHCP asigna una dirección IP cuando un sistema arranca, la secuencia de acontecimientos es la siguiente:

1. Un usuario enciende un ordenador con un cliente DHCP.
2. El ordenador cliente envía una petición broadcast, llamada DISCOVER, buscando un servidor DHCP que le conteste.
3. El router direcciona la petición DISCOVER al servidor correspondiente.
4. El servidor recibe el paquete DISCOVER. Basado en la viabilidad y las políticas de uso establecidas en el servidor, este determina la dirección IP adecuada para el cliente. En ese momento el servidor reserva temporalmente la dirección para el cliente y le manda un paquete oferta, llamado OFFER o DHCPOFFER, con la información de esa dirección. El servidor también configura en el cliente los servidores DNS, WINS, NTP y otro tipo de servicios.
5. El cliente envía una petición, denominada REQUEST o DHCPREQUEST, haciendo saber al servidor que tiene la intención de usarla dirección IP facilitada.
6. El servidor envía un paquete ACK, o DHCPACK, confirmando que el cliente está identificado con la dirección IP durante un periodo de tiempo especificado por él mismo.

7.2.3.4.2 Active Directory

Active Directory (**AD**), es una estructura utilizada en ordenadores y servidores que corren bajo sistemas operativos de Microsoft Windows y se utiliza para almacenar información e la red de ordenadores, el dominio e información del usuario.

Su estructura normalmente está constituida en tres categorías que incluyen hardware, como impresoras y escáneres, servidores de correo web y objetos que constituyen las principales funciones dela red y el dominio. Principalmente utilizado por los

[21] Dynamic Host Configuration Protocol.

administradores para la gestión delos paquetes de software, cuentas y archivos en organizaciones de tamaño medio- grande.

El AD funciona como una base de datos de funcionalidad especial para los ordenadores con Windows. El sistema no está diseñado como sustituto del registro de Windows, sino que lo está tanto para gestionar un número elevado de operaciones de lectura y búsqueda, como cambios y actualizaciones. Los datos almacenados en el AD están diseñados para ser replicados, jerarquizados y extensibles.

La información relevante que normalmente se almacena en el Active Directory incluye datos de contacto del usuario, información de la cola de impresión y datos específicos de la configuración del ordenador o la red.

7.2.3.4.3 NFS

El sistema de archivos de red **NFS**[22]. Se trata de un sistema de archivos desarrollado por *Sun Microsystems* consistente en un sistema cliente – servidor que permite a los usuarios acceder a archivos a través de la red y tratarlos como si residieran en el directorio local de archivos.

Está diseñado para ser independiente del ordenador, sistema operativo, arquitectura de red o protocolo de transporte.

7.2.3.4.4 CIFS

El sistema de archivos común de Internet **CIFS**[23], también es conocido como bloque de mensajes del servidor[24]. Es un protocolo de red cuyo uso más común es la compartición de archivos en una red de área local, o LAN[25]. El protocolo se utiliza entre otras funciones para:

- Permitir a un cliente la manipulación de archivos como si se encontraran en su propio ordenador.

  Funciona enviando paquetes del cliente al servidor, normalmente peticiones de apertura, cierre o lectura de archivos, en una secuencia que se podría resumir de la siguiente manera (CodeFX, 2001):

[22] Network File System.
[23] Common Internet File System.
[24] Server Message Block o SMB.
[25] Local Área Network.

1. Una vez que le llega una petición del cliente, el servidor comprueba si la petición es legal, acorde con los parámetros definidos.
2. Verifica si el cliente goza de los permisos adecuados para la petición en cuestión.
3. Si es así ejecuta la petición y devuelve la contestación en un paquete de respuesta al cliente.
4. El cliente en ese momento comprueba la respuesta y determina si se corresponde o no con la petición inicial.

- Compartir archivos con otros clientes.
- Restaurar las conexiones automáticamente en caso de fallo en la red.
- Utilizar nombres de archivos *Unicode*. Unicode es un estándar de codificación de caracteres. Especifica un nombre identificador único para cada carácter o símbolo. El estándar es mantenido por el Unicode *Technical Comitee (UTC)*, integrado en el *Unicode Consortium*, del que forman parte empresas como Microsoft, IBM, Oracle y Google entre otras, además de distintas instituciones, profesionales y académicos.

En ocasiones puede ser problemático recabar toda la información anteriormente reseñada, por lo que la opción más aconsejable, será, que en caso de necesitar reinstalar un nuevo servidor se disponga de software que automatice la tarea, algunos ejemplos de este tipo de aplicaciones son:

- ***Jumpstart*** de *Sun.*
- ***Ignite-Ux*** de *Hp.*
- ***Kickstart*** de *Linux.*

7.2.4 QUÉ DATOS COPIAR

Una vez que se dispone de toda la información necesaria, es el momento de tomar una decisión crucial: qué datos incluir en la copia de seguridad.

Sobre este aspecto existen dos corrientes de actuación claramente diferenciadas: la que considera que es necesario realizar una copia total del sistema[26] y, en

[26] El concepto copia total, se refiere a la copia de la que se parte en la secuencia programada de copias, no implica en modo alguno que en cada sesión de copia se realice una copia total del sistema. La programación de las

contraposición, la que es partidaria de realizar una copia parcial del mismo. La decisión sobre qué política seguir dependerá en gran medida de las particularidades de cada tipo de escenario, no obstante se pueden, a priori, distinguir dos tipos de escenario básicos: servidores de datos y puestos de trabajo (ordenadores personales y portátiles).

Si bien esta división no es ni mucho menos definitiva, ya que se pueden dar multitud de combinaciones (servidores dedicados, servidores con puesto de trabajo, puestos de trabajo que realizan de funciones de servidores de daos, etc.), si es lo suficientemente representativa como para que sea válida como ejemplo.

7.2.4.1 SERVIDORES

En el caso de realizar copias de seguridad de servidores de datos, la opción más adecuada consiste en realizar copias completas del sistema.

Existen varias razones que desaconsejan el uso de copias de seguridad selectivas en entornos de servidores (Preston Curtis, 2007, págs. 26,27), entre las cuales la más importante es la dificultad de administración.

Las copias parciales del sistema implican la modificación de los scripts, o delas tareas programadas del software de respaldo utilizado, en cada ocasión que se produce un cambio significativo en el seno del servidor, tales como actualizaciones, inclusión de nuevas unidades, cambio de ubicación de datos, etc. Este hecho dificulta su gestión y obliga a un mantenimiento constante de las funciones de copiado, con el consiguiente riesgo de equivocaciones y olvidos involuntarios que esto supone.

Por otro lado, aunque se pudiera tener una primera impresión de que las copias totales incrementan en demasía el volumen de datos respaldados, es una percepción no del todo correcta si se tiene en cuenta el porcentaje que en el conjunto sistema/datos tiene en sistema. En la mayoría de los entornos actuales de trabajo el porcentaje que ocupa el sistema es significativamente menor que el de los datos, por lo que su carga en el global de la copia de respaldo (y más si tenemos en cuenta la utilización de copias incrementales) es lo suficientemente pequeña como para que la copia total sea la opción más segura y por tanto a tomar.

No obstante y para minimizar en la medida de lo posible ese aumento del volumen de los archivos de respaldo, es buena práctica la utilización de listas de exclusión, las cuales, además de disminuir el tamaño de la copia, despreciando los datos

copias incluirá, tal y como se verá en secciones posteriores, copias diferenciales, incrementales o de la modalidad que convenga en cada caso.

innecesarios, aligeran la carga de transferencia en caso de copias vía red y disminuyen el tiempo empleado, disminuyendo de esta manera el coste asociado a la operación. Algunos ejemplos de estas listas pueden ser:

- En servidores bajo Microsoft Windows. Exclude: *.tmp, *Archivos temporales de internet, ~*.*, *.mp3.
- En servidores _unix, Linux y Mac. Exclude: /tmp, /junk1, /junk2.

Las copias completas ofrecen absoluta automatización en el proceso de respaldo, además dela seguridad de que la totalidad del sistema podrá ser restaurada en caso de ser necesario.

7.2.4.2 PUESTOS DE TRABAJO

A medida que el volumen de datos producido en una organización aumenta, también lo hace el coste que supone el subsanar los errores producidos en ordenadores personales y portátiles. Por ese motivo, cada vez con mayor frecuencia las organizaciones aplican nuevas políticas en materia de almacenamiento de datos es sus dispositivos.

Debido a ello, la decisión a tomar en cuanto a qué tipo de copia realizar en este tipo de dispositivos depende en gran medida de las medidas en materia de seguridad de datos adoptadas por la organización. Es preciso realizar un estudio que permita alcanzar la decisión más acertada, para lo cual se tendrán que tener en cuenta algunas (De Guise, 2009, pág. 104).

En primer lugar será necesario conocer si la política de seguridad de la organización contempla la posibilidad de que los usuarios almacenen datos en sus ordenadores personales o portátiles. En caso afirmativo la realización de los respaldos se puede desarrollar mediante dos vías:

- Replicado automático de la información desde los equipos hacia un servidor central, del que se realizará la correspondiente copia de seguridad.
- La realización de la copia de seguridad de cada una de los ordenadores personales y portátiles, en cuyo caso se tendrán que tener en cuenta, entre otras, cada una de las siguientes consideraciones, que permitirán ajustar la política a seguir a cada situación particular:
    - ¿Es posible realizar la copia automáticamente sin la intervención del usuario?

- La copia en ningún momento debe interferir en la productividad del usuario, es decir, no debe impedirle continuar realizando su labor durante el proceso de la misma.
- ¿Las recuperaciones de datos deben ser iniciadas por el usuario?
- ¿Cómo se realizaran los respaldos y posibles revolcados de datos de los portátiles cuando no se encuentren en la oficina de la organización?
- Si normalmente los portátiles trabajan sin conexión a la red ¿Comenzarán la copia automáticamente al producirse la reconexión a la misma?
- Si se decide una política de copias de seguridad fuera de horas de trabajo, es necesario que todos los usuarios estén informados y concienciados de que no deben desconectar sus equipos al finalizar su jornada laboral.
- Como norma general, políticas de respaldo que contemplen la necesidad de que el usuario sea el que comience el proceso de copia, fracasarán.

En el presente escenario, la decisión acerca de si realizar copia de seguridad total o parcial de los datos, viene en gran medida supeditada a las políticas en materia de guardado de datos adoptadas por las organizaciones.

En los casos en los que dicha política impida el almacenamiento de datos en los dispositivos, puede ser una opción viable la realización de copias de seguridad parciales, asumiendo los costes que supone una reinstalación total del sistema en caso de desastre, ya que el grueso de los datos se encuentra en el servidor central, por lo que el volumen de datos a respaldar será en la mayoría de los casos mínimo (o incluso nulo).

Por el contrario, si la política de seguridad admite el almacenamiento de datos en sus equipos por parte de los usuarios, la opción más adecuada es, al igual que en el caso de los servidores y por las mismas razones, la realización de copias totales del sistema.

7.3 FRECUENCIA

7.3.1 INTRODUCCIÓN

Conjuntamente con los distintos modalidades de copias de seguridad (total, incremental, diferencial, etc.), de los que ya se ha hablado anteriormente, existen diversos niveles de profundidad de copia que se pueden aplicar a los mismos. Las denominaciones de dichos niveles varían ligeramente entre distintos autores, no obstante las denominaciones más utilizadas junto con su descripción sin las que a continuación se exponen:

- Nivel 0 / total: consistente en una copia total del sistema.
- Nivel 1: generalmente aplicado a copias incrementales que copian todos los datos que han cambiado o creado desde la última copia total (o de nivel 0).
- Niveles 2-9: en el caso de los niveles que abran desde el 2 al 9, cada una realiza una copia de todos aquellos datos que han experimentado cambios o han sido creados desde la última copia de menor nivel más cercana. Es decir, si se dispone de una programación de copias con la secuenciad e niveles 0, 3, 2, la copia de nivel 2 respaldará los datos que hayan sido modificados o creados desde la copia de respaldo de nivel 0.

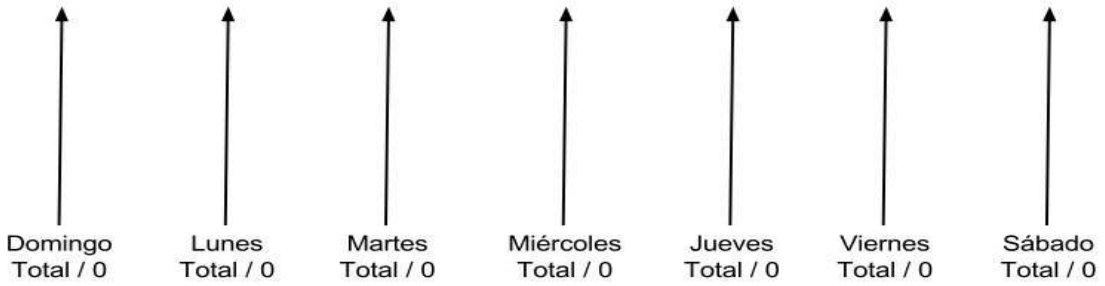
Una buena política de copias de seguridad implica la realización del respaldo diariamente, todos los días de la semana. La utilización de niveles de profundidad en las copias permiten ajustar la programación de las mismas a las necesidades, tanto funcionales como de costes, de cada situación en particular.

7.3.2 EJEMPLOS TIPO DE PROGRAMACIONES

Teniendo en cuenta las distintas modalidades de copias de seguridad y de los diferentes niveles de profundidad que se les puede aplicar, existen multitud de combinaciones que se pueden utilizar a la hora de realizar la programación de las copias.

A continuación se expondrán alguna de las más utilizadas[27] y funcionales, no obstante, como ya se ha comentado, se ha de tener en cuenta que la decisión acerca de cuál utilizar depende de cada caso en particular.

7.3.2.1 TIPO 1. PROGRAMACIÓN SEMANAL DE COPIAS TOTALES



En este caso la programación utilizada es de un solo nivel, en ella se realizan copias totales, o de nivel 0, cada día de la semana y en volúmenes distintos.

Este tipo de procedimiento ofrece una seguridad total pero a un alto precio, ya que además de que el volumen de la copia se incrementa diariamente, se emplean siete volúmenes distintos en donde almacenar cada una de las copias.

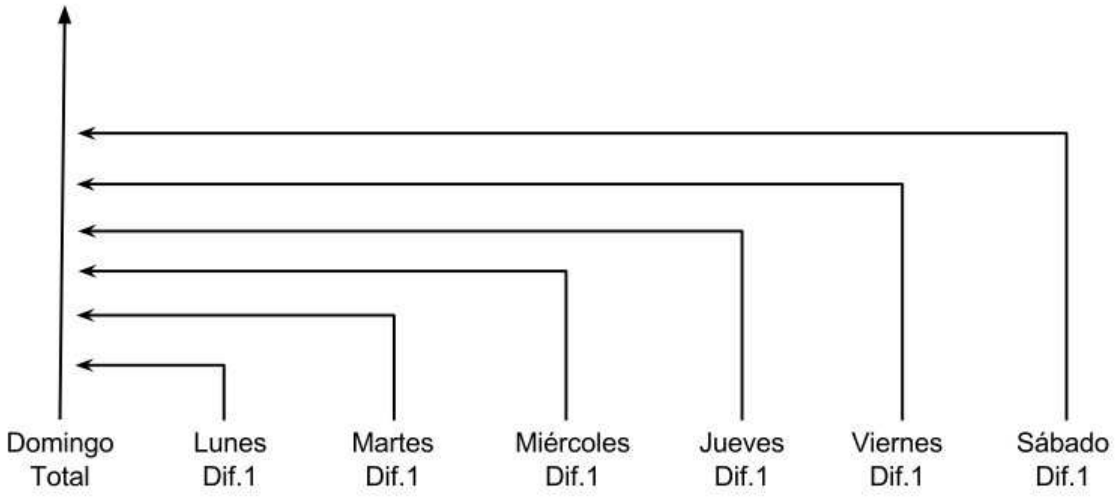
Únicamente está recomendado para sistemas de un tamaño medio – grande. Actualmente este tipo de programación no es realmente necesario debido las aplicaciones comerciales de respaldo de datos que existen.

Tabla 1. Programación semanal con copias totales.

Día	Domingo	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado
Nivel	Total/0	Total/0	Total/0	Total/0	Total/0	Total/0	Total/0

[27] Se utilizará la notación con semana inglesa, la cual comienza en domingo.

7.3.2.2 TIPO 2. COPIA TOTAL SEMANAL CON COPIAS DIFERENCIALES DE NIVEL 1



Se realiza una copia total, de nivel 0, a principios de semana, y cada uno de los restantes días se realizan copias de seguridad diferenciales de nivel 1 todas ellas. De esta manera únicamente se necesitan dos volúmenes a la hora de efectuar la restauración: el correspondiente a la copia total semanal y el correspondiente a la última copia diferencial viable, ya que como se ha comentado anteriormente, las copias de nivel 1 guardan todos los datos modificados o creados desde la última copia total.

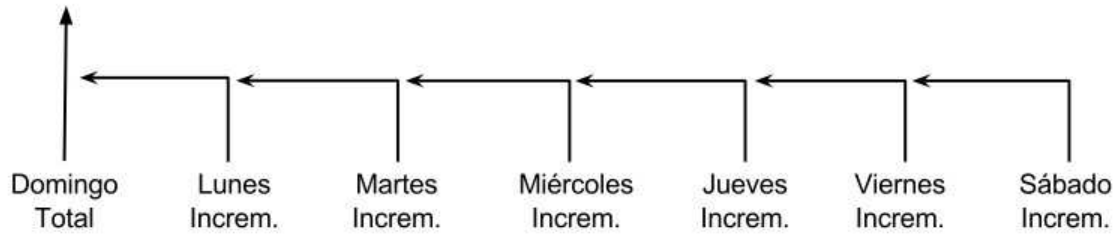
Este método está especialmente indicado si no se utilizan aplicaciones que gestionen los volúmenes, ya que sólo se utilizan dos.

Tiene fundamentalmente dos ventajas, la primera se debe a la utilización de dos volúmenes ya que facilita la labor de reconstrucción total de datos, y la segunda radica en el hecho de que en todo momento se tienen copias múltiples de los archivos que han cambiado a lo largo de la semana, facilitando así la reconstrucción de datos parciales.

Tabla 2. Copia total semanal con copias diferenciales de nivel 1.

Día	Domingo	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado
Nivel	Total/0	Difer./1	Difer./1	Difer./1	Difer./1	Difer./1	Difer./1

7.3.2.3 TIPO 3. COPIA TOTAL SEMANAL CON COPIAS INCREMENTALES



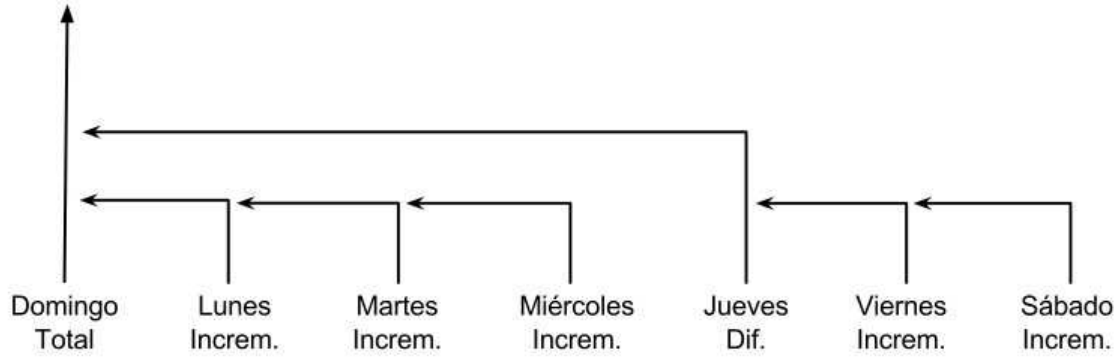
En este caso se realiza una copia total el primer día de la semana y en los seis días restantes, copias incrementales, cada una de las cuales respalda los datos cambiados o creados desde la copia incremental más próxima o en su defecto, desde la última total.

Tiene la ventaja de que el proceso de copia incremental diario es, normalmente, rápido, pero se corre el riesgo de que al estar las copias secuenciadas, si se produce una corrupción de datos en algún eslabón de la cadena, se pueden perder varios días de datos. Otro inconveniente que conviene tener en cuenta a la hora de decidirse por este tipo de programación es que el tiempo de restauración en caso de desastre es lento, ya que se ha de partir de la última copia total del sistema y seguidamente ir restaurando secuencialmente cada una de las copias diarias, por otro lado, y como contrapartida, las restauraciones parciales de datos son rápidas.

Tabla 3. Copia total semanal con copias incrementales diarias.

Día	Domingo	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado
Nivel	Total	Increm.	Increm.	Increm.	Increm.	Increm.	Increm.

7.3.2.4 TIPO 4. COPIA TOTAL, DIFERENCIAL E INCREMENTALES



La programación de las copias de seguridad en este caso utiliza los tres modelos de copias de seguridad más utilizados: total, incremental y diferencial.

El primer día de la semana se realiza una copia total del sistema seguidos de tres días de copias incrementales. El jueves se efectúa una copia diferencial que guarda todos los datos cambiados o creados desde la última copia total, es decir, desde el domingo. Finalmente se realizan copias incrementales el viernes y el sábado que respaldan los datos cambiados o creados el jueves y el viernes respectivamente.

Con esta programación se consigue distribuir el volumen de datos a restaurar en caso de desastre, en la siguiente tabla se puede observar los archivos de respaldo necesarios dependiendo del día de la semana en el que se produzca la restauración.

Día	Respaldo necesario
Domingo	Total + Diferencial + Incremental Viernes + Incremental Sábado.
Lunes	Total
Martes	Total + Incremental Lunes.
Miércoles	Total + Incremental Lunes + Incremental Martes.
Jueves	Total + Incremental Lunes + Incremental Martes + Incremental Miércoles
Viernes	Total + Diferencial.
Sábado	Total + Diferencial + Incremental Viernes

Tabla 4. Copia total, diferencial e incrementales.

Día	Domingo	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado
Nivel	Total	Increm.	Increm.	Increm.	Dif.	Increm.	Increm.

7.3.2.5 TIPO 5. COPIAS MULTINIVEL. TORRE DE HANÓI

Si el software utilizado para la creación de las copias de seguridad es capaz de gestionar múltiples volúmenes y niveles de forma adecuada, una de las programaciones más interesantes y que consumen menos tiempo y recursos, consiste en la utilización de copias de seguridad multinivel, y más especialmente la configuración denominada Torre de Hanói.

La programación en torre de Hanói, tiene su base en un juego de lógica ideado en 1883 por el matemático francés Édouard Lucas (1842 – 1891). El juego consiste en tres varillas verticales. En una de ellas se han apilado un número indeterminado de discos de madera de distinto diámetro de manera que forman una torre piramidal escalonada, situándose el disco con el diámetro más alto en la base y el de menor diámetro en la cúspide. El fin del juego consiste en mover la torre de discos de una varilla a otra siguiendo ciertas reglas:

- Sólo se puede mover un disco a la vez.
- Un disco no puede descansar sobre otro de menor diámetro que él.
- Sólo se puede desplazar el disco que se encuentra en la posición más elevada de cada varilla.

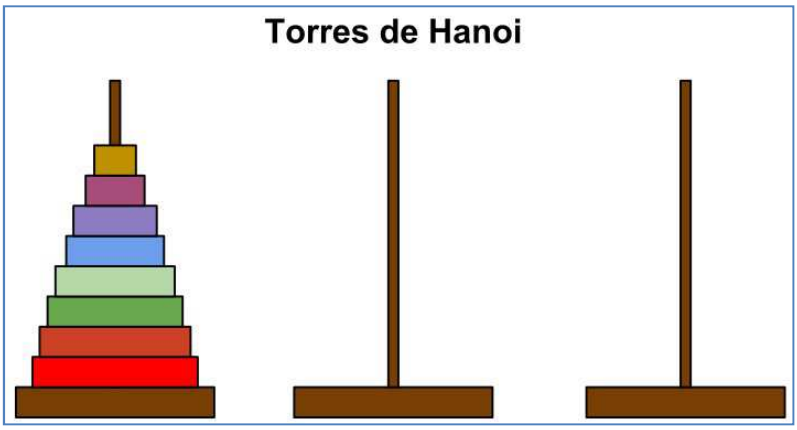


Ilustración 29. El juego de las torres de Hanói.

La solución pasa por mover el primer anillo cada dos movimientos (1, 3, 5, 7,…), el segundo anillo cada cuatro movimientos (2, 6, 10,…), el tercero cada ocho movimientos (4, 12,…) y de esta manera sucesivamente. Por ejemplo con un juego en el que se tienen 5 anillos, etiquetados A, B, C, D y E, la solución total sería la que refleja la siguiente tabla de movimientos.

Tabla 5. Solución al problema de las torres de Hanói con cinco niveles.

Anillo	Movimiento																														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	A		A		A		A		A		A		A		A		A		A		A		A		A		A		A		A
2		B				B				B				B				B				B				B				B	
3				C								A								C								C			
4								D																D							
5																E															

En la programación de las copias de seguridad mediante la progresión de las torres de Hanói, se basa en el mismo patrón, pero operando con sesiones en lugar de movimiento de anillos y niveles de copia en lugar de anillos.

Utilizando una torre de Hanói de cinco niveles de copia, se puede conseguir una programación que abarque 16 sesiones de copias, tal y como se muestra en la siguiente tabla, en la que los volúmenes están etiquetados con las letras A, B, C, D y E.

Nivel	Sesión															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	A		A		A		A		A		A		A		A	
2		B				B				B				B		
3				C								C				
4								D								
5																E

El objetivo final consiste en mantener una copia de todos los datos que hayan cambiado o creado en más de un volumen, mientras al mismo tiempo se reduce sensiblemente el volumen total de datos utilizado, permitiendo la recuperación de datos e copias de seguridad que tienen uno, dos, cuatro, ocho y dieciséis días de antigüedad (según el patrón anterior).

Se trata de una estrategia que, por su complejidad, requiere para su implementación la utilización de software especializado en copias de seguridad que las gestione adecuadamente en diferentes niveles de profundidad.

Está especialmente indicada para pequeñas empresas en las que el factor costes sea determinante (como se ha visto son más económicas en cuanto al uso de recursos) y sin embargo necesiten poder realizar, en caso de necesidad, restauraciones completas de sus sistemas de datos.

7.4 PROTECCIÓN DE LAS COPIAS DE SEGURIDAD

7.4.1 INTRODUCCIÓN

La planificación de la política de copias de seguridad no finaliza con la toma de decisiones acerca de qué datos copiar y cómo copiarlos, sino que va más allá. También es necesario planificar otros aspecto, que no siendo tan obvios resultan fundamentales a la hora de conseguir una estrategia de copias segura y eficiente. Entre esos aspectos añadidos se encuentran el aislamiento y protección de los volúmenes de datos de respaldo que diariamente se van generando en el proceso de copia.

La mejor política de copias de seguridad puede resultar totalmente ineficaz si las copias de respaldo sufren daños de cualquier tipo, por esa razón es altamente aconsejable separar físicamente volúmenes representativos de las copias de respaldo fuera del lugar en el que se generan, evitando de esta manera la posibilidad de que sean destruidas en caso de desastre o borradas, ya sea accidentalmente o de una forma malintencionada.

En el mismo sentido de salvaguardar la integridad de las copias, se debe también que tener en cuenta la posible pérdida, robo o acceso no autorizado a las mismas, por lo que cobra importancia, no solo la protección de los volúmenes de respaldo en sí, sino la de la privacidad de los datos que contienen, que se puede garantizar mediante su encriptación o codificación.

Teniendo en cuenta lo expuesto en los párrafos anteriores, se puede deducir que la protección de las copias de seguridad pasa por abordar la cuestión en tres fases distintas: duplicación de las copias, su almacenamiento y su protección.

7.4.2 DUPLICACIÓN DE COPIAS DE SEGURIDAD

El término duplicación, o clonación, de copias de seguridad se aplica a la generación de un grupo de copias duplicadas que servirán como fuente de recuperación en el caso de que las originales hayan sufrido algún tipo de desperfecto que provoque que no se encuentren operativas. Se trata de una tarea fundamental si lo que se persigue es la certeza de una recuperación total en caso de desastre.

Se puede llevar a cabo de dos maneras dependiendo del momento en el que se realice: duplicación posterior al proceso de copia de seguridad (post-copia) o duplicación simultánea, en el momento en el que se realiza la copia.

7.4.2.1 DUPLICACIÓN POST-COPIA

La duplicación post-copia de copias de seguridad consiste en la realización del duplicado del volumen de respaldo una vez se hayan finalizado todos los procesos de respaldo que se tienen programados para dicho volumen. Normalmente se puede realizar de dos maneras distintas: duplicación de medios o duplicación de la copias de seguridad.

La duplicación de medios consiste simplemente en la creación de una copia de medio a medio (cinta - cinta, cd - cd, dvd - dvd, etc.) del volumen generado en el proceso de respaldo.

Tiene el inconveniente de que la duplicación, para que se lleve a cabo de una manera satisfactoria, ha de realizarse entre tipos de medios exactamente iguales, la más mínima diferencia entre ellos puede originar que falle el proceso de copia.

Como contrapartida, el proceso de copia es sensiblemente más rápido que el efectuado de manera simultánea, del que se hablará en el siguiente apartado.

Por otro lado la duplicación de respaldos consiste en la realización de copias de seguridad de los archivos de respaldo una vez que se ha finalizado el proceso de copia original. Tienen como inconveniente el ser más lentas ya que se ha de esperar la finalización de la primera copia.

7.4.2.2 DUPLICACIÓN EN LÍNEA

El término duplicación en línea hace referencia a la generación de una imagen de copia de seguridad y a su duplicado, realizándose en el mismo periodo de tiempo.

Por norma general, este proceso implica que el servidor de copias de seguridad ha de escribir en dos, o más, dispositivos contenedores de copias de una manera simultánea.

Aunque en teoría se trata de un buen método, tiene como inconvenientes una serie de aspectos:

- Las copias en línea no serán más rápidas a la hora de recuperar sus datos que las originales.
- Existen varias restricciones relativas a la mezcla de medios.
- La verificación de los datos no se produce de manera automática como parte del proceso de copia simultánea. La razón es que en este tipo de copia no existe los conceptos de fuente o destino entre las múltiples copias. Por esa razón será necesaria alguna técnica posterior de verificación de datos.

7.4.3 ALMACENAMIENTO DE VOLÚMENES

Una vez se ha solucionado la cuestión de la clonación de las copias de seguridad, se debe abordar el tema de dónde y bajo qué condiciones ubicarlas.

El procedimiento más seguro consiste en el mantenimiento de una de las copias on-site, esto es, en el mismo sitio de generación, y la otra copia off-site, en una ubicación distinta del lugar de generación. Esta doble ubicación salvaguardará el proceso de restauración del sistema en caso de desastre, por lo que es importante tomar las decisiones adecuadas tanto en cuanto a la modalidad de almacenamiento, como, en caso necesario, la elección correcta de la empresa que lo efectuará.

7.4.3.1 ALMACENAMIENTO ON-SITE

Como ya se ha comentado, el almacenamiento on-site consiste en el guardado de los volúmenes de respaldo en el mismo lugar en el que se generan los datos. En este punto es necesario comentar que si bien parecería innecesaria la clonación de los datos, anteriormente comentada, debido a que serán almacenados en el mismo lugar que los originales, cabe decir que por motivos de seguridad ante posibles fallos, siempre es aconsejable dicha clonación.

La mejor opción en cuanto a almacenamiento de volúmenes de respaldo pasa por la utilización de dispositivos robotizados, tales como librerías de cintas o máquinas de discos, de los cuales ya se ha hablado anteriormente.

Sin embargo, si esta opción no fuera posible se deberá almacenar el material de respaldo teniendo en cuenta unas mínimas consideraciones en cuanto a la seguridad tanto física como lógica del mismo. Cuestiones como un almacenamiento aislado y privado, estrategias de seguimiento y encriptación de los datos son fundamentales para salvaguardar la seguridad de los datos almacenados.

7.4.3.1.1 Seguridad Física

En orden de garantizar la seguridad física de los volúmenes de copias de seguridad, es aconsejable que sean almacenados en contenedores de seguridad o estancias habilitados a tal efecto, aislados en la medida de lo posible tanto de los agentes

externos que pudieran dañarlas (ignífugos, sellados, aislados térmicamente[28] y con control ambiental independiente).

Así mismo se debe mantener una política de seguridad de acceso acorde a las características del material almacenado. Actualmente la capacidad de los dispositivos de almacenamiento externo posibilita que una única copia de seguridad contenga toda la información relevante de una organización. Esa, a priori, ventaja se convierte en catastrófica en el caso de robos o accesos no autorizados los volúmenes de respaldo, por lo que es imperativo impedir dicha situación.

7.4.3.1.2 Seguimiento

Así mismo es fundamental el etiquetado de cada uno de los volúmenes almacenados de manera única, por ejemplo mediante la utilización de códigos de barras u otro tipo de sistema válido para tal labor, así como un mantenimiento de un inventario actualizado de todos ellos. Un método funcional que ayuda a mantener el control a cerca del continuo trasiego de volúmenes de respaldo consiste en almacenar toda la información al respecto en una base de datos diseñada, en la que se almacenará como mínimo la siguiente información para cada volumen:

- Número.
- Nombre.
- Propósito.
- Tipo de datos almacenados.
- Fecha de inicio de uso.
- Fecha de último uso.
- Ubicación de almacenamiento.

Además de los datos indicados, la base de datos deberá permitir mantener un seguimiento de los volúmenes de almacenamiento, más concretamente, deberá permitir entre otras funcionalidades:

- Saber dónde se encuentra un determinado volumen en un momento dado.
- Realización de informes de inventario.

[28] Es un error común pensar que una caja ignífuga protege completamente, la integridad de las copias de respaldo. En caso de fuego prolongado, si bien este no alcanza al material de copia, la alta temperatura generada puede llegar a dañarlo. De ahí un la necesidad de un buen sistema de aislamiento térmico.

- Determinación de en cuántas ocasiones ha sido utilizado un volumen determinado.
- Actualización automática de la base de datos mediante códigos de barras (en caso de utilizarlos).
- Generación de códigos de barras (en caso de utilizarlos).

El almacenamiento on-site ofrece la ventaja de la inmediatez y de la disminución de costes asociados, sin embargo como y contrapartida, no ofrece seguridad total ya que la coincidencia de ubicación de las copias y sus clones hace que, en caso de producirse algún tipo de desastre en al lugar de almacenamiento, se puedan llegar a perder ambas, imposibilitando de esta manera cualquier oportunidad de reinstalación del sistema. Una posible solución a esta eventualidad consistiría en el almacenamiento en distintos contenedores de las copias, por ejemplo en distintas plantas del edificio, disminuyendo así en parte el riesgo de pérdida.

7.4.3.2 ALMACENAMIENTO OFF-SITE

El almacenamiento off-site, del que ya se ha hablado en anteriores secciones de ente trabajo, consiste en el envío y almacenamiento de las copias de seguridad de los datos fuera del lugar de generación de los mismos.

Este tipo de almacenamiento elimina el riesgo de pérdida de datos por desastre acaecido en el lugar de origen, permitiendo, siempre que los datos respaldados lo permitan, una completa restauración del sistema en caso de necesidad.

En este punto es importante señalar que si los datos que son objeto de respaldo y contenidos en las copias de seguridad, contienen datos de carácter personal, hay que tener muy en cuenta la normativa legal vigente al respecto. La sección 3 del artículo 3 del Real decreto 994/1999, del 11 de Junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (Ley de Protección de Datos de Carácter personal, o LOPD), indica la operativa a aplicar en el caso de copias de seguridad que respalden datos clasificados como de nivel alto[29] especificando que "*deberá conservarse una copia de respaldo y de los procedimientos de recuperación de datos en un lugar diferente de aquel en que se encuentran los equipos informáticos que los tratan cumpliendo en todo caso las*

[29] El Real decreto 994/1999, del 11 de Junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal define como datos personales de nivel alto "los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.

medidas de seguridad exigidas en este Reglamento" (se puede encontrar un extracto de la ley mencionada en el anexo I del presente documento). Atendiendo a esta normativa, la posible elección en cuanto al tipo de almacenamiento (on-site u off-site) desaparece, siendo obligado su almacenamiento fuera del lugar de origen.

Existen básicamente dos modalidades de almacenamiento off-site: el almacenamiento físico de los volúmenes de respaldo y el almacenamiento electrónico de los datos que los forman.

7.4.3.2.1 Almacenamiento físico

En el almacenamiento off-site físico de los volúmenes de respaldo, son los originales de los dispositivos de copia (cintas o discos principalmente) los que deben ser separados físicamente de su lugar de origen. La razón de porque es preferible la separación de las copias originales y no de sus clones descansa en el hecho de que las copias separadas son utilizadas únicamente cuando las que se mantienen en la ubicación de origen fallan. Al utilizar en las sesiones de restauración de datos ordinarias los clones de las copias, se está verificando constantemente todo el proceso de creación de respaldos, ya que las unidades utilizadas son copia exacta del original, por lo que su correcta operatividad implica, por norma general la operatividad de este, no obstante, y para mayor seguridad, es aconsejable incluir a los clones en las tareas periódicas de pruebas de operatividad.

Si se ha decidido utilizar este tipo de almacenamiento se dispone básicamente de dos métodos para realizarlo. El primero consiste en la contratación de una de las numerosas empresas dedicadas a estas labores que existen en el mercado y el otro en la utilización, si ello es posible, de instalaciones de la propia organización situadas en una ubicación distinta al origen de los datos (preferiblemente otro edificio situado a una distancia suficientemente segura que minimice los riesgos en caso de, por ejemplo, desastre natural tales como inundaciones, incendios, actos terroristas, etc).

Al decidirse por la contratación de una empresa que almacene las copias de seguridad, conviene tener en cuenta una serie de servicios que como mínimo debería ofrecer y cuyo incumplimiento debe ser razón suficiente para la no elección del candidato:

- **Almacenamiento individual de cada unidad**: la empresa debe responsabilizarse individualmente de cada volumen de copia suministrada, almacenando cada uno de ellos por separado y posibilitando su seguimiento pormenorizado.

  Conviene, en la medida de lo posible, prescindir de empresas que se responsabilicen únicamente del almacenamiento en bloque de todos los volúmenes de copias, almacenándolos todos en el mismo contenedor y delegando en la empresa contratante la tarea de seguimiento de los mismos.

- **Identificación de cada volumen por medio de códigos de barras**: una práctica correcta por parte de la empresa contratada consiste en el escaneo de cada unidad suministrada cada vez que se produce un cambio de ubicación de la misma e imperativamente en el momento de la entrega y en el de la devolución a la empresa contratante.

- **Doble comprobación de los códigos de barras**: es aconsejable que el etiquetaje mediante códigos de barra de los volúmenes almacenados, pueda ser cotejado tanto por la empresa contratada como por la contratante. Para ello la empresa de almacenamiento ha de ser capaz de suministrar a la contratante el software apropiado para tal efecto.

  Con esta opción será posible el doble seguimiento de los volúmenes posibilitando el cotejo de información entre las dos empresas y facilitando de ésta manera la solución de los posibles problemas que pudieran surgir en caso de información errónea por alguna de las partes.

- **Garantía de seguridad**: si bien es un aspecto que se supone, es conveniente que la empresa contratada garantice por escrito la seguridad física de las copias suministradas. Comprometiéndose a almacenarlas en instalaciones especialmente diseñadas a tal efecto, en las que sean protegidas no solo de los factores ambientales sino, además, de otros como el robo o el acceso no autorizado.

7.4.3.2.2 Almacenamiento electrónico

En el proceso de almacenamiento electrónico, las copias de seguridad son enviadas directamente a los sistemas de almacenamiento de la empresa contratada.

Si bien todas las empresas de almacenamiento remoto de datos ofrecen un servicio similar en cuanto a funcionalidad de almacenamiento, difieren entre si sensiblemente en cuanto a opciones de accesibilidad soportada, utilidades y soporte, diferencias que hacen que el coste del servicio varíe.

A la hora de contratar un servicio de almacenamiento electrónico, se han de tener en cuenta ciertas características que debe ofrecer y que decidirán la elección final.

7.4.3.2.2.1 Espacio de almacenamiento

Una de las principales características que se han de tener en cuenta a la hora de elegir un proveedor de almacenamiento de datos remoto, es la capacidad de almacenamiento.

Existen numerosos modelos ofertados por las empresas de almacenamiento de datos, determinados proveedores ofrecen almacenamiento ilimitado a cambio del pago de cuotas fijas, otros por el contrario basan su modelo de negocio en ofertar almacenamientos de tamaño fijo con la posibilidad de ser aumentados a medida que se produce la necesidad.

En este aspecto concreto, la elección del tipo de proveedor dependerá en cada caso tanto de las necesidades de operatividad como de las posibilidades económicas.

7.4.3.2.2.2 Características

Otro punto a tener en cuenta es la capacidad de ofrecer determinados servicios que faciliten el proceso de almacenamiento.

- Sistemas que permitan el compartir carpetas remotas de manera sencilla.
- Sistemas que faciliten el proceso de subida de los datos y que utilicen procesos que eviten la saturación del ancho de banda.
- Sistemas de sincronización off-line funcionales.
- Sistemas de control de versiones de archivos.

7.4.3.2.2.3 Acceso a los datos y soporte

El proveedor de almacenamiento online debería permitir almacenar todo tipo de archivos, independientemente del formato de los mismos. De la misma manera debería ofrecer accesibilidad total a dichos archivos. Este hecho se traduce en que deberá ser capaz de permitir subir y acceder a los datos desde cualquier tipo de dispositivo, incluyendo ordenadores personales, servidores e incluso portátiles o dispositivos móviles.

7.4.3.2.2.4 Ayuda y soporte

Un último punto a considerar consiste en que el proveedor de servicios de almacenamiento remoto deberá ofrecer un buen servicio de asistencia remota en caso de necesidad, además de todos los manuales de referencia necesarios para solucionar los problemas que se pudieran originar en el proceso.

Es un error pensar que por el hecho de utilizar los servicios de un proveedor de almacenamiento remoto, el sistema se encuentra completamente respaldado en caso de desastre.

Para que se tenga seguridad total al respecto se ha tener por seguro que la empresa contratada no centraliza sus datos en una única ubicación, y que a su vez cuenta con las correspondientes medidas de seguridad que garantizan la recuperación de los datos en caso de desastre en sus propias instalaciones.

7.4.4 ENCRIPTACIÓN O CIFRADO

7.4.4.1 INTRODUCCIÓN

Puede definirse formalmente un sistema de cifrado como una quíntupla (M, C, K, E, D), donde:

- M representa el conjunto de todos los mensajes sin cifrar (lo que se denomina texto claro, o *plaintext*) que pueden ser enviados.
- C representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- K representa el conjunto de claves que se pueden emplear en el sistema de cifrado.
- E es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de M para obtener un elemento de C. Existe una transformación diferente Ek para cada valor posible de la clave k.
- D es el conjunto de transformaciones de descifrado, análogo a E.

Todo sistema de cifrado ha de cumplir la siguiente condición: ***Dk(Ek(m)) = m***, es decir, teniendo un mensaje *m*, si dicho mensaje es cifrado empleando la clave *k*, al descifrarlo empleando la misma clave, se obtiene de nuevo el mensaje original *m*.

Todo proceso de cifrado o encriptación tiene su base en un Algoritmo, que tiene como función básica codificar la información para que no pueda ser reconocida y por tanto leída de manera normal. El algoritmo utiliza las claves de encriptación de manera que la información únicamente se podrá descifrar, esto es, retornar a su estado natural aplicando dicha clave. Principalmente existen tres tipos de algoritmos: DES (simétrico), AES y RSA (asimétrico).

7.4.4.2 TIPOS DE SISTEMAS DE CIFRADO

Existen dos tipos fundamentales de sistemas de cifrado:

- **Sistemas de cifrado simétricos o de clave privada:** este tipo de sistema de cifrado se caracteriza por la utilización de la misma clave **k** tanto para el cifrado como para su posterior descifrado. Tienen el inconveniente de que, para ser empleados en comunicaciones, la clave k debe estar en posesión tanto en el emisor como en el receptor, lo cual genera el problema de la transmisión entre los dos de la clave de una manera segura.

- **Sistemas de cifrado asimétricos o de clave pública:** en este caso el sistema de cifrado emplea una doble clave (**kp, kP**). **kp** se la conoce como clave privada y **kP** se la conoce como clave pública. Una de ellas sirve para la transformación o función **E** de cifrado y la otra para la transformación **D** de descifrado. En muchos casos son intercambiables, esto es, si se emplea una para cifrar la otra sirve para descifrar y viceversa.

  Estos sistemas de cifrado deben cumplir además que el conocimiento de la clave pública kP no permita calcular la clave privada kp. Ofrecen un abanico superior de posibilidades, pudiendo emplearse para establecer comunicaciones seguras por canales inseguros puesto que únicamente viaja por el canal la clave pública, que sólo sirve para cifrar, o para llevar a cabo autenticaciones. Sin la clave privada (que no es deducible a partir de la clave pública) un observador no autorizado del canal de comunicación será incapaz de descifrar el mensaje cifrado.

En la práctica se emplea una combinación de estos dos tipos de sistemas de cifrado, puesto que los asimétricos presentan el inconveniente de ser computacionalmente mucho más costosos que los primeros. En el mundo real se hace uso de la criptografía asimétrica para codificar las claves simétricas y poder así enviarlas a los participantes en la comunicación incluso a través de canales inseguros. Después se codificarán los mensajes (más largos) intercambiados en la comunicación mediante algoritmos simétricos, que suelen ser más eficientes.

7.4.4.3 TIPOS DE ALGORITMOS DE CIFRADO

7.4.4.3.1 DES. Estándar de cifrado de datos

El algoritmo DES (Data Encryption Standard), tiene sus origen a principio de los años 1970. En 1973 la agencia nacional de normalización de EEUU, hoy día denominada Instituto Nacional de Normalización y Tecnología, solicitó, mediante el Registro Federal[30], la creación de un algoritmo cifrado que se convirtiera en estándar gubernamental para el cifrado de información confidencial.

[30] El Registro Federal de EEUU es el equivalente al Boletín Oficial del Estado de España.

Tras un segundo llamamiento en Agosto de 1974, IBM presentó un candidato que fue considerado aceptable. Se trataba del algoritmo Lucifer, que había estado desarrollándose desde 1971, en el que desde un principio colaboró en su desarrollo la Agencia Nacional de Seguridad de EEUU (NSA). La NSA, encargada del espionaje y monitorización de las comunicaciones en todo el mundo, preocupada por la aparición en el mercado de un sistema de cifrado de difícil ruptura, negoció con IBM la disminución de la clave del algoritmo, que paso de sus 128 bits iniciales a 56 bits, además de clasificar como secretos determinados detalles de la selección de las fórmulas que realizaban las transformaciones.

El DES fue aprobado por la agencia nacional de normalización (NBS) en 1978 y estandarizado por el Instituto Nacional Americano de Estándares (ANSI) bajo el nombre de *ANSIx3.92*, más conocido como *DEA* (Data Encryption Algorithm).

Como ya se ha comentado, el nombre original del algoritmo, tal como lo denominó IBM, era Lucifer, y trabajaba sobre bloques de 128 bits, teniendo la clave igual longitud. Se basaba en operaciones lógicas booleanas y podía ser implementado fácilmente, tanto en software como en hardware.

7.4.4.3.2 AES. Rijndael

El algoritmo AES (Advanced Encryption Standard), o Estándar Avanzado de Encriptado, fue desarrollado por los belgas *Joan Daemen* y *Vincent Rijmen*.

En enero de 1997, el Instituto de Estándares y Tecnología de EEUU (NIST), anunció una iniciativa para desarrollar un nuevo modelo de estándar de codificación, el AES. La intención de dicha iniciativa no era otra que sustituir al anterior DES, y convertirse en un proceso estándar de encriptación federal (FIPS). Se trató de un concurso abierto en el que todas las propuestas fueron evaluadas y, para ello, el NIST solicitó la ayuda de toda la comunidad dedicada al mundo de la criptografía para que intentaran descifrar todas las propuestas candidatas.

El proceso de selección culminó con la victoria de los belgas *Joan Daemen* y *Vincent Rijmen* y su algoritmo ***Rijndael***, que fue aprobado como un estándar gubernamental, lo que le confirió un certificado de calidad oficial. El algoritmo ***Rijndael*** está reconocido por ISO, IETF (Internet Engineering Task Force) e IEEE (Institute of Electrical and Electronics Engineers). El factor más determinante que ha posibilitado la rápida aceptación del algoritmo de ***Rijndael*** consiste en que no tiene derechos de autor y puede ser implementado de una manera fácil en multitud de plataformas sin reducir el ancho de banda de manera significativa (Daemen & Rijmen, 2002).

7.4.4.3.3 RSA

El algoritmo RSA (Rivest, Shamir y Adleman) es un sistema de cifrado de clave pública desarrollado en 1977 por Ronald Rivest, Adi Shamir y Leonard Adleman y ha estado bajo patente de los Laboratorios RSA hasta Septiembre de 2000. Una peculiaridad que hace único a este algoritmo es que sus dos claves sirven indistintamente tanto para cifrar como para autenticar.

Este tipo de algoritmo denominados asimétricos por norma general utilizan longitudes de clave mucho mayores que los simétricos, que usan una única clave secreta. Por ejemplo, mientras que para algoritmos simétricos se considera segura una clave de 128 bits, para la mayoría de algoritmos asimétricos (incluido el del RSA), se recomiendan actualmente claves de al menos 1024 bits de longitud. Además, la complejidad de cálculo que comportan los algoritmos de los sistemas de cifrado asimétricos los hace considerablemente más lentos que los algoritmos de cifrado simétricos. Por eso en la práctica los métodos asimétricos se emplean principalmente para codificar la clave de sesión (simétrica) de cada comunicación o transacción particular.

La criptografía basada en sistemas de cifrado de clave pública es relativamente reciente, pues los primeros algoritmos asimétricos aparecen después de 1975. El sistema de cifrado de esta clase más importante y extendido hoy en día es el RSA, que utiliza la exponenciación modular para cifrar y descifrar y basa su seguridad en la complejidad del problema de la factorización de enteros grandes.

7.4.4.4 CIFRADO Y COPIAS DE SEGURIDAD

La encriptación de las copias salvaguarda, en la medida de lo posible, la confidencialidad de los datos en el caso de que las procedimientos de seguridad adoptados no hayan impedido el robo o el acceso no autorizado a los volúmenes de respaldo, más aun teniendo en cuenta la legalidad vigente en cuanto a las medidas de seguridad a adoptar en caso de datos de carácter personal, las cuales incluyen por ejemplo la adopción de las medidas necesarias para impedir cualquier recuperación indebida de datos en el caso de que los soportes que los albergan fueran a salir de los locales en donde se encuentran ubicados los ficheros.

Estas premisas hacen de la encriptación de los datos un procedimiento por un lado indispensable en el caso de los volúmenes de copias que abandonen la ubicación de origen y altamente aconsejable en el resto (en el caso de copias almacenadas on-site, el hecho de que se encuentren encriptadas hace que, dependiendo de la sofisticación

de la encriptación, disminuya en más o menos medida las consecuencias negativas que puede originar un acceso no autorizado o incluso robo de las mismas).

Si se ha optado por el almacenamiento off-site electrónico, el proceso de cifrado generalmente lo realiza automáticamente el software cliente encargado de procesar la información, comprimirla y enviarla a su destino de almacenamiento.

7.5 PRUEBAS DE OPERATIVIDAD (TESTING)

7.5.1 INTRODUCCIÓN

El diseño de una correcta y sofisticada política de copias de seguridad no garantiza totalmente que se pueda recuperar el sistema en caso de desastre. En numerosas ocasiones la recuperación se hace inviable debido a que los volúmenes de respaldo utilizados para tal fin se encuentran inoperativos y no es posible su utilización. La única manera de tener completa seguridad de que un sistema podrá recuperarse mediante sus copias de seguridad es mediante la realización periódica de pruebas de operatividad, o testing, de las mismas.

Los procedimientos de testing son un paso que en demasiadas veces se pasa por alto en los procesos de gestión de copias de respaldo. Organizaciones que invierten tiempo, recursos y esfuerzo en asegurarse de tener copias de todos sus datos, se encuentran con que no pueden utilizarlos debido a algún fallo en el proceso de almacenamiento (Cook, 2008).

Según el informe de investigación sobre recuperación de desastres de *Symantec* (Symantec, 2007), el 48% de los test de recuperación, efectuados por compañías en el transcurso de pruebas de sus planes de recuperación ante desastres, fracasaron, y un amplio porcentaje de esos fracasos fueron originados por la utilización en la recuperación de copias de seguridad en mal estado.

Las copias de seguridad, por tanto, deben ser probadas periódicamente. Dichas pruebas no deben únicamente ceñirse al hecho de una comprobación de una lectura correcta de los datos que contienen[31], sino que deben incluir procedimientos que verifiquen la recuperación de archivos, aplicaciones o sistemas operativos y confirmen que la información recuperada es plenamente operativa, esto es, que su integridad no se ha visto comprometida.

Existen dos reglas básicas que aplicar a la hora de efectuar una prueba de recuperación:

- Realizar de las pruebas aleatoriamente. Es importante realizar las pruebas en diferentes momentos del día, bajo distintas circunstancias y con diferentes datos, esto reducirá el riesgo de falta de detección de problemas que se pueden producir a horas determinadas y el segundo.

[31] Es un error bastante común asumir que el hecho de que se pueda leer el contenido de un volumen de respaldo signifique sin género de dudas de que sea recuperable.

- No permitir bajo ningún concepto que las pruebas que se realicen pongan en peligro los datos sobre los que se está realizando el test.

7.5.2 PAUTAS

Como en todos los aspectos que afectan al diseño de la política de copias de seguridad, cada caso en distinto y tiene sus propias características y necesidades, sin embargo en el ámbito de la realización de las pruebas de recuperación, es conveniente seguir una serie de pautas que son aplicables a cualquier tipo de situación y que, en la medida en que se sigan, ayudarán a conseguir procedimientos:

- **Realizar las pruebas de manera realista**: en la medida de lo posible las pruebas deben reproducir las condiciones que se darían en caso de ser necesario una restauración del sistema o parte de él.

  Si es posible, se deberían probar en el mismo hardware en el que se realizará la restauración. Esta condición se debe al hecho de que determinadas aplicaciones de respaldo de datos se vinculan en demasía al hardware en el que se ejecutan, presentando posteriormente problemas al intentar volcar los datos en una máquina diferente.

- **Realizar pruebas de todo**: cada aplicación crítica debería ser probada regularmente, y si es posible, en cada test de recuperación.

- **Realizar pruebas de copias de distinto tipo**: las copias totales y las copias parciales pueden presentar interacciones con el entorno diferentes y pueden llevar a fallos por razones completamente distintas. Conviene hacer pruebas con las distintas configuraciones que se hayan utilizado: totales, incrementales, diferenciales o de cualquier otro tipo en orden a detectar y solucionar dichos problemas.

- **Tomar precauciones al realizar pruebas destructivas**: las pruebas de copias de seguridad destructivas se deberían realizar únicamente tras haber realizado un copia comprobada de los datos sobre los que se va a realizar y esta copia no debería ser la de seguridad que se está probando.

- **Restaurar varios archivos**: restaurar archivos de distinta índole y utilizar versiones antiguas de los mismos.

- **Restaurar el sistema de archivos**: restaurar completamente el sistema de archivos y posteriormente comparar su tamaño con el original. Esta comparación de tamaños servirá para comprobar la validez de la copia.

- **Simular volúmenes dañados**: realizar la simulación de fallo en volúmenes de copias aleatorios, lo cual implica, si se ha optado por la contratación de una empresa externa de almacenamiento, el solicitar a dicha empresa los volúmenes a comprobar.

- **Comprobar la respuesta de la empresa de almacenamiento**: siguiendo con la pauta anterior, es buena práctica en pos de comprobar la rápida respuesta de la empresa de almacenamiento contratada, solicitarla aleatoriamente volúmenes de respaldo. Realizando posteriormente el correspondiente seguimiento de inventario de volúmenes.

- **En caso de respaldo de bases de datos**:

    - Simular la restauración completa de la base de datos y comprobar que no se han perdido archivos.

    - Simular la restauración parcial de la base datos, restaurando únicamente determinados datos de la misma.

    - Restaurar la base de datos a partir de un punto concreto en el tiempo anterior a la fecha de la prueba.

Al realizar las pruebas de operatividad de las copias de seguridad se debe dejar constancia de los resultados obtenidos, de esta manera podrán ser subsanados posteriormente. Esa constancia debe ser lo suficientemente clara como para que cualquier otro profesional distinto al que ha realizado la prueba sea capaz de comprenderla y actuar en consecuencia. Los informes de las pruebas realizadas deberán contener como mínimo la información que a continuación se detalla:

- Nombre de la persona que realiza la prueba.

- Cargo que ostenta.

- Qué pruebas se han realizado.

- Fecha de realización de la prueba.

- Que dispositivos se han utilizado a la hora de realizar la prueba.

- Detalles del éxito o fracaso:

    - Secuencia de las actividades realizadas en caso de fallo de la prueba.

    - Anormalidades encontradas durante la prueba las cuales, si bien no han causado el fallo de la misma, deben ser investigadas.

- Comentarios de cualquier tipo que ayuden a mejorar el plan de recuperación de acuerdo a los acontecimientos observados durante el proceso de prueba.

- Referencia a cualquier SLA[32] que cubra el sistema que se ha probado, con la inclusión, si fuera preciso, sobre la validez de dicha SLA y su conveniencia o no de revisión.

A continuación se expone el ejemplo de un posible formulario cumplimentado que incluye la información anteriormente descrita.

Prueba (Número): Recuperación de archivos y directorios en Windows 2003

Fecha:

Descripción: prueba para la comprobación que los archivos y directorios respaldados previamente por <producto> pueden ser recuperados satisfactoriamente

Requisitos: Los siguientes requisitos deben ser satisfechos antes de que se efectúe esta prueba.

1. Se ha tenido que informar que se ha producido una copia de seguridad total con resultado satisfactorio.

2. Se han tenido que añadir archivos al sistema de archivos en regiones comentadas más abajo en el "procedimiento de la prueba".

3. Se ha tenido que informar que se ha producido una copia incremental con resultado satisfactorio.

Procedimiento de la prueba:

1.- Borrado del directorio "D:\User Documents"

2.- Siguiendo las instrucciones reflejadas en la guía de usuario del producto, completar una recuperación total de los archivos y directorios que se describen más abajo.

a.- (Prueba 1) "D:\User Documents" a su ubicación original, eligiendo sobrescribir los archivos existentes.

[32] SLA (Service Level Agreement) o acuerdo de nivel de servicio es un documento, habitualmente anexo al contrato de prestación de servicios, en el que se estipulan las condiciones y parámetros que comprometen al prestador del servicio a cumplir con unos niveles de calidad del servicio frente al contratante de los mismos (Acens Tecnologies S.A.)

b.- (Prueba 2) “D:\User Documents” a “E:\Recovery”

c.- (Prueba 3) “D:\User Documents” a su ubicación original, eligiendo no sobrescribir los archivos existentes

Resultados Esperados

1.- La prueba 1 debería tener éxito sin errores ni avisos.

2.- La prueba 2 debería tener éxito sin errores ni avisos.

3.- La prueba 3 debería mostrar los archivos no recuperados, ya que todos deberían haber sido recuperados por la prueba 1.

Resultados obtenidos (*Anotar sólo “Éxito” o “Fracaso”*).

Test 1:

Test 2:

Test 3:

SE DEBEN TOMAR LAS SIGUIENTES MEDIDAS COMO RESULTADO DE ESTA PRUEBA

PERSONAL QUE HA REALIZADO LA PRUEBA

Nombre:

Cargo:

7.6 RESUMEN

A lo largo del presente capítulo se han expuesto la base de una serie de hitos que se deberían tener en cuenta a la hora de la planificación de una política de copias de seguridad funcional.

Como ya se ha comentado en varias ocasiones a lo largo del capítulo, cada situación tiene su propia problemática y características, por lo que la metodología explicada ha de adaptarse en su conjunto a cada caso en particular, pudiéndose, aun teniendo en cuenta todos, hacer más hincapié en unos hitos que en otros.

El cuadro que a continuación figura expone esquemáticamente un resumen de la metodología explicada en los apartados anteriores y se corresponde con los hitos que se deberían cubrir en el momento de diseñar una correcta política de copias de seguridad.

	Cuadro resumen. Metodología de copias de seguridad
1	Qué datos copiar
	• Recopilación de la información. • Realización de inventario. • Decisión.
2	Frecuencia de las copias
	• Elección del tipo y la frecuencia.
3	Protección de las copias
	• Duplicación de copias. • Almacenamiento. • Seguimiento. • Cifrado.
4	Testing
	• Realización de pruebas de operatividad e integridad.

8 PLAN DE RECUPERACIÓN DE DESASTRES. FUNDAMENTOS

Un plan de recuperación de desastres o DRP (del inglés Disaster Recovery Plan) es una declaración completa de acciones coherentes para ser tomadas antes, durante y tras un desastre. El plan debe ser documentado y probado para asegurar la continuidad de operaciones y la disponibilidad de recursos críticos en caso de desastre, y debe abarcar todos los aspectos que afecten a la normal operatividad de la organización (servicios informáticos, stocks, proveedores, información a los posibles clientes, etc.). Un plan adecuado para una organización en concreto no tiene porqué serlo para otra, aunque sea de características similares y los equipos informáticos implicados prácticamente los mismos, sin embargo si es del todo correcto afirmar que los fundamentos de elaboración del plan de desastre de cada una de ellas son los mismos. En esta sección se perfilarán los fundamentos necesarios para construir un plan de recuperación de desastres operativo únicamente desde el punto de vista de los datos y equipos informáticos.

El principal objetivo de un plan de recuperación de desastre es protegen a la organización en caso de que parte o la totalidad de sus operaciones o servicios informáticos se tornen no utilizables.

El proceso de planificación debería minimizar el impacto de la interrupción de las operaciones y asegurar algún nivel de estabilidad organizativa y de recuperación ordenada tras el desastre.

Otros objetivos que se buscan con un plan de recuperación de desastres son:

- Proporcionar una sensación de seguridad.
- Minimizar el riesgo de demoras.
- Garantizar la viabilidad de los sistemas de reserva.
- Minimizar la disminución de toma de decisiones durante el desastre.

8.1 PORQUÉ SE DEBE REALIZAR EL PLAN DE RECUPERACIÓN DE DESASTRES

Como ya se ha comentado anteriormente un DRP describe un grupo de acciones que se deben tomar antes, durante y tras un desastre. Cinco son las razones fundamentales por las que se debería disponer de un plan de recuperación de desastre:

8.1.1 COSTE DE LA PÉRDIDA DE DATOS

El coste económico generado por la pérdida de datos en un episodio de desastre está originado por dos tipos de costes distintos: el coste directo y el coste por la pérdida de oportunidad.

El coste directo es el originado por la pérdida material de los datos, equipos e instalaciones, los cuales han de ser recuperados mediante los medios necesarios y que genera un gasto económico que será de menor o mayor cuantía, dependiendo del volumen y del trabajo necesario para su recuperación.

El coste de oportunidad, es más difícil de cuantificar, ya que se corresponde con la pérdida de los beneficios que se habrían obtenido con los datos de no haber ocurrido el desastre. Este coste, en determinadas circunstancias, puede llegar a ser de más cuantía que el directo.

El plan de recuperación ante desastres deberá minimizar en la medida de lo posible los dos tipos de coste, pero especialmente el segundo ya que si bien han de ser repuestos datos, equipos e instalaciones, con el coste que ello origina, si dicho plan es el adecuado, las oportunidades de negocio no deberían verse mermadas en exceso.

8.1.2 RIESGO DE FRACASO EMPRESARIAL

Es un hecho comprobado estadísticamente que una pérdida definitiva de datos en el seno de una empresa puede llegar a hacer que quiebre. Según un estudio realizado en 1987 por la Universidad de Texas, que tiene por título "*Impactos funcionales y financieros de apagones informáticos en empresas*" el 43% de los negocios que sufrieron un desastre y no tenían plan de recuperación nunca reabrieron.

Actualmente y debido a la crisis financiera global, los estragos que originan comercialmente la pérdida de datos son aún mayores, fruto de la mayor competitividad que las circunstancias económicas han provocado.

Otro hecho no menos importante a tener en cuenta es el coste de imagen que se produce por un episodio de perdida de datos. Incluso si la empresa afectada por la pérdida logra recuperarse económicamente, su credibilidad de cara al público se ve seriamente mermada y le afectará económicamente de una manera casi irremediable.

Frente a estos posibles escenarios, el coste de diseñar, poner en marcha y aplicar un plan de recuperación de desastre, debería ser asumible.

8.1.3 RIESGO DE PENALIZACIONES POR VULNERAR LA LEGALIDAD VIGENTE

La carencia de un DRP, no solo puede originar perjuicios económicos de manera directa y casi inmediata derivados de un desastre comercial. El incumplimiento de la legalidad vigente por la que se rija la actividad de la corporación puede llegar, según el caso, a originar grandes pérdidas económicas, la retirada de la licencia que faculte a la empresa a ejercer su negocio o incluso penas de prisión.

Existen numerosos incidentes documentados de empresas, multadas con grandes sumas de dinero, debido a incumplimientos de normativas e incapacidad de proporcionar datos almacenados adecuados a requerimiento de la autoridad competente.

Un plan de recuperación de desastre ayuda a prevenir dichos incidentes, ya que debe contemplar todos los posibles escenarios en los que la empresa puede verse comprometida.

8.1.4 AUMENTO DE LA PRODUCTIVIDAD DE LOS EMPLEADOS

Aunque la mayoría de las organizaciones utilizan los planes de recuperación de desastre únicamente con fines de recuperación, existe la posibilidad de utilizar las políticas y procedimientos usados también como medio para aumentar la productividad de los empleados. El tener toda la información centralizada, catalogada, respaldada y monitorizada revierte directamente en la productividad general del negocio.

Al buscar soluciones para la rápida recuperación del sistema y al acceso rápido a la información, se están buscando procedimientos que optimizan dichos procesos y que pueden ser aplicados directamente al trabajo diario de la organización.

8.1.5 TRANQUILIDAD DE ESPÍRITU

Simplemente el hecho de disponer de un buen plan de recuperación de desastre, que sea conocido, aprobado y valorado por los integrantes de la empresa, genera un ambiente de trabajo mucho más relajado, derivado de la certidumbre de que la información que se maneja a diario no se encuentra comprometida y que podrá ser recuperada en caso de ser necesitada.

Este estado de ánimo revierte indirectamente la productividad de los empleados, que no se sienten presionados por las posibles consecuencias de una pérdida de datos, ya sea por desastre, fallo del sistema o incluso error humano.

8.2 ELABORACIÓN DEL PLAN DE RECUPERACIÓN DE DESASTRE

Sobre el proceso de elaboración de planes de recuperación ante desastres hay numerosas tendencias, sin embargo todas ellas se pueden sintetizar en una serie de pasos secuenciales, comunes a la mayoría de ellas:

1. Realización de inventario.
2. Análisis de riesgos.
3. Desarrollo del DRP.
4. Pruebas del DRP.

8.2.1 REALIZACIÓN DE INVENTARIO

El primer paso a realizar en el momento de comenzar a definir un plan de recuperación ante desastres consiste en la elaboración de un inventario completo de los equipos y dispositivos del sistema (incluyendo equipos, switches, controladores WLAN, puntos de acceso, etc.).

El inventario deberá incluir, como mínimo:

- Marca y modelo.
- Situación física.
- Usuario (en el caso de existir).
- Configuraciones.

8.2.2 ANÁLISIS DE RIESGOS

Una vez el inventario de los equipos y dispositivos del sistema, se ha elaborar un completo análisis de riesgos de los sistemas inventariados.

Se deberá realizar un listado de todos los posibles riesgos que amenacen de cualquier modo el sistema, evaluando en cada caso su grado de inminencia en el caso particular del sistema, desde los relativamente comunes virus informáticos o borrados accidentales de datos, hasta los menos probables escenarios de desastre como las inundaciones, incendios o deflagraciones.

El Riesgo Total (RT) se suele calcular a partir de dos magnitudes: la probabilidad de ocurrencia del desastre y el valor promedio de impacto del desastre en términos económicos. Utilizando las dos magnitudes se llega a la formulación del riesgo total como: Riesgo Total (RT) = Probabilidad de ocurrencia x Valor promedio de impacto.

Como ejemplo ilustrativo, téngase en consideración el cálculo del riesgo total ante un desastre como puede ser una inundación, con los siguientes parámetros:

- Probabilidad de ocurrencia de inundaciones al año = 0.001.
- Valor promedio de impacto de una inundación en el sistema = 150.000 €.
- Riesgo Total = 0.001 x 150.000 = 150.

Al riesgo total se le debe aplicar un como modificador el efecto de las medidas destinadas a paliarlo total o parcialmente. Con lo que se obtiene el Riesgo Residual (RR).

Siguiendo con el ejemplo anterior, considérense dos situaciones.

En la primera, la organización tiene subscrito un seguro que en caso de inundación cubre la totalidad de las pérdida d económicas, por lo tanto el Riesgo Residual tendría como valor cero.

En la segunda el mismo seguro cubre únicamente la mitad de las pérdidas ocasionadas por el desastre, con lo que el Riesgo Residual alcanzaría el valor 75.

Existen en el mercado multitud de herramientas que facilitan el proceso de evaluación y ponderación de riesgos. Principalmente basan su funcionamiento en la aplicación de dos tipos de métodos:

- Cualitativos: tienen como principal característica que permiten agilizar el proceso de análisis, permitiendo la asignación de valores de impacto medio y riesgo.
- Cuantitativos: permiten precisión y exactitud. Son más lentos pero ofrecen un mayor nivel de detalle.

El resultado final del proceso de evaluación de riesgos, ha de ser un informe en el que figure la relación de todos los riesgos que pueden potencialmente amenazar al sistema u organización, constando para cada uno de ellos como mínimo la siguiente información:

- Riesgo Total.
- Riesgo Residual.

- Probabilidad de ocurrencia.
- Valor promedio de impacto.

8.2.3 DESARROLLO DEL DRP

Una vez que se dispone del informe de riesgos, se puede comenzar a diseñar el plan de recuperación ante desastre., teniendo en cuenta los resultados obtenidos y estableciendo como principal referencia el RTO.

El tiempo objetivo de recuperación, o RTO (Recovery Time Objetive), se define como el máximo periodo de tiempo en el que en caso de desastre se deben restaurar determinados servicios mínimos de una empresa u organización, en orden de evitar consecuencias inaceptables para su viabilidad o incluso existencia.

Un buen DRP ha de contener como mínimo la siguiente información (Bradbury, 2007):

- Declaración que en detalle describa el alcance y la capacidad del plan, más exactamente deberá especificar cuándo se debería ejecutar el plan y qué cubre. En este punto es importante destacar que el plan en ningún momento tratará del porqué del desastre producido, sino que se centrará en las acciones a seguir para recuperarse del mismo.
- Una descripción detallada de los roles y responsabilidades de todas las personas vinculadas de alguna manera con la ejecución del plan. Se deben definir equipos de actuación para cada sector de recuperación, formados con personal especializado en dicho sector y entrenados para la ocasión.

  El objetivo de definir roles no es otro que el de que llegada la ocasión, cada componente del equipo de recuperación sepa qué hacer en cada momento y sea autosuficiente en el desempeño de su tarea.
- Un sumario de los servicios críticos, sus objetivos de recuperación y sus prioridades de recuperación. Al reflejar estas informaciones en el plan, se evita el tener que tomar decisiones en tiempo real que pudieran llevar a diferencias de opinión entre los distintos componentes de los equipos de recuperación.
- Detalles terceros agentes, particularmente de aquellos que deberán prestar soporte en el momento de la recuperación. Esta información deberá ser todo lo clara posible y estar convenientemente actualizada (cambio de proveedores de servicios de almacenamiento, cambio de datos de algún agente, etc.).

- Una relación detallada de las actividades a realizar, con la secuencia de los acontecimientos perfectamente especificada, incluyendo prerrequisitos, dependencias y responsabilidades.

  Este punto es crucial, ya que de su correcta implementación dependerá que las actividades de recuperación se lleven a cabo en un orden correcto y por las personas adecuadas, evitando de esta manera posibles episodios de incompatibilidades de actuaciones, por ejemplo intentando realizar una determinada actividad que, dependiendo de otra secuencialmente anterior, se ha comenzado antes que ella.

8.2.4 PRUEBAS DEL DRP

El plan de recuperación ante desastres ha de ser probado regularmente, con una frecuencia que dependerá de las necesidades particulares de cada organización.

Es importante realizar pruebas de todos los actores implicados en la recuperación: el plan, los equipos de recuperación, las infraestructuras, o cualquier otro agente que juegue un papel en el proceso de recuperación.

Las pruebas han de realizarse bajo las condiciones más parecidas a las que se producirían en caso de desastre, evitando situaciones “cómodas” en las que la recuperación sería sencilla.

Los principales puntos que se deberían tener en cuenta a la hora de la realización de las pruebas son:

- La calidad de los procesos de recuperación y sus procedimientos.
- La familiarización de del personal que se ocupará de la recuperación con el proceso y su documentación.
- La verificación de la calidad de la documentación del plan.
- El establecimiento de la viabilidad de los objetivos de recuperación marcados como alcanzables.
- La identificación de posibles mejoras en cualquiera de los componentes del plan definido.

Un correcto plan ante desastre es un ente que evoluciona Es un error considerar que tras haber definido un DRP viable y que ha sido probado con éxito en numerosas ocasiones se puede considerar acabado y perdurable en el tiempo. Por el contrario el

DRP debe revisarse y modificarse, si es preciso, constantemente, reflejando en cada momento la realidad de la organización.

9 CASO PRÁCTICO

9.1 INTRODUCCIÓN

En este último capítulo se expondrá un caso práctico en el que se aplicará la metodología explicada en anteriores secciones del documento. Para ello se simulará el caso de un cliente (notario) que está interesado en contratar los servicios de una empresa dedicada a la programación, configuración y seguimiento de copias de seguridad de datos, en orden a planificar la política de copias de seguridad de su notaría.

Se ha elegido como caso práctico el de una Notaría por tratarse de una empresa de carácter oficial, en la que se trabaja con información de carácter privado, por lo que se tendrá que tener en cuenta la actual ley de protección de datos e carácter personal, y cuyo volumen de datos es lo suficientemente grande como para servir a los fines didácticos que se persiguen.

Como ya se ha comentado al principio de esta introducción, la metodología que se empleará será un reflejo de la ya explicada en apartados anteriores del presente trabajo, y consistirá de una manera esquemática en los siguientes pasos:

1. **Qué datos copiar**: se comenzará recabando toda la información posible, se realizará un inventario completo de los equipos y software de la notaría y finalmente se decidirá qué datos se han de respaldar.

2. **Frecuencia de las copias**: se estudiará y determinará la frecuencia con la que se han de realizar los respaldos, es decir, se programarán las rutinas de copias de seguridad.

3. **Protección de los volúmenes**: se tomará las decisiones necesarias para proteger en la medida de lo posible, integridad y confidencialidad de las copias generadas.

4. **Testing**: para finalizar, se fijarán con el diseño de la política de copias de seguridad, se fijarán las rutinas más adecuadas de control y comprobación de los volúmenes de respaldo.

Durante la resolución del caso, si bien no se hará de manera exhaustiva, se utilizarán las herramientas propias de la ingeniería del software que se consideren necesarias para lograr el objetivo final perseguido.

9.2 PRESENTACIÓN DEL CASO

Una notaría es el lugar físico dónde el notario ejerce su cargo de funcionario público, consistente básicamente en la aportación a los ciudadanos la seguridad jurídica que promete la Constitución en su artículo 9º en el ámbito del tráfico jurídico extrajudicial.

El notario contratante requiere que se le diseñe y mantenga una política de copias de seguridad que proteja los datos de la notaría en caso de desastre, y que tanto su implementación como su mantenimiento no supongan, en ningún momento y bajo ningún concepto, la detención del trabajo diario de la notaría.

9.3 QUÉ DATOS COPIAR

La primera decisión importante que es necesario tomar al comenzar a planificar la política de seguridad a seguir en la notaría consiste en decidir qué datos se han de incluir en las copias de seguridad. Para poder alcanzar dicho fin, se han de realizar previamente una exhaustiva labor de investigación, mediante entrevistas con el cliente y usuarios, en pos de recabar toda la información que se pueda obtener del sistema que funciona en la notaría. Seguidamente es necesario realizar un inventario de todos aquellos elementos que ayuden a tomar la decisión final. Para finalizar se realizará un informe que dará cuenta de todos los datos que se necesitarán ser incluidos en los volúmenes de respaldo.

9.3.1 INFORMACIÓN RECABADA

Tras realizar numerosas reuniones tanto con el notario contratante, como con cada uno de los empleados de la notaría, se han realizado un análisis previo cuyos resultados figuran a continuación.

La notaría cliente ha organizado su trabajo en cinco áreas claramente diferenciadas[33]:

9.3.1.1 RECEPCIÓN

El recepcionista se ocupa de recibir a los clientes. A efectos de trasiego de datos, su principal labor consiste en dar de alta a los clientes en la base de datos de la notaría controlada por un software específico de gestión de notarías.

Para dicha labor utiliza un escáner de documentos que, tras realizar la lectura de los documentos identificativos de cada cliente, enlaza con el programa de gestión y los da de alta de manera automática en la base de datos.

A diario realiza trabajos que requieren la utilización de documentos en formato Microsoft Word, tales como informes, listados de clientes o cartas a los mismos. Los modelos que utiliza, junto con los documentos que va creando o modificando, los almacena en una carpeta denominada "*Varios*", y ubicada en una partición del disco duro denominada "Datos", con "F" como letra de unidad.

[33] Por motivos de claridad se ha supuesto que existe, para cada área de trabajo de la notaría, una única persona que desarrolla dicha tarea.

9.3.1.2 EL OFICIAL

Es el los encargado de elaborar los documentos de los que finalmente dará fe el notario.

Para ello utiliza un software de procesamiento de textos, basado en Microsoft Word, y que está especialmente diseñado para el trabajo de notarías. Los archivos en formato Word que utiliza en su trabajo diario los almacena en carpetas de su equipo, un ordenador personal, denominada "*modelos escrituras*", y ubicada en una partición del disco duro denominada "Datos", con "F" como letra de unidad. El contenido de las carpetas de almacenamiento de documentos varía diariamente.

Una vez que una escritura está finalizada, a falta de que el notario la haya firmado, la envía a una carpeta ubicada en un disco duro interno del servidor dedicado a datos, de letra de unidad G (Datos), denominada "*Pendientes de firma*". Esta carpeta es volátil y únicamente sirve de puente entre el oficial y el copista, por lo que sólo contiene documentos del día, por lo que a efectos de copias de respaldo no tiene ninguna transcendencia.

9.3.1.3 COPIAS

En cuanto a datos informáticos, el copista se encarga de elaborar el protocolo electrónico. Para ello, cada vez que un oficial ha finalizado una escritura y la ha enviado a la carpeta "*Pendientes de firma*", el copista la toma de dicha carpeta, la revisa, completa con los datos faltantes, por ejemplo el número de protocolo[34] o la fecha, e inserta la documentación unida en caso que sea necesario. Finalmente lo guarda en la carpeta "*Protocolo*" del servidor.

La carpeta "*Protocolo*", ubicada en el disco de datos, G (Datos), del servidor de datos de la notaría, contiene todo el protocolo electrónico del notario. Actualmente el protocolo electrónico del notario contiene los protocolos de los últimos cuatro años y su volumen en datos ronda los 5 GB.

Los documentos que utiliza el copista en el transcurso de su trabajo y que almacena en una carpeta de su equipo denominada "*modelos copias*", ubicada en una partición del disco duro denominada "Datos", con "F" como letra de unidad y consisten básicamente en modelos con formato Microsoft Word, y una vez configurados, varían muy poco en el tiempo.

[34] Los documentos en papel oficial que un notario "genera" se denominan protocolos, y tienen una numeración única y consecutiva por ejercicio y notario. Cada protocolo en papel tiene su correspondiente versión digital, y al conjunto de todos ellos se le denomina protocolo electrónico.

También utiliza el programa de gestión para consultar datos de los clientes.

Utiliza una impresora multifunción de gran capacidad que utiliza, además de cómo impresora, como escáner de documentación unida. El software de escaneado que utiliza la impresora es de tipo Twain, por lo que las imágenes se insertan directamente en los documentos en formato Word.

9.3.1.4 GESTIÓN Y CONTABILIDAD

El contable desarrolla toda su labor mediante la utilización de un software específico para entornos notariales. Dicho software almacena toda la información centralizada en una única carpeta del servidor de datos denominada "*Datos Gestión*", ubicada en el disco de datos G (Datos).

El puesto de trabajo del contable (que es el mismo que el del personal de recepción), consiste simplemente en una interfaz cliente que accede al software servidor de gestión que se encuentra instalado en el servidor de datos e la notaría. Si bien es necesario instalar el cliente en el puesto de trabajo, dicha instalación es en extremo sencilla y rápida.

Eventualmente utiliza también el programa de textos para la elaboración de cartas o comunicaciones varias, cuyos modelos almacena en una carpeta de su equipo denominada "*cartas*", y ubicada en una partición del disco duro denominada "Datos" con "F" como letra de unidad, además de hojas de cálculo en formato Microsoft Excel que guarda en la misma carpeta.

9.3.1.5 NOTARIO

Es el dueño de la notaría y responsable legal de todos los documentos de la misma.

Dispone de un ordenador personal en el que trabaja casi exclusivamente con documentos de Microsoft Word que guarda en una carpeta a la que ha denominado "Personal", ubicada en una partición del disco duro denominada "Datos" con "F" como letra de unidad.

También utiliza el programa de gestión para consultar datos de los clientes.

9.3.1.6 AGENDA

Además de lo anteriormente expuesto, se ha de tener en consideración que la gestión de la agenda de citas de la notaría se realiza mediante un software de código abierto instalado en cada equipo, y cuyo archivo de datos reside en el servidor, en una carpeta denominada "*Agenda Notaria*", y es compartido y utilizado por todos los equipos de la notaría.

9.3.1.7 CORREO ELECTRÓNICO Y LIBRETA DE DIRECCIONES

También se ha de tener en cuenta que una parte importante del trabajo de todos los usuarios lo constituyen tanto su correo electrónico como la libreta de direcciones de contactos asociada al mismo. Para esa función utilizan el software de Microsoft Outlook Express, y como medida de seguridad y con el fin de no recargar en exceso la partición del disco duro que alberga al sistema operativo, la carpeta de almacenamiento en donde se guardan los correos, se ha movido a una carpeta llamada "*Correo Usuario*", ubicada en la partición "*Datos*", que todos los equipos poseen.

9.3.1.8 APLICACIONES Y LICENCIAS DE SOFTWARE

En cuanto al software notarial anteriormente indicado, la notaría tiene en su poder, tanto los discos de instalación como la documentación necesaria para su reinstalación en caso de que fuera necesario. No obstante la notaría tiene un contrato de mantenimiento con la empresa suministradora del software, que en caso de necesidad, se haría cargo de la completa reinstalación de los programas, tanto en los equipos como en el servidor. El software en cuestión guarda toda la información en dos carpetas, una de configuración y otra de datos (en la que se incluyen las bases de datos que utiliza), denominadas respectivamente "*Configuración Gestión*", ubicada en "*Archivos de Programa*" del servidor y "*Datos Gestión*" ubicada en la raíz de un disco duro interno dedicado a datos en el servidor de letra de unidad G. El propio software realiza una copia viable diaria de sus bases de datos en una carpeta no compartida denominada "*Copia Gestión*", ubicada en un disco duro externo (E) del servidor habilitado para tal efecto y con ruta: *E:\Copia Gestion*.

9.3.1.9 CONFIGURACIÓN DE RED

En la notaría no existe ningún tipo de dominio, sino que se ha establecido un grupo de trabajo denominado NOTARIA, en el que han sido incluidos todos los equipos de la red.

Las direcciones IP de los equipos e impresoras no son asignadas automáticamente, sino que son prefijadas. La relación de todas las direcciones IP de la notaría se guarda en un documento de extensión .txt denominado "*configuraciones_red*", que se actualiza cuando es necesario y se encuentra en una carpeta de nombre "C*onfiguraciones*" ubicada en el disco externo comentado anteriormente.

Así mismo dicho archivo "configuraciones_red" guarda una relación de los nombres de usuario, contraseña[35] y nombre de equipo de cada usuario de la notaría. El contenido de dicho archivo se ve reflejado en las siguientes tablas:

	IP	Máscara Subred	Puerta Enlace	DNS 1	DNS 2
Servidor	192.168.0.1	255.255.255.0	111.0.0.111	10.11.12.13	10.11.12.14
Recepción	192.168.0.2	255.255.255.0	192.168.0.1	10.11.12.13	10.11.12.14
Oficial	192.168.0.3	255.255.255.0	192.168.0.1	10.11.12.13	10.11.12.14
Copias	192.168.0.4	255.255.255.0	192.168.0.1	10.11.12.13	10.11.12.14
Gestor	192.168.0.5	255.255.255.0	192.168.0.1	10.11.12.13	10.11.12.14
Notario	192.168.0.6	255.255.255.0	192.168.0.1	10.11.12.13	10.11.12.14
Impr_Recepción	192.168.0.102	255.255.255.0	192.168.0.1	10.11.12.13	10.11.12.14
Impr_Oficial	192.168.0.103	255.255.255.0	192.168.0.1	10.11.12.13	10.11.12.14
Impr_Copias	192.168.0.104	255.255.255.0	192.168.0.1	10.11.12.13	10.11.12.14
Impr_Gestor	192.168.0.105	255.255.255.0	192.168.0.1	10.11.12.13	10.11.12.14
Impr_Notario	192.168.0.106	255.255.255.0	192.168.0.1	10.11.12.13	10.11.12.14

[35] Se han simplificado las contraseñas, nombres de usuario y de equipo por motivos de claridad.

	Usuario	Contraseña	Nombre Equipo
Recepción	recepción	Recepcion1	Pc_Rececion
Oficial	oficial	Oficial1	Pc_Oficial
Copias	copias	Copias1	Pc_Copias
Gestor	gestor	Gestor1	Pc_Gestor
Notario	notario	Notario1	Pc_notario

9.3.1.10 HARDWARE (EQUIPOS E IMPRESORAS)

Todos los ordenadores personales de la notaría se adquirieron a la vez y tienen, a excepción del servidor, exactamente las mismas características. El sistema operativo de todos los equipos es Microsoft Windows XP SP3, excepto el servidor que corre bajo Windows Server 2008.

Todos los empleados disponen de una impresora en su despacho conectada en red, es decir, no hay ninguna conectada directamente a ningún equipo. Las impresoras fueron adquiridas a un mismo proveedor en el momento de poner en marcha la notaría, y son todas del mismo modelo de Hp, concretamente **Hp 4200 dtn**. La única que es diferente es la impresora multifunción de gran capacidad que utiliza el copista, se trata de una impresora Canon modelo **adv 6055**, **con módulo de escaneo incorporado**. La información de las acerca de las direcciones IP de las impresoras se encuentra almacenada en el archivo “configuraciones_red”, comentado con anterioridad.

Un dato importante a tener en cuenta es que el notario en ningún caso contempla la idea de adquirir ningún dispositivo de copias de seguridad basado en cintas magnéticas, por lo que la obtención de estas pasará por considerar únicamente sistemas que incluyan dispositivos ópticos y discos magnéticos.

Por último comentar que en la notaría se trabaja todos los días laborables de lunes a viernes además de determinados domingos y festivos que tiene que permanecer de guardia y cuyas fechas son conocidas mensualmente.

9.3.2 PRIMERAS CONCLUSIONES

Tras analizar la información anteriormente descrita, fruto de entrevistas y observación en la propia notaría, se puede llegar a las primeras conclusiones a cerca del trasiego de datos que se produce en su seno.

En las siguientes tablas se indica para cada usuario, qué tipo de datos utiliza, su tamaño aproximado, su ubicación y con qué frecuencia cambian. Se ha de tener en cuenta que los datos que son compartidos por los usuarios, tales como la base de datos del programa de gestión, la carpeta "*Protocolo*", la carpeta "*Pendientes de firma*" o la agenda, figuran bajo la responsabilidad del servidor que es dónde se encuentran ubicados.

Usuario: Recepción

	Tamaño	Ubicación	Cambio
Tipo: *.doc	Pequeño	F:\Varios	Diario
Tipo: *.dbx	Grande	F:\Correo Recepcion	Diario

Usuario: Oficial

	Tamaño	Ubicación	Cambio
Tipo: *.doc	Medio	F:\Modelos Escrituras	Diario
Tipo: *.dbx	Grande	F:\Correo Oficial	Diario

Usuario: Copias

	Tamaño	Ubicación	Cambio
Tipo: *.doc	Pequeño	F:\Modelos Copias	Casi nunca
Tipo: *.dbx	Grande	F:\Correo Copias	Diario

Usuario: Gestor

	Tamaño	Ubicación	Cambio
Tipo: *.doc	Pequeño	F:\Cartas	Diario
Tipo: *.dbx	Grande	F:\Correo Gestor	Diario
Tipo: *.xls	Pequeño	F:\Cartas	Diario

Usuario: Notario

	Tamaño	Ubicación	Cambio
Tipo: *.doc	Pequeño	F:\Personal	Casi nunca
Tipo: *.dbx	Grande	F:\Correo Notario	Diario

Usuario: Servidor

	Tamaño	Ubicación	Cambio
Tipo: *.doc	Grande	G:\Protocolo	Diario
Tipo: *.txt	Pequeño	E:\ Configuraciones	Casi nunca
Tipo: *.ges[36]	Grande	G:\Datos Gestion	Diario
Tipo: *.age[37]	Pequeño	G:\Agenda_Notaria	Diario
Tipo: *.gestion (copia)	Grande	E:\ Copia_Gestion	Diario

La ilustración que a continuación figura resume el movimiento de datos que en la actualidad y diariamente se produce en el seno de la notaría. En él, las flechas orientadas representan movimiento de datos, y la leyenda asociada a cada una de ellas, el tipo de dato involucrado.

[36] Se ha considerado que las bases de datos el software de gestión tienen como extensión ficticia "*.ges*"
[37] Se ha utilizado como extensión de los archivos de la agenda "*.age*"

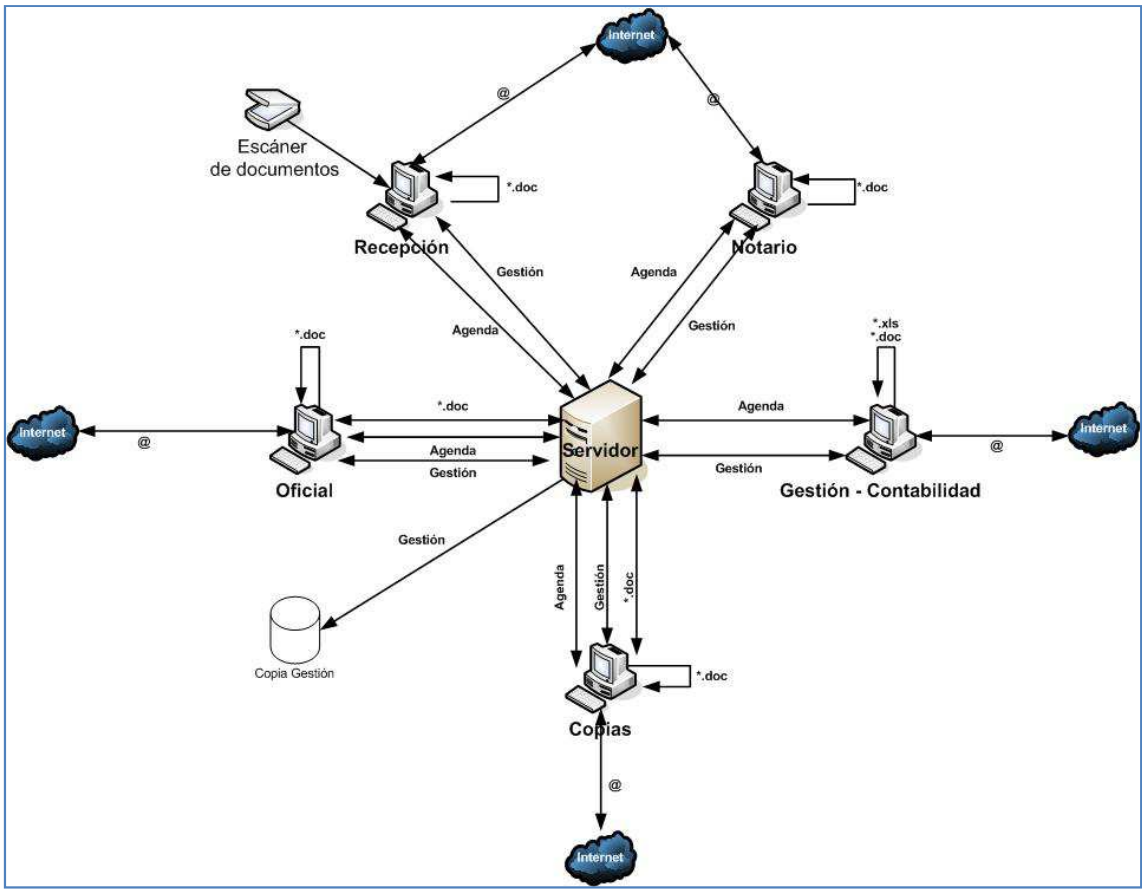


Ilustración 30. Esquema de movimiento de datos actual de la notaría.

9.3.3 REALIZACIÓN DE INVENTARIO

Una vez que se ha obtenido toda la información posible de los usuarios y su forma de trabajar, será necesario hacer un inventario del sistema que es utilizado en la notaría.

Con él, no sólo se podrá tomar una decisión lo más acertada posible en cuanto a qué datos se deberán incluir en las copias de respaldo, sino que servirá como una valiosa fuente de información que agilizará de una manera sensible la recuperación de todo o parte del sistema en caso de desastre.

La información obtenida en este punto ha de ser almacenada en lugar seguro e incluida en alguno de los volúmenes de respaldo, además de ser, en la medida de lo posible, transcrita y trasladada a papel.

Siguiendo la metodología explicada en apartados anteriores del presente trabajo, el inventario se efectuará teniendo en cuenta varios aspectos:

- Listado de discos y particiones.

- Hardware.
- Configuración de bases de datos y contenedores de datos.
- Configuración de DHCP, Active Directory, NFS y CIFS.

9.3.3.1 LISTADO DE DISCOS Y PARTICIONES Y HARDWARE

Como se ha comentado en la sección dedicada a la recopilación de datos, todos los ordenadores personales de la notaría, a excepción del servidor, tienen exactamente las mismas características técnicas, por lo que sus unidades de disco y particiones son idénticas.

Por ese motivo el listado de discos y particiones de la notaría consta únicamente de dos tipos de casos: ordenadores personales y servidor.

9.3.3.1.1 Ordenadores personales

Los ordenadores personales de la notaría constan de un único disco duro de 250 GB de capacidad, dividido en dos particiones, la primera, de 100 GB, alberga el sistema operativo y la segunda, denominada "*Datos*" de 150 GB, es utilizada para guardar los documentos necesarios en el transcurso de su jornada laboral.

Partiendo de *la ventana de MS-DOS (Símbolo del Sistema) de Windows* y realizando los pasos indicados en el apartado dedicado a la obtención de la información de discos y particiones en sistemas basados en Windows, que figura en anteriores apartados del presente trabajo, se obtiene la siguiente información (marcada en negrita) que debe ser imprimida y guardada en lugar seguro y accesible, ya que será de gran importancia en caso de desastre.

En el propio informe se puede apreciar en cursiva los comandos que se han ido utilizando en la obtención del mismo.

```
C:\Documents and Settings\Usuario>diskpart

Microsoft DiskPart versión 5.1.3565

Copyright (C) 1999-2003 Microsoft Corporation.
En el equipo: Pc_usuario

DISKPART> select disk 1

El disco 1 es ahora el disco seleccionado.
DISKPART> list partition
  Partición ###  Tipo              Tamaño     Desplazamiento
  ------------  ----------------  -------  -------
  Partición 1    Principal           100 GB    32 KB
  Partición 2    Principal          150 GB    49 GB

DISKPART> select partition 1
La partición 1 es ahora la partición seleccionada.

DISKPART> detail partition
Partición 1
Tipo: 07
Oculta: No
Activa: Sí

  Volumen ###  Etiqueta  Ltr         Fs     Tipo        Tamaño     Estado     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
* Volumen 1    C               NTFS   Partición     100 GB  Correcto   Inicio

DISKPART> select partition 2
La partición 2 es ahora la partición seleccionada.

DISKPART> detail partition

Partición 2
Tipo: 07
Oculta: No
Activa: No

  Volumen ###  Etiqueta  Ltr         Fs     Tipo        Tamaño     Estado     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
* Volumen 2     F   Datos        NTFS   Partición    150 GB  Correcto

DISKPART>
```

El archivo generado por este procedimiento será guardado en una carpeta del servidor que será incluida en el proceso de copia de respaldo del mismo. En la carpeta *Configuraciones*, ubicada en el disco E del servidor, irán almacenando los distintos informes que se vayan obteniendo de los ordenadores personales.

Así mismo es necesario de disponer de toda la información relativa al hardware que sea posible. Esto permitirá acelerar el proceso de recuperación en caso de que los discos de instalación de los drivers propios de cada ordenador, o la documentación de los mismos (modelo de placa madre, modelo de tarjeta de red, modelo de tarjeta de video, etc.) se extravíe.

Para este cometido existen multitud de aplicaciones, muchas de ellas gratuitas, que permiten obtener un informe detallado de todos los componentes instalados en el ordenador. Una vez obtenido dicho informe deberá ser almacenado en el mismo lugar que el anterior correspondiente a los discos duros y las particiones, y al igual que el mismo, ser transcrito, si es posible a papel y depositado en lugar seguro y de fácil acceso en caso de ser necesitado.

En este caso se utilizará para tal tarea la aplicación de uso libre ***Everest***. La aplicación dispone de un asistente para generar informes que se ha utilizado para generar un informe del hardware del equipo. Dicho informe, al igual que el anteriormente obtenido de los discos y sus particiones, se trasladará a papel y almacenará en lugar seguro y accesible en caso de necesidad. Del mismo modo el archivo creado se incluirá en el proceso de copia de seguridad, guardándolo en la carpeta *Configuraciones* anteriormente creada en el servidor.

Como ejemplo se muestra parte del informe obtenido, más concretamente las secciones dedicadas al sistema operativo, la placa base, el monitor, la tarjeta de sonido, los dispositivos de entrada y a la tarjeta de red.

Ordenador:

Sistema operativo	Microsoft Windows XP Professional
Service Pack del Sistema Operativo	Service Pack 3
DirectX	4.09.00.0904 (DirectX 9.0c)
Nombre del sistema	Pc_Usuario
Nombre de usuario	usuario

Placa base:

Tipo de procesador	AMD Athlon 64, 2400 MHz (12 x 200) 3400+
Nombre de la Placa Base	Asus K8N (5 PCI, 1 AGP, 3 DDR DIMM, Audio, LAN)
Chipset de la Placa Base	nVIDIA nForce3 250, AMD Hammer
Memoria del Sistema	2560 MB (PC3200 DDR SDRAM)
Tipo de BIOS	AMI (02/16/06)
Puerto de comunicación	Puerto de comunicaciones (COM1)
Puerto de comunicación	Puerto de impresora ECP (LPT1)

Monitor:

Tarjeta gráfica	RADEON 9250 - Secondary (256 MB)
Tarjeta gráfica	RADEON 9250 (256 MB)
Acelerador 3D	ATI Radeon 9250 (RV280)
Monitor	Monitor Plug and Play [NoDB] (5777632ABCDE)

Multimedia:

Tarjeta de sonido	Creative SB0312 Audigy LS Sound Card

Dispositivos de entrada:

Teclado	Dispositivo de teclado HID
Ratón	Mouse compatible con HID

Red:

Tarjeta de Red	NVIDIA nForce Networking Controller – Minipuerto del administrador de paquetes (192.168.1.15)

Cada usuario de la notaría tiene como obligación la custodia de todos los discos de instalación de su equipo, por lo que en caso de necesidad serán los responsables de suministrarlos.

9.3.3.1.2 Servidor

El listado de los discos y particiones del servidor se obtiene realizando los mismos procedimientos que en el caso de los ordenadores personales.

Los informes obtenidos deberán ser imprimidos y almacenados, y los archivos de los que proceden guardados en la carpeta *Configuraciones* del disco duro externo del servidor.

En cuanto a los discos de instalación del servidor, un Fujitsu modelo TX200, son custodiados por el propio notario, que en caso de necesidad será el encargado de suministrarlos.

9.3.3.2 CONFIGURACIONES DE BASES DE DATOS Y CONTENEDORES DE DATOS

La notaría trabaja principalmente con dos tipos de bases de datos: gestión y documentos (.doc, .xls y .dbx).

Los primeros son directamente gestionados por el software especializado en notarías y tanto su configuración como su mantenimiento y primera copia de seguridad corren a cargo de la empresa suministradora del software que, como ya se ha comentado anteriormente, tiene un contrato de mantenimiento con la notaría.

No obstante, a efectos poder realizar una programación eficiente de la copia de seguridad de los datos totales de la notaría, dicha empresa informa que su software de gestión efectúa una copia diaria de sus bases de datos, que es ubicada, como ya se ha comentado anteriormente, en una carpeta denominada *Copia_gestion* del disco duro externo del servidor (E). Esta copia diaria es total y cada día de la semana sobrescribe los datos sustituyendo los antiguos por los nuevos, es decir, contiene una carpeta para cada día de la semana con los datos actualizados. Dicha carpeta es la que se deberá incluir en la programación de las copias de seguridad.

En cuanto al resto de los datos, tanto de los ordenadores personales como del servidor, se tratan de meros contenedores de datos sin ningún tipo de configuración más allá de su ubicación y contenido.

Los datos de la siguiente tabla reflejan las carpetas, junto con sus ubicaciones, que se tendrán que incluir finalmente en la programación de las copias de seguridad. La tabla únicamente informa de contenedores de datos, la decisión acerca de qué tipo de copia se realizará se tomará posteriormente.

9.3.3.3 CONFIGURACIÓN DE DHCP, ACTIVE DIRECTORY, NFS Y CIFS

En caso de desastre, la configuración de Active Directory, NFS y CIFS, se realizarán mediante la utilización de los discos de instalación del servidor.

El proceso está completamente automatizado, teniendo únicamente que configurar todos los aspectos relativos a las cuentas de usuario. En este aspecto cabe destacar que todos los usuarios de la notaría han sido incluidos en un grupo de usuarios denominado “NOTARIA”, ya que no se hace distinción alguna entre ellos en cuanto a permisos de lectura, escritura y modificación de los datos compartidos del servidor.

La lista de usuarios del servidor deberá ser exportada a algún tipo de archivo, por ejemplo de extensión .txt, y como en el resto de casos imprimida y almacenada en lugar seguro y accesible, guardando el archivo en la carpeta *Configuraciones* del servidor.

En cuanto a la configuración de DHCP no será necesaria, ya que como se ha comentado con anterioridad, la dirección IP de cada puesto de trabajo, o periférico en funcionamiento en la notaría, son asignadas manualmente y su configuración se ha guardado en el archivo correspondiente que se ha almacenado en la carpeta *Configuraciones* del servidor.

9.3.4 QUÉ DATOS COPIAR

Una vez que se han recabado todos los datos necesarios, es posible tomar una decisión acerca de qué datos serán incluidos en la copia de respaldo de la notaría. Para ello se realizará un informe final detallado, por usuario, de los datos a copiar. Dicho informe incluirá el tipo de dato, su ubicación, tamaño medio e índice aproximado de cambio diario.

Estos datos, especialmente los dos últimos (tamaño e índice de cambio), servirán para poder decidir adecuadamente con posterioridad qué tipo de copia se realiza (incremental, diferencial, total, etc.).

9.3.4.1 USUARIO: RECEPCIÓN

Recurso	Ubicación	Tipo	Tamaño	Índice
Documentos	F:\Varios\	*.doc	Pequeño	Diario
Documentos Personales	C:\Documents and Settings \ recepción \ Mis Documentos\	Varios	Medio	Medio
Correos Electrónicos	F:\Correo Recepcion\	*.dbx	Grande	Diario
Libreta Direcciones	C:\Documents and Settings \ recepcion\ Datos de programa \ Microsoft \ Adress Book \	*.wab	Pequeño	Medio
Favoritos de Internet	C:\Documents and Settings \ recepcion \ Favoritos\	Varios	Pequeño	Bajo

9.3.4.2 USUARIO: OFICIAL

Recurso	Ubicación	Tipo	Tamaño	Índice
Documentos	F:\Modelos Escrituras\	*.doc	Medio	Diario
Documentos Personales	C:\Documents and Settings \ oficial \ Mis Documentos\	Varios	Medio	Medio
Correos Electrónicos	F:\Correo Oficial\	*.dbx	Grande	Diario
Libreta Direcciones	C:\Documents and Settings \ oficial\ Datos de programa \ Microsoft \ Adress Book \	*.wab	Pequeño	Medio
Favoritos de Internet	C:\Documents and Settings \ oficial \ Favoritos\	Varios	Pequeño	Bajo

9.3.4.3 USUARIO: COPIAS

Recurso	Ubicación	Tipo	Tamaño	Índice
Documentos	F:\Modelos Copias\	*.doc	Pequeño	Bajo
Documentos Personales	C:\Documents and Settings \ copias \ Mis Documentos\	Varios	Medio	Medio
Correos Electrónicos	F:\Correo Copias\	*.dbx	Grande	Diario
Libreta Direcciones	C:\Documents and Settings \ copias\ Datos de programa \ Microsoft \ Adress Book \	*.wab	Pequeño	Medio
Favoritos de Internet	C:\Documents and Settings \ copias \ Favoritos\	Varios	Pequeño	Bajo

9.3.4.4 USUARIO: GESTOR

Recurso	Ubicación	Tipo	Tamaño	Índice
Documentos	F:\Cartas\	*.doc	Pequeño	Diario
Documentos	F:\Cartas\	*.xls	Pequeño	Diario
Documentos Personales	C:\Documents and Settings \ gestor \ Mis Documentos\	Varios	Medio	Medio
Correos Electrónicos	F:\Correo Gestor\	*.dbx	Grande	Diario
Libreta Direcciones	C:\Documents and Settings \ gestor\ Datos de programa \ Microsoft \ Adress Book \	*.wab	Pequeño	Medio
Favoritos de Internet	C:\Documents and Settings \ gestor \ Favoritos\	Varios	Pequeño	Medio

9.3.4.5 USUARIO: NOTARIO

Recurso	Ubicación	Tipo	Tamaño	Índice
Documentos	F:\Personal\	*.doc	Pequeño	Diario
Documentos Personales	C:\Documents and Settings \ notario \ Mis Documentos\	Varios	Medio	Medio
Correos Electrónicos	F:\Correo Notario\	*.dbx	Grande	Diario
Libreta Direcciones	C:\Documents and Settings \ notario\ Datos de programa \ Microsoft \ Adress Book \	*.wab	Pequeño	Medio
Favoritos de Internet	C:\Documents and Settings \ notario \ Favoritos\	Varios	Pequeño	Medio

9.3.4.6 SERVIDOR

Recurso	Ubicación	Tipo	Tamaño	Índice
Bases de datos de gestión	E:\Copia Gestion\	.ges	Grande	Diario
Protocolo electrónico	G:\Protocolo\	.doc	Grande	Diario
Agenda Notaría	G:\Agenda Notaria\	.age	Pequeño	Diario
Configuraciones	E:\Configuraciones\	Varios	Pequeño	Bajo

9.4 FRECUENCIA (PROGRAMACIÓN DE LAS COPIAS DE RESPALDO)

9.4.1 INTRODUCCIÓN

Previamente a realizar la labor del diseño de la programación de las copias de seguridad, se ha de decidir qué dispositivos darán soporte a las mismas. En este sentido, y teniendo en cuenta la imposibilidad de instalación de dispositivos de grabación de cintas magnéticas, se ha optado por el almacenamiento de las mismas en discos duros externos, que se utilizarán para el almacenamiento on-site de los volúmenes de respaldo, junto con la utilización de dispositivos ópticos (Cd y DVD) para su almacenamiento off-site.

La elección del almacenamiento de los volúmenes de respaldo en discos duros externos, implica tomar una nueva decisión a cerca de la ubicación de los mismos. En este sentido se puede optar básicamente por dos vías de actuación:

- **Centralización**: la centralización se llevaría a cabo instalando uno o varios discos duros externos en el servidor. Si se opta por este método, consecuentemente se ha de decidir qué cliente realiza la copia:
    - Servidor: en este caso es el servidor quién mediante un software especializado en copias de seguridad ejecuta la rutina de copias, accediendo a los diferentes equipos de la notaría, recabando los datos y almacenándolos en el disco duro externo correspondiente.
    - Equipos: en este caso es cada equipo el que ejecuta la rutina de copias de seguridad, recabando los datos y enviándolos al disco duro externo del servidor que se tenga configurado.
- **Descentralización**: la descentralización consiste en la instalación en cada equipo de la notaría de un disco duro externo en el que se almacenarán los volúmenes de copias de seguridad. En este caso es cada equipo quién se hace cargo de la rutina de copia.

Cada uno de los métodos descritos goza de ventajas e inconvenientes que hacen que la elección entre uno y otro dependa de las circunstancias particulares de cada caso.

En el caso que se está considerando, la notaría, la centralización de las copias de seguridad en un único punto tiene como ventaja que el seguimiento y mantenimiento de las mismas es más sencillo, debido a su carácter centralizado. Todo el proceso de copia, las pruebas de operatividad y su almacenamiento se hacen desde un mismo punto, con lo que es más sencillo tener una “visión global” del conjunto del proceso.

Sin embargo, y como contrapartida, se ha de tener especial cuidado a la hora de organizar la secuencia de las copias en los distintos equipos del sistema, en orden a evitar posibles solapamientos que pudieran sobresaturar al servidor. Así mismo la carga que soportará la red se incrementa, debido que todos los datos de respaldo del sistema serán enviados al servidor, dato que hay que tener en cuenta en el caso de que se necesitara realizar las copias en horario laborable. Por último también ha de tenerse en cuenta el coste energético de la operación. El centralizar la copia de seguridad implica que, en el caso de realizarse fuera de horas de trabajo, generalmente por la noche, y suponiendo que la rutina de copia ejecutada en el servidor sea capaz de controlar este aspecto, los equipos no podrán ser apagados hasta que se haya finalizado el proceso, con el consiguiente aumento de costes tanto energéticos como de tiempo de uso y desgaste de los ordenadores.

Como resultado de estas consideraciones se opta, en el caso de la notaría, por la instalación en cada puesto de trabajo de un disco duro externo que albergará los volúmenes de copias. Esta opción, si bien tiene la desventaja de un seguimiento más laborioso debido a la dispersión de datos en distintos dispositivos que genera, proporciona varias ventajas que hacen de ella la idónea para la notaría:

- Permite personalizar el horario de copia del respaldo, posibilitando la opción de programarlo a una hora adecuada para cada caso y apagando el equipo en el mismo momento de su finalización.
- Los datos del volumen de respaldo se adaptan especialmente a cada usuario, permitiendo una reducción del tiempo de búsqueda en caso de necesidad.
- El riesgo de pérdida de datos debido a fallo en el dispositivo de almacenamiento se minimiza debido a que están repartidos y no centralizados en una única unidad.

En base a la decisión tomada se instalará en cada equipo de la notaría, incluido el servidor, unidades de disco duro externas, con conexión USB, de suficiente capacidad para al almacenar los datos de respaldo[38].

Una vez alcanzado se han recabado y almacenado toda la información necesaria para poder hacer frente a un episodio de desastre, se ha alcanzado el objetivo de conocer qué datos se han de incluir en las copias de respaldo y se ha decidido que procedimiento se va a seguir en lo relativo a la ubicación de los volúmenes de respaldo, el siguiente paso consiste en diseñar la programación de dichas copias.

Teniendo como referencia las tablas obtenidas en el paso correspondiente a qué datos copiar y los distintos modelos de copias, se llega a la conclusión que se utilizarán dos

[38] Por motivos de sencillez, todas las unidades de disco duro externo instaladas tendrán como letra de unidad “H”.

tipos distintos de programaciones, uno para el servidor y otro para el resto de equipos de la notaría.

9.4.2 PROGRAMACIÓN EN PUESTOS DE TRABAJO

Se puede observar el las tablas obtenidas en el paso dedicado a qué datos copiar, que en todos los puestos de trabajo la configuración de las carpetas de datos, su tamaño, e índice de cambio, son similares, por lo que se puede aplicar una misma política de copias de seguridad para todos ellos.

Se puede observar que el único dato que tiene un tamaño considerado grande se corresponde al correo electrónico. La carpeta en la que se almacena el correo electrónico, suele estar formada, en el caso del Outlook Express, por distintos archivos correspondientes a las bandejas virtuales que utiliza la aplicación para la gestión de los correos electrónicos: entrada, salida, enviados, eliminados, borradores y sus correspondientes copias. Una modificación, por pequeña que sea, en uno de esos archivos implica un respaldo completo del mismo, por lo que virtualmente no se obtiene ninguna diferencia, en cuanto a mejora de tiempo de respaldo, en la utilización de copias incrementales o diferenciales.

Teniendo esto en cuenta se opta por la separación de los datos a respaldar mediante la programación de dos tareas distintas, una correspondiente al correo electrónico y su agenda asociada y otra correspondiente al resto de datos.

En el caso del correo electrónico se utilizará una programación del tipo 3, expuesto en el apartado dedicado a los distintos modelos de programación de copias de seguridad, consistente en la realización de una copia de seguridad total de los datos un día de la semana, en este caso el viernes, con lo que se recogerán todos los datos generados a lo largo de la semana, y una copia incremental el resto de días. La siguiente imagen muestra gráficamente el proceso.

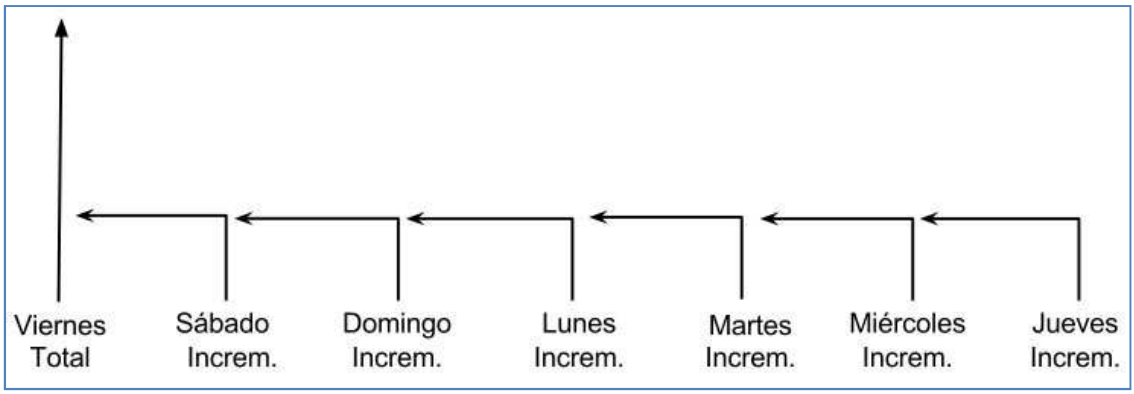


Ilustración 31. Programación puestos de trabajo. Correo electrónico.

Dicha copia será almacenada en una carpeta del nuevo disco duro instalado (H), y llevará por nombre "*Copia_Seguridad_Correo*".

Para el resto de datos, se opta por una programación del tipo 2, similar a la anterior pero con la diferencia de que las copias diarias serán diferenciales.

El tamaño pequeño – medio de los datos hacen que la elección de copias diferenciales no suponga un problema en cuanto al tamaño acumulativo de las mismas. Por otro la utilización de copias diferenciales facilita sensiblemente la tarea de reconstrucción de los datos en caso de desastre. La imagen siguiente refleja la opción adoptada.

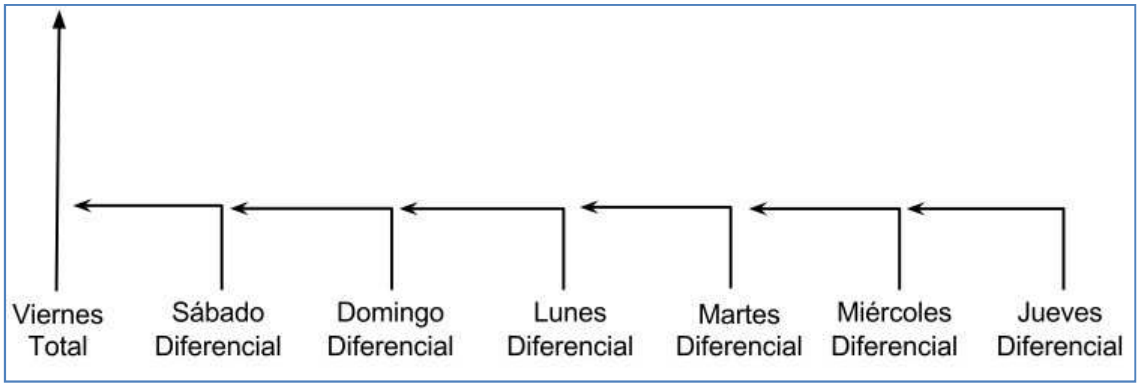


Ilustración 32. Programación puestos de trabajo. Datos.

El respaldo resultante será almacenado en una carpeta del disco duro externo (H), y se denominará "*Copia_Seguridad_Datos*".

Se ha de procurar que la secuencia de las copias se produzca de tal manera que no se solapen, por este motivo, y teniendo en cuenta que los usuarios, en circunstancias normales, han dejado de utilizar los equipos a las 21:00 horas, se programará la primera copia correspondiente al correo electrónico, a esa misma hora. La segunda copia, la correspondiente al resto de datos, se programará para que comience dos horas después, a las 23:00 horas.

Finalmente se ha de tener en cuenta que se ha de programar el script necesario para que los equipos se apaguen al terminar el proceso de copia, en el caso de utilizar software de copias de seguridad, asegurarse que permite este tipo de acción y utilizarla adecuadamente.

9.4.3 PROGRAMACIÓN EN EL SERVIDOR

En el servidor confluyen los datos finales del trabajo desarrollado en la totalidad de la notaría. Su carácter aglutinador hace que se deba tener especial cuidado a la hora de programar las tares de copias de respaldo. Por ese motivo y por el carácter bien diferenciado de los datos que alberga: bases de datos de gestión y base de datos de protocolo electrónico (además de otro tipo de archivos de menos transcendencia pero así mismo importantes), se opta por la separación del proceso de copia en cuatro tareas distintas, una para cada tipo de dato.

La separación en tareas diferenciadas permitirá no solo aplicar la política de copias adecuada para cada caso, sino que facilitará el seguimiento de cada una de ellas por separado y proporcionará autonomía entre los distintos tipos de datos a la hora de ser necesaria una reconstrucción total o parcial de los mismos. Por ejemplo en el caso de que sea necesite la reconstrucción del protocolo electrónico, no será necesario volcar además las bases de datos de gestión o viceversa.

Por lo tanto se programarán cuatro tareas de respaldo distintas correspondientes cada una de ellas a: gestión, protocolo, agenda y configuraciones.

9.4.3.1 PROGRAMACIÓN DEL RESPALDO DE GESTIÓN

Según la información facilitada por la empresa suministradora del software de gestión de la notaría, la aplicación realiza copias seguras de sus bases de datos y las almacena en una carpeta, ubicada del disco duro externo del servidor (E), denominada *Copia Gestion*. Dicha copia se realiza a las 00: 00 horas todos los días de la semana. La carpeta contiene a su vez tantas subcarpetas como días de la semana, y en cada una de las subcarpetas la copia de las bases de datos del día correspondiente.

Como se puede observar en las tablas que contienen qué datos copiar, las copias de bases de datos de gestión cambian diariamente y son de tamaño grande, por lo que la programación de sus archivos de respaldo ha de recoger dichos cambios diarios

Por lo tanto, la copia de seguridad se realizará de esa carpeta y será ubicada en otra del nuevo disco duro externo instalado (H), a la que se dará el nombre de "*Copia_Seguridad_Gestion*".

El modelo de copia de seguridad elegido será del tipo 3, consistente en la realización de una copia total el domingo, y copias incrementales el resto de días de la semana.

Se ha optado por las copias incrementales debido a que la carpeta de copias contiene subcarpetas con los respaldos de todos los días de la semana. Si se eligiera un tipo de copia diferencial, cada día se irían acumulando los datos de toda la semana, cuando en realidad únicamente ha cambiado la subcarpeta correspondiente a un día en concreto, incrementando en exceso el volumen de la copia.

La siguiente imagen muestra gráficamente el proceso de copia.

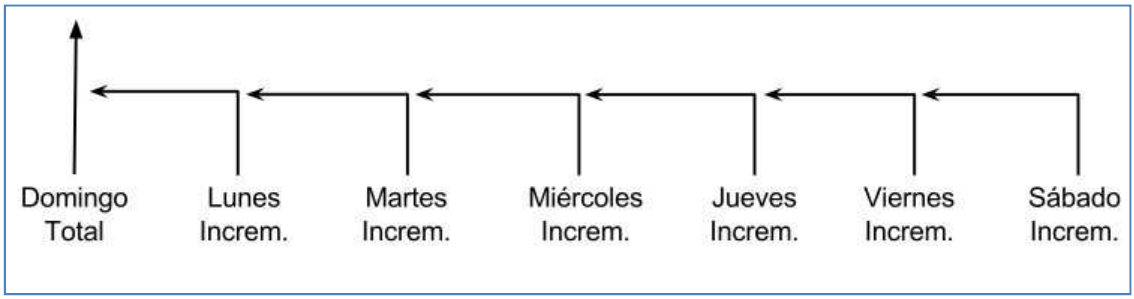


Ilustración 33. Programación de los datos de gestión.

9.4.3.2 PROGRAMACIÓN DEL RESPALDO DE PROTOCOLO

Como ya se ha comentado anteriormente, el protocolo electrónico se almacena en una carpeta del disco G del servidor denominada "*Protocolo*". Contiene todo el protocolo electrónico del notario. Dicha carpeta está constituida por un conjunto de subcarpetas, una por año, que contiene cada una de ellas el protocolo electrónico correspondiente a dicho año. La carpeta cambia diariamente y su volumen aumenta cada día, siendo actualmente de unos 5 GB.

Por lo tanto la copia de seguridad se realzará de dicha carpeta "Protocolo" y será almacenada en otra del disco duro H, denominada "*Copia_Seguridad_Protocolo"*.

Debido a que la carpeta protocolo contiene subcarpetas con años anteriores de datos, y que únicamente se realizan cambios en la carpeta correspondiente al año en curso, la elección del modelo de copias de seguridad pasa por utilizar copias incrementales o diferenciales, que únicamente respaldarán los cambios realizados cada día.

Si bien los datos cambian diariamente, al tratarse de documentos de Microsoft Word, el volumen de datos diario que ha cambiado o creado, no es grande, al contrario de lo que ocurría con las copias de las bases de datos, por lo que la acumulación de datos que originan las copias diferenciales no supone un problema de espacio ni de tiempo de copia o utilización de recursos. Por ese motivo se optará por una programación de copias de seguridad basada en copias diferenciales.

Como consecuencia se opta por una programación del tipo 2, consistente en una copia total el domingo en conjunción con copias diferenciales el resto de días de la semana.

La siguiente imagen ilustra la programación de copias de seguridad decidida.

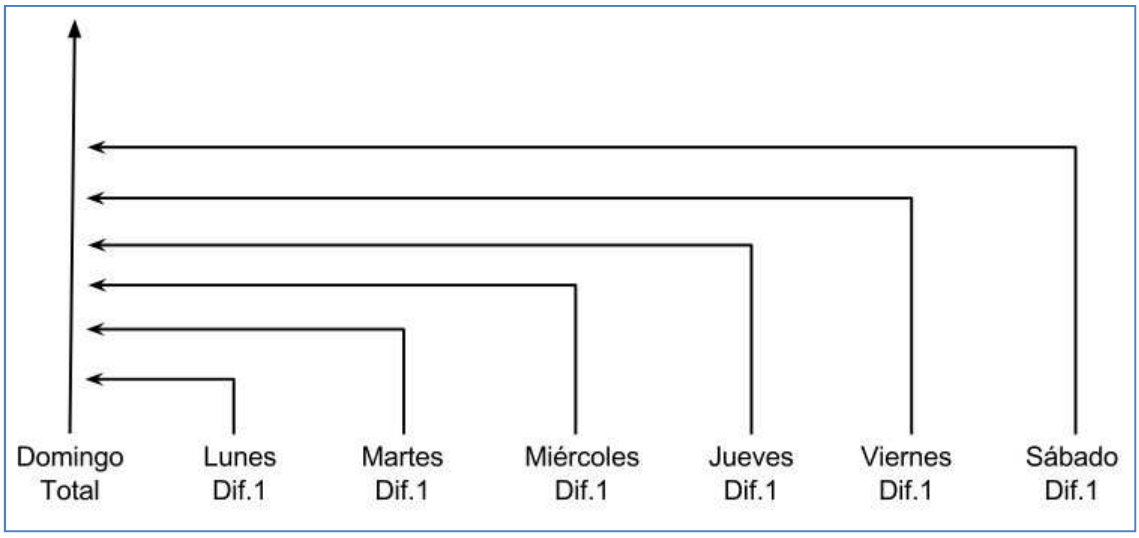


Ilustración 34. Programación de la copia de Protocolo.

La programación decidida permitirá, por un lado una restauración total en caso de desastre y por otro restauraciones parciales rápidas ya que las copias diferenciales, al ser acumulativas, permiten un respaldo rápido de los datos diarios.

9.4.3.3 PROGRAMACIÓN DEL RESPALDO DE AGENDA

Los archivos de la agenda de citas de la notaría se almacenan en un la carpeta "Agenda" del disco G del servidor, son de tamaño pequeño y cambian diariamente.

La copia de respaldo se realizará de dicha carpeta "Agenda" y se almacenará en otra denominada "Copia_Agenda" que se ubicará en el disco duro externo H.

Si bien, como se ha comentado, los datos que contiene la carpeta en cuestión cambian diariamente, su tamaño es lo suficientemente pequeño como para que no suponga un problema de ningún tipo la realización de copias totales diarias de la misma.

Por lo tanto se realizará una programación del tipo 1, basada en copias de seguridad diarias totales de dicha carpeta "Agenda".

La siguiente imagen ilustra el proceso de copias de seguridad que se llevara a cabo.

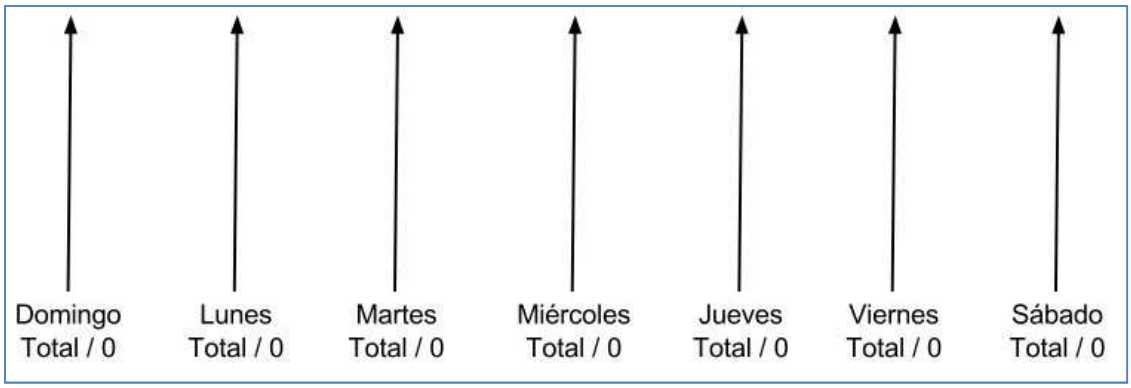


Ilustración 35. Programación de copias de seguridad de la agenda de la notaría.

Las copias de seguridad totales diarias, ofrecen completa seguridad en caso de desastre y permiten reconstrucciones rápidas de los datos respaldados.

9.4.3.4 PROGRAMACIÓN DEL RESPALDO DE CONFIGURACIONES

La carpeta *Configuraciones* contiene los datos que se han ido recabando en el proceso de documentación del sistema de la notaría. Más concretamente contiene datos relativos a:

- Configuraciones de red de los equipos e impresoras de la notaría.
- Listado de nombres de usuario, contraseñas y nombres de equipo de la notaría.
- Informes de hardware de los equipos.
- Informes de particiones de los discos de los equipos.
- Listado de usuarios del servidor.

Esta información además de figurar en archivos de pequeño tamaño, raramente cambia en el tiempo, por lo que no será necesario hacer copias diarias de la misma. En lugar, de ello será suficiente con la realización una vez por semana, de una copia simple total de la información.

9.4.3.5 SECUENCIA

La secuencia de las copias de seguridad en el servidor se ha de hacer teniendo en cuenta los datos que componen cada una de las tareas programadas, prestando especial atención en el tiempo que el sistema necesitará para realizar cada una de ellas.

Se comenzará la primera de las tareas a las 01:00 horas y se dejará un lapso de tiempo suficiente entre ellas con el fin de evitar que se solapen unas a otras. La secuencia de realización de las copias será la que refleja la siguiente tabla.

Tarea	Hora inicio	Periodicidad
Respaldo Datos Gestión	02:00	Diaria
Respaldo Datos Protocolo	05:00	Diaria
Respaldo Datos Agenda	07:00	Diaria
Respaldo Datos Configuración	07:30	Semanal

9.4.3.6 ELECCIÓN DEL SOFTWARE A UTILIZAR

Debido a la amplia oferta que existe en el mercado de aplicaciones, tanto gratuitas como comerciales, especializadas en la gestión de copias de seguridad, se ha desechado la opción de crear una aplicación desde cero, optado por la utilización de una de ellas, y especialmente, por motivos de ahorro de costes, por una de código abierto.

Existen numerosas aplicaciones de uso gratuito especializadas en copias de seguridad de reconocida calidad. Se ha incluido en el anexo IV una relación de los seis más utilizados a nivel empresarial. Para cada uno de ellos se ha incluido una breve explicación de sus características más importantes. Tras haber cotejado las características de cada uno de ellos, se ha llegado a la conclusión de que el que mejor se ajusta a las características de la notaría es la aplicación Cobian Backup 11 (Gravity), el cual se puede descargar de forma gratuita desde la dirección *http://www.cobiansoft.com/cobianbackup.htm*.

Las principales razones por las que se ha elegido esta aplicación son principalmente:

- Es gratuita.
- Es ligera. Apenas consume recursos del sistema.
- Dispone de todas las modalidades de copias de seguridad que se necesitan en este caso (total, incremental y diferencial).
- Está especialmente diseñada para trabajar en sistemas en los que no se van a utilizar copias de seguridad que impliquen almacenamientos vía internet.

- Posibilita la utilización de scripts ya predefinidos que permitirán apagar los equipos tras la realización de la copia.
- Totalmente traducida (tanto español como catalán)

Las principales características de la aplicación se pueden encontrar, como se ha comentado, en el anexo IV del presente trabajo, por lo que en este momento no se redundará en dicha cuestión. Sin embargo, y dado que es la aplicación que se ha elegido para gestionar las copias de seguridad de la notaría, a continuación se describirá tanto el proceso de instalación, como el de configuración de las distintas tareas de respaldo.

9.4.3.6.1 Instalación de Cobian Backup 11 (Gravity)

Tras descargar y ejecutar el archivo de instalación desde la dirección electrónica *http://www.cobiansoft.com/cobianbackup.htm*, se procederá a elegir los parámetros de instalación.

1. Elección del idioma y aceptación de los términos de uso.
2. Elección de la carpeta de instalación, creación de un script para instalaciones automáticas e instalación del solicitante de Volume Shadow Copy.

   En este punto se aceptará la carpeta de instalación por defecto y se desmarcarán las opciones de creación del script y la instalación del solicitante de Volume Shadow Copy[39].

[39] Shadow Copy permite respaldar ficheros en uso sin necesidad de cerrar el programa que los utiliza. Esto se consigue mediante la utilización de la tecnología Volume Shadow Services en Windows XP y posteriores versiones.

Ilustración 36. Instalación de Cobian Backup 11. Carpeta de instalación.

3. Elección del Tipo de instalación.

Ilustración 37. Instalación de Cobian Backup 11. Tipo de instalación.

La aplicación ofrece distintos tipos de instalaciones:

- *Aplicación (sin auto-inicio)*: se instalará el sistema como aplicación pero no será iniciado automáticamente al iniciar el sistema.
- *Aplicación (auto-inicio para usuario actual)*: se instalará el programa como aplicación y se iniciará automáticamente solo en el caso del usuario actual.

- *Aplicación (Auto-inicio para todos)*: se instalará el programa como aplicación y se iniciará automáticamente sin importar qué usuario ha iniciado la sesión.
- *Como un servicio*: instalará el programa como un servicio de Windows. Si se ha elegido esta opción se habrá de decidir entre dos modalidades:
    - *Usar cuenta de Sistema local*: cuanta como usuario local del sistema. Dependiendo del caso, podrían no tenerse acceso a la red.
    - *Usar cuenta normal*: Utilizar cuanta normal para ejecutar el servicio, en cuyo caso se debe suministrar tanto usuario como contraseña de la cuenta.

En el caso de la notaría será suficiente con que se **active la opción *Aplicación (Auto-inicio para todos)***.

4. Comienzo de la instalación.

   Una vez finalizada la instalación es posible comenzar la configuración de las distintas tareas de respaldo de los datos de la notaría.

9.4.3.6.2 Configuración de las tareas de respaldo en los puestos de trabajo

Se realizará como ejemplo la programación de las tareas de respaldo del Gestor, teniendo en cuenta que en el resto de puestos de trabajo el procedimiento es el mismo, la única diferencia radicará en la elección de las carpetas a respaldar en cada caso, pudiéndose mantener los mismos horarios y unidades.

La programación de las copias de seguridad en los puestos de trabajo mediante Cobian Backup es bastante sencilla gracias a su intuitiva interfaz. Antes de comenzar la programación de la copia es preciso tener claro determinados aspectos, que, por otro lado ya se han decidido con anterioridad:

- Cuántas tareas serán necesarias
- Qué datos se van a respaldar.
- Donde se encuentran.
- En qué unidad y carpeta se ubicarán las copias.
- Qué modelo de copias se utilizará.

- En qué horario se hará la copia.
- La necesidad o no de apagar el equipo tras la finalización del respaldo.

Teniendo los anteriores datos en cuenta se procederá a configurar las tares de respaldo, que deberán ser fieles a las decisiones tomadas en fases anteriores de la planificación de la política de copias de seguridad de la notaría.

Respondiendo a la primera cuestión, como ya se decidió anteriormente, serán necesarias dos tares de respaldo, una para el correo electrónico y otra para el resto de datos.

9.4.3.6.2.1 Programación del respaldo del correo electrónico

Se ha de recordar que se persigue programar una tarea de copia de seguridad basada en la realización de una copia total semanal junto a copias incrementales diarias.

9.4.3.6.2.1.1 Pestaña General

El primer paso consiste en fijar los parámetros generales de la tarea, para lo cual, a través de la pestaña ***General***, se fijará tanto el nombre de la tarea, como del tipo de respaldo.

- *Nombre de la tarea*: Copia_Seguridad_Correo.
- *Tipo de respaldo*: Incremental. En otro punto de la configuración se indicará a la aplicación en qué momento se desea una copia total de los datos.
- *Uso de Volume Shadow Copy*: desactivado.

El resto de opciones pueden quedarse según la configuración que por defecto ofrece la aplicación. La imagen siguiente muestra la ventana con las opciones adecuadas.

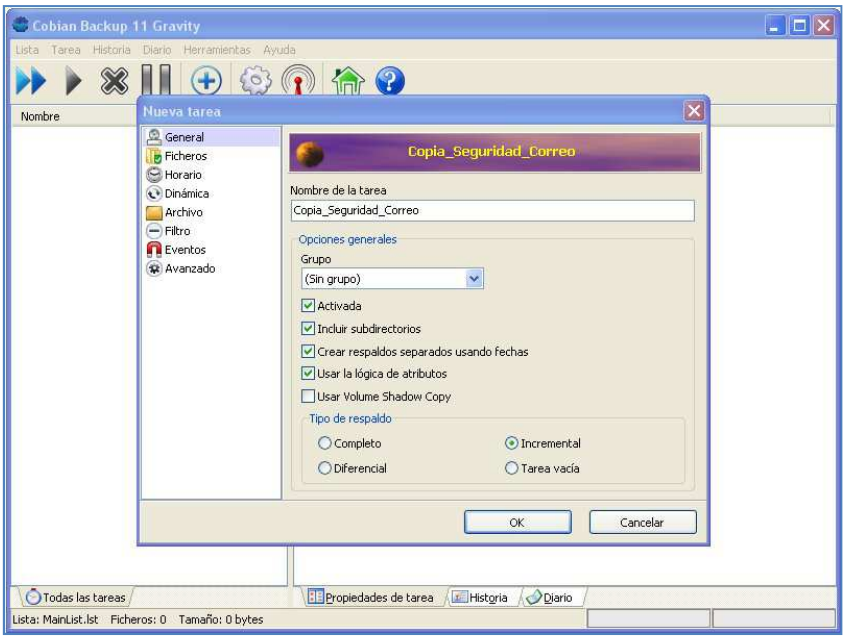


Ilustración 38. Configuración de Cobian Backup 11. Correo - Parámetros generales.

9.4.3.6.2.1.2 Pestaña Ficheros

A continuación, a través de la pestaña ***Ficheros***, se deberán especificar las carpetas que se desean respaldar y la carpeta de destino de dichos respaldos. En el caso actual, se deberán seleccionar tanto la carpeta que contiene los archivos de correos electrónicos como la que contiene la libreta de direcciones, es decir:

- Correo electrónico: *F:\Correo Gestor*
- Libreta de direcciones de contactos: *C:\Documents and Settings\gestor\Datos de programa\Microsoft\Address Book*

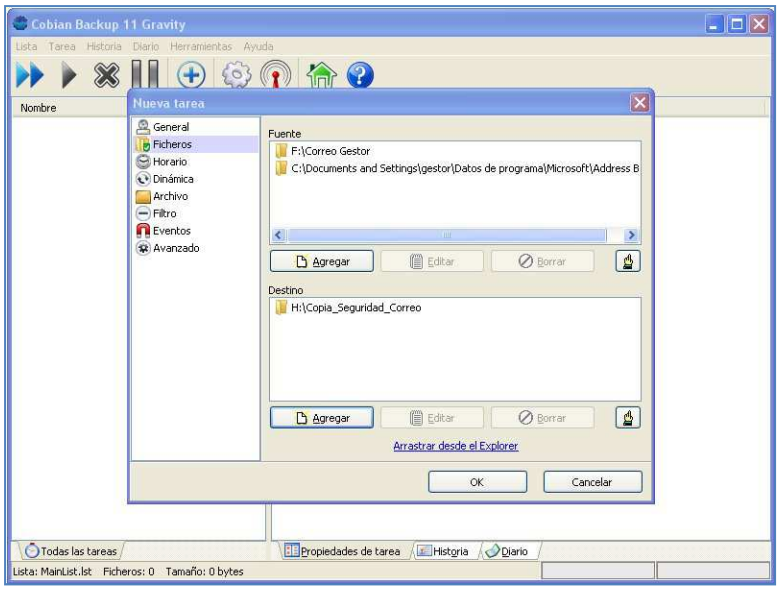


Ilustración 39. Configuración de Cobian Backup 11. Correo - Ficheros de respaldo

9.4.3.6.2.1.3 Pestaña Horario

A continuación se deberá especificar qué días de la semana se va a realizar la copia de seguridad y a qué hora comenzará el proceso.

Teniendo en cuenta el horario de trabajo de la notaría se toma las siguientes decisiones:

- *Tipo de horario*: semanal, todos los días de la semana de lunes a viernes, ya que los equipos permanecerán desconectados el sábado y el domingo.
- *Hora*: 21:30.

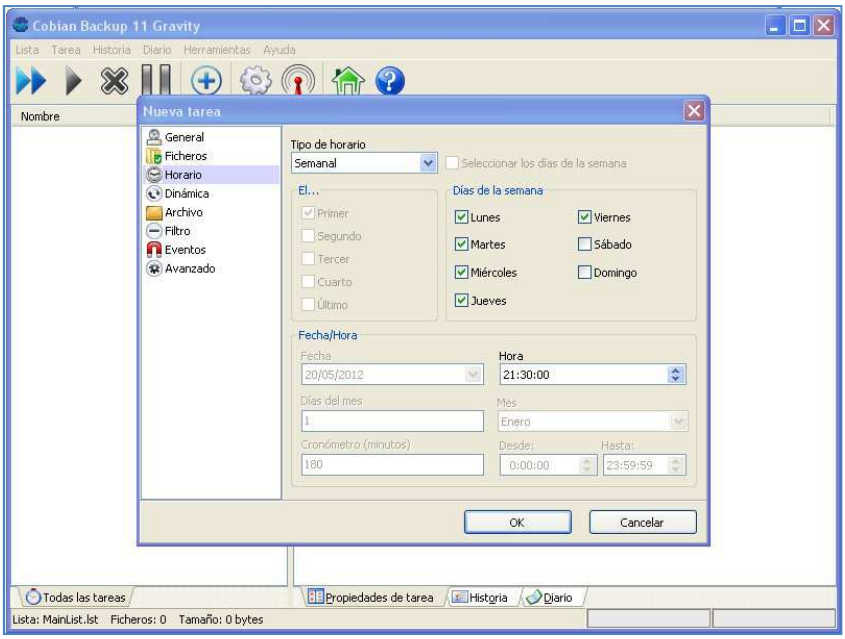


Ilustración 40. Configuración de Cobian Backup 11. Correo - Horario de copias.

9.4.3.6.2.1.4 Pestaña Dinámica

En la pestaña dinámica se especificará el número de copias completas que se desea almacenar, así como el día que se requiere se realicen dichas copias completas. Con arreglo a las decisiones tomadas en anteriores secciones, las opciones que se deben especificar son las siguientes:

- *Prioridad*: normal.
- *Copias completas a guardar*: 2. Por seguridad se ha optado por almacenar más de una copia completa de los datos.
- *Día de la semana que se realizarán las copias completas*: viernes.

En la imagen que a continuación figura se puede apreciar las opciones elegidas de la ventana *Dinámica*.

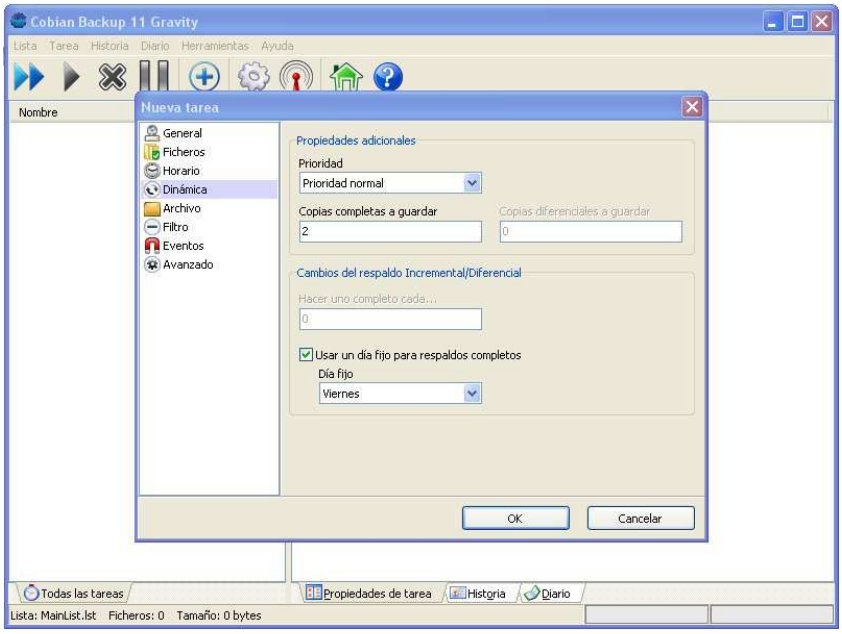


Ilustración 41. Configuración de Cobian Backup 11.Correo - Dinámica.

9.4.3.6.2.1.5 Pestaña Archivo

En la ventana correspondiente a la pestaña archivo, se ha de indicar si las copias deberán ser comprimidas y cifradas.

Teniendo en cuenta los medios de almacenamiento actuales, se han instalado discos duros con la suficiente capacidad como para que no sea necesario, a priori, realizar ningún tipo de compresión a los datos de respaldo.

Al tratarse de copias ubicadas en discos duros externos, que siempre han de estar conectados a los equipos que respaldan, el cifrado de datos en fundamental en orden a conseguir la mayor seguridad posible. Por esa razón se ha decidido utilizar un cifrado de 192 bits, suficiente para el contexto actual, con una contraseña de cifrado de 10 caracteres (cifras, letras y caracteres especiales), que se consensuará con algún responsable de la seguridad notaría.

Por cuestiones obvias de seguridad, dicha contraseña en ningún momento ha de ser conocida por ninguna persona ajena a la notaría. Idealmente, lo más seguro sería que únicamente la conociera el responsable de la notaría anteriormente indicado[40], siendo desconocida para el resto de usuarios del sistema.

[40] Es error habitual el compartir de manera irresponsable determinada información confidencial que los usuarios no tienen por qué conocer. Únicamente los responsables de seguridad de las empresas deben conocer las contraseñas de cifrado de los datos.

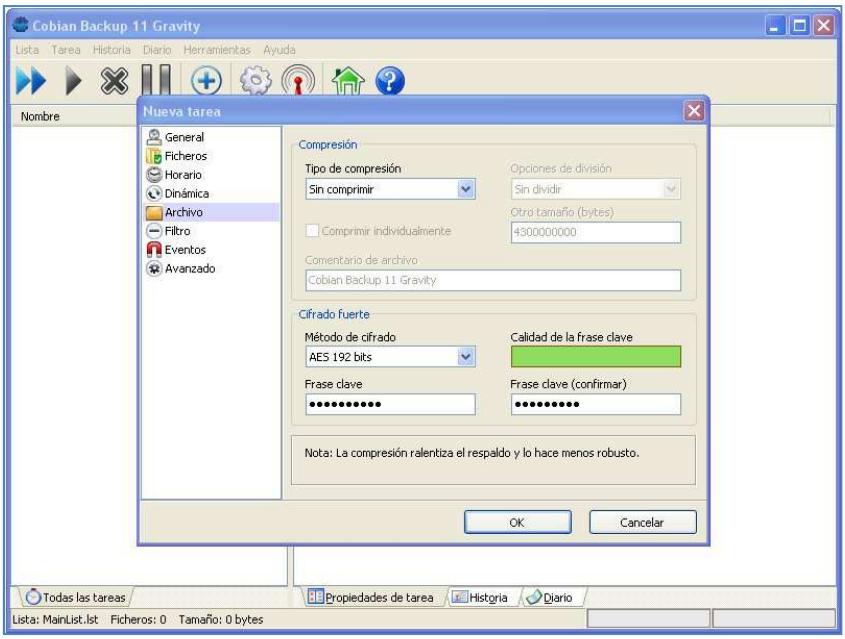


Ilustración 42. Configuración de Cobian Backup 11. Correo - Archivo.

En principio, el resto de opciones de configuración no es necesario que sean modificadas. La tarea de respaldo para el correo electrónico del gestor queda de esta manera finalizada.

9.4.3.6.2.2 Programación del respaldo del resto de datos

Tras haber configurado la tarea de respaldo de los datos correspondientes al correo electrónico, se procederá a programar la correspondiente al resto de datos del gestor de la notaría.

Se ha de recordar que se persigue programar una tarea de copia de seguridad basada en la realización de una copia total semanal junto a copias incrementales diarias.

El proceso a seguir es idéntico al anterior, con la única diferencia de que en determinadas momentos se elegirán otro tipo de opciones acordes con las decisiones tomadas en fases anteriores.

9.4.3.6.2.2.1 Pestaña General

En la ventana correspondiente a la pestaña correspondiente a la pestaña general se deberán especificar los siguientes parámetros:

- Nombre de la tarea: Copia_Seguridad_Datos.

- Tipo de respaldo: Diferencial. En otro punto de la configuración se indicará a la aplicación en qué momento se desea una copia total de los datos.
- Uso de Volume Shadow Copy: desactivado.

El resto de parámetros no se ven alterados.

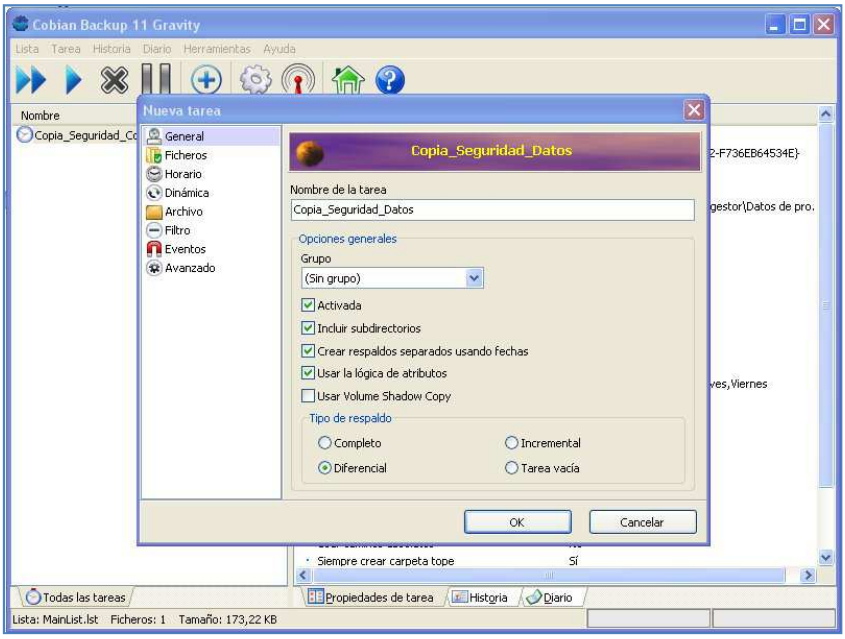


Ilustración 43. Configuración de Cobian Backup 11. Datos - General.

9.4.3.6.2.2.2 Pestaña Ficheros

Al igual que en el caso del respaldo del correo, a continuación, a través de la pestaña ***Ficheros***, se deberán especificar las carpetas que se desean respaldar y la carpeta de destino de dichos respaldos. En este caso:

- Documentos (*.xls y *.doc): *F:\Cartas*.
- Carpeta Mis Documentos: *C:\Documents and Settings\gestor\Mis documentos*.
- Favoritos de internet: *C:\Documents and Settings\gestor\Favoritos*.

La imagen siguiente muestra las carpetas seleccionadas.

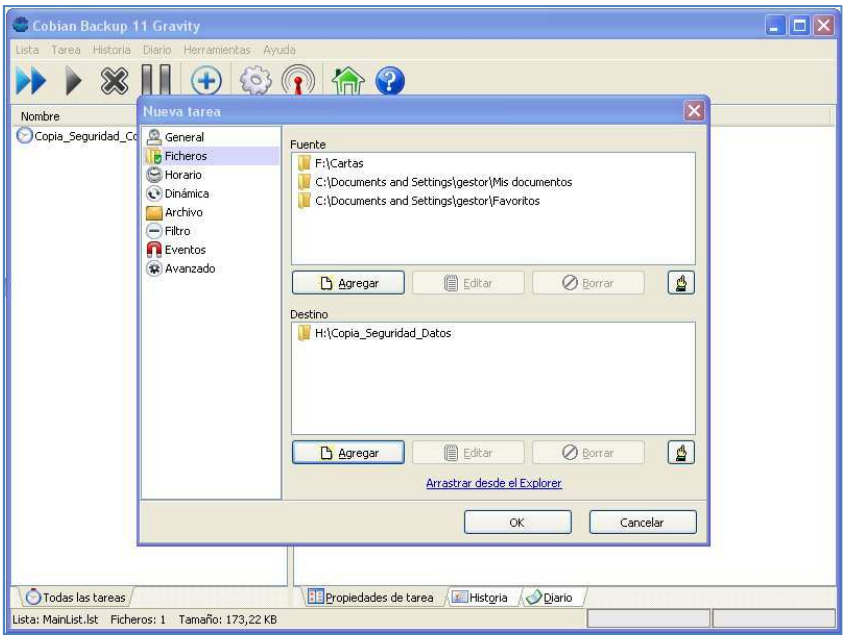


Ilustración 44. Configuración de Cobian Backup 11. Datos - Ficheros.

9.4.3.6.2.2.3 Pestaña Horario

En el caso de determinar el horario de la copia de respaldo se ha de tener en cuenta que se ha programado la anterior tarea para que comience a las 21:30, por lo que se deberá indicar una hora de comienzo lo suficientemente separada de ella como para que no se produzca ningún tipo de solapamiento.

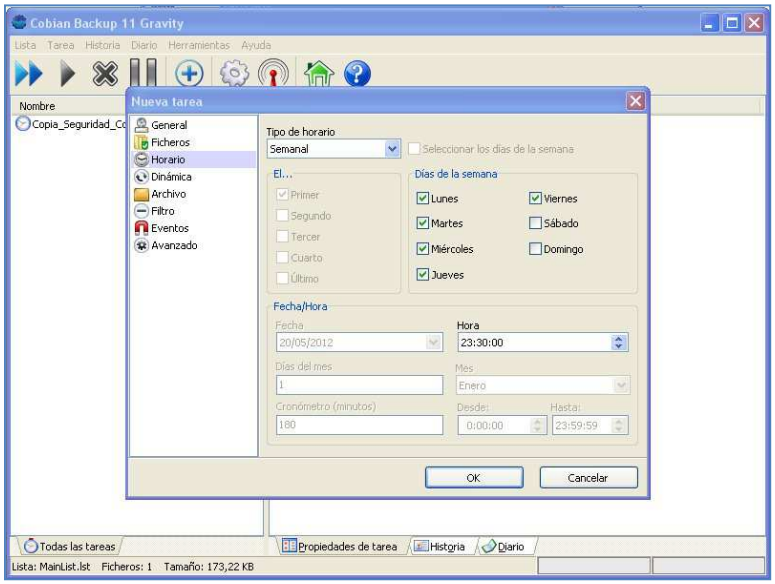


Ilustración 45. Configuración de Cobian Backup 11. Datos - Horario.

Teniendo en cuenta que las copias se van a efectuar cuando el usuario no se encuentra trabajando, el equipo no se encontrará realizando ningún otro trabajo que no sea el correspondiente a la copia. Por ese motivo es de suponer que la primera tarea de

copia programada trascurrido un periodo de dos horas habrá finalizado, por lo que se puede programar que la segunda tarea comience a realizarse a las 23:30 horas sin temor a que se produzcan solapamientos.

9.4.3.6.2.2.4 Pestaña Dinámica

En el respaldo del resto de datos, a diferencia del caso de la copiad el correo electrónico, se he de indicar el número de copias diferenciales que se desean guardar. El resto de los valores son los mismos que en la tarea anterior:

- *Prioridad*: normal.
- *Copias completas a guardar*: 2
- *Copias diferenciales a guardar*: 6. Se ha optado por almacenar una copia de seguridad diferencial para cada día de la semana.
- *Día de la semana que se realizará la copia total*: viernes.

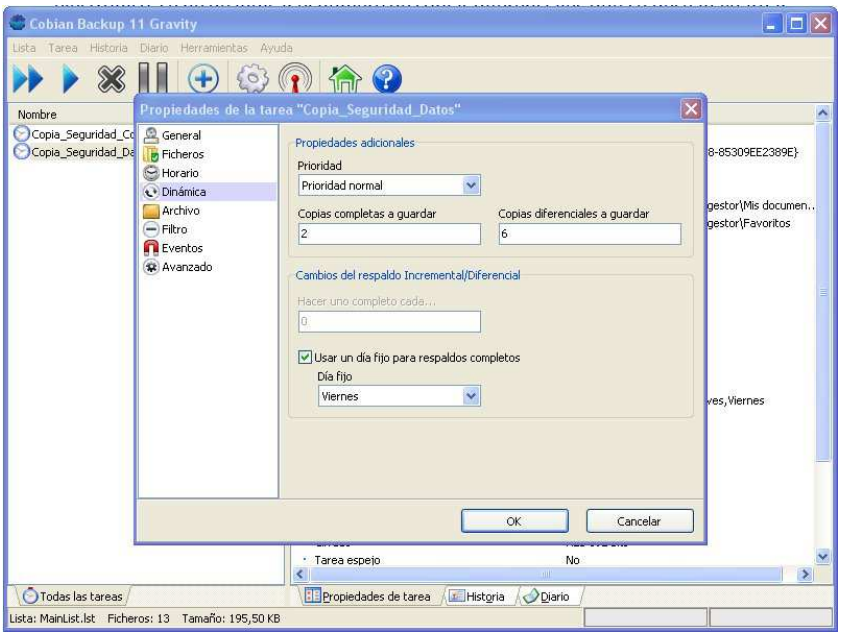


Ilustración 46 Configuración de Cobian Backup 11. Datos - Dinámica.

9.4.3.6.2.2.5 Pestaña Archivo

Las opciones y consideraciones correspondientes a la compresión y cifrado del respaldo permanecen inalteradas con respecto a la tarea anterior correspondiente a la

copia de seguridad del correo electrónico, por lo que no se ofrecerá ningún comentario más al respecto.

Como ejemplo se incluye la imagen de la ventana resultante, la cual refleja las opciones seleccionadas.

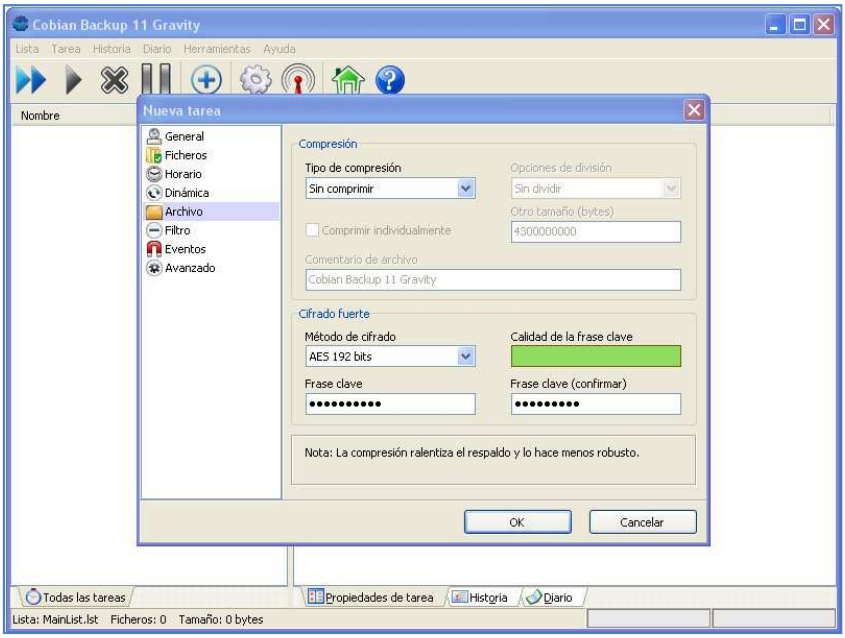


Ilustración 47 Configuración de Cobian Backup 11. Datos - Archivo.

9.4.3.6.2.2.6 Pestaña Eventos

En la ventana correspondiente a la pestaña eventos, se pueden especificar determinados acontecimientos que se desea se produzcan antes y/o después de la realización de la copia:

- Antes de la copia
    - Pausa.
    - Ejecutar una aplicación.
    - Ejecutar una aplicación y esperar.
    - Cerrar un programa.
    - Ejecutar un servicio.
    - Detener un servicio.
- Después de la copia

- Pausa.
- Ejecutar una aplicación.
- Ejecutar una aplicación y esperar.
- Cerrar un programa.
- Ejecutar un servicio.
- Detener un servicio.
- Iniciar una tarea.
- Suspender el equipo.
- Hibernar el equipo.
- Reiniciar el equipo.
- Apagar el equipo.

En el caso actual, se ha decidido que tras finalizarse la última tarea de copia de seguridad, la tarea que se está programando actualmente, se apague automáticamente el ordenador. Para ello se deberá agregar, en los eventos correspondientes a realizar tras la copia de seguridad, la correspondiente opción, tal y como se muestra en la siguiente imagen.

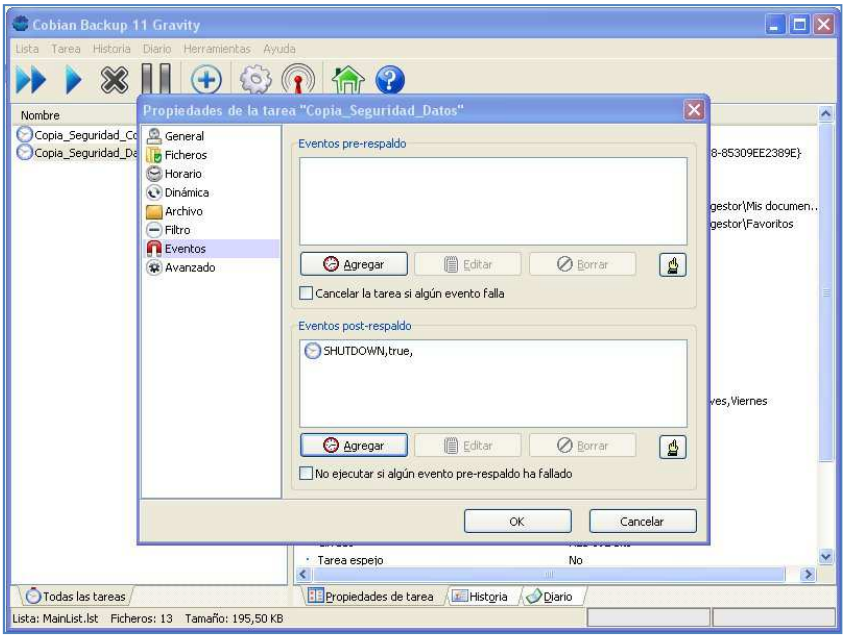


Ilustración 48. Configuración de Cobian Backup 11. Datos - Eventos.

Con la inclusión de esta opción se da por terminada la programación de la copia de respaldo de datos del gestor, y consecuentemente de las dos tareas de copias de seguridad que se había planeado programar para el usuario.

9.4.3.6.3 Configuración de las tareas de respaldo en el servidor

En primer lugar se ha de recordar las decisiones tomadas con respecto a la copia de seguridad de los datos del servidor:

- Se realizarán cuatro tareas de respaldo consecutivas, que siguen los siguientes horarios y periodicidades

Tarea	Hora inicio	Periodicidad
Respaldo Datos Gestión	02:00	Diaria
Respaldo Datos Protocolo	05:00	Diaria
Respaldo Datos Agenda	07:00	Diaria
Respaldo Datos Configuración	07:30	semanal

- Las copias de seguridad de cada tarea cumplen con las siguientes modalidades

Respaldo	Tipo	Modelo
Gestión	3	Total el domingo + incrementales el resto de días.
Protocolo	2	Total el domingo + diferenciales el resto de días.
Agenda	1	Totales diarias
Configuraciones	-	Total semanal

- Al tratarse del servidor ninguna en ninguna de las tareas ha de programarse el apagado de éste tras la finalización de la copia.

El procedimiento para programar las tareas de copias de seguridad de los datos del servidor coincide con los explicados anteriormente para los puestos de trabajo. Las diferencias, obviamente, radican en las diferentes opciones configuradas en cada caso en orden a que la tarea de respaldo correspondiente se ajuste a las necesidades planeadas.

A continuación se hará un recorrido por cada una de las pestañas de la aplicación necesarias para la correcta configuración de las tareas a programar. En cada una de

ellas se indicarán las opciones que se han de configurar para cada una de las cuatro tareas comentadas.

Únicamente se mostrarán aquellas opciones que deben ser modificadas con respecto al comportamiento por defecto de la aplicación.

9.4.3.6.3.1 Pestaña General

- **Respaldo Gestión:**
    - Nombre de tarea: Copia_Seguridad_Gestion.
    - Tipo de respaldo: incremental.
    - Usar Volume Shadow Copy: desmarcado.
- **Respaldo Protocolo**:
    - Nombre de tarea: Copia_Seguridad_Protocolo.
    - Tipo de respaldo: diferencial.
    - Usar Volume Shadow Copy: desmarcado.
- **Respaldo Agenda**:
    - Nombre de tarea: Copia_Seguridad_Agenda.
    - Tipo de respaldo: completo.
    - Usar Volume Shadow Copy: desmarcado.
- **Respaldo Configuraciones**:
    - Nombre de tarea: Copia_Seguridad_Configuraciones.
    - Tipo de respaldo: completo.
    - Usar Volume Shadow Copy: desmarcado.

9.4.3.6.3.2 Pestaña Ficheros

- **Respaldo Gestión:**
    - Fuente: E:\Copia Gestion.
    - Destino: H:\Copia_Gestion.

- **Respaldo Protocolo**:
    - Fuente: G:\Protocolo.
    - Destino: H:\Copia_Protocolo.
- **Respaldo Agenda**:
    - Fuente: G:\Agenda Notaria.
    - Destino: H:\Copia_Agenda.
- **Respaldo Configuraciones**:
    - Fuente: E:\Configuraciones
    - Destino: H:\Configuraciones

9.4.3.6.3.3 Pestaña Horario

- **Respaldo Gestión**:
    - Tipo de horario: diario. Seleccionando este tipo de horario se realizará la copia todos los días de la semana.
    - Hora: 02:00
- **Respaldo Protocolo**:
    - Tipo de horario: diario.
    - Hora: 05:00
- **Respaldo Agenda**:
    - Tipo de horario: diario.
    - Hora: 07:00
- **Respaldo Configuraciones**:
    - Tipo de horario: semanal
    - Día de la semana: marcar únicamente el lunes.
    - Hora: 07:30

9.4.3.6.3.4 Pestaña Dinámica

- **Respaldo Gestión:**
  - Prioridad: normal.
  - Copias Completas a guardar: 2
- **Respaldo Protocolo**:
  - Prioridad: normal.
  - Copias completas a guardar: 2
  - Copias diferenciales a guardar: 6
- **Respaldo Agenda**:
  - Prioridad: normal.
  - Copias completas a guardar: 2
- **Respaldo Configuraciones**:
  - Prioridad: normal.
  - Copias completas a guardar: 2

9.4.3.6.3.5 Pestaña Archivo

- **Respaldo Gestión:**
  - Tipo de compresión: sin comprimir.
  - Método de cifrado: AES de 192 Bits.
  - Frase clave: a consensuar con el encargado de seguridad de la notaría[41].
- **Respaldo Protocolo:**
  - Tipo de compresión: sin comprimir.
  - Método de cifrado: AES de 192 Bits.
  - Frase clave: a consensuar con el encargado de seguridad de la notaría.

[41] Si se desea un grado elevado de seguridad, es conveniente establecer una contraseña de cifrado distinta para las tres tareas principales: copia de gestión, copia de protocolo y copia de agenda.

- **Respaldo Agenda:**
    - Tipo de compresión: sin comprimir.
    - Método de cifrado: AES de 192 Bits.
    - Frase clave: a consensuar con el encargado de seguridad de la notaría.
- **Respaldo Configuraciones**:
    - Tipo de compresión: sin comprimir.
    - Método de cifrado: sin cifrar. La información contenida en la copia de respaldo de las configuraciones el sistema no es confidencial y por lo tanto se puede prescindir del proceso de cifrado.

Como se ha podido observar, la programación y configuración de las distintas tareas de respaldo mediante la utilización de la aplicación Cobian Backup 11 es del todo sencilla.

No obstante dispone de multitud de opciones que, por no haber sido necesarias, no se han utilizado. Si se desea consultar la documentación completa de la aplicación se puede hacer accediendo a la página *http://www.cobiansoft.com/index.htm*.

9.5 PROTECCIÓN DE LOS VOLÚMENES DE RESPALDO

Tras haber tomado la decisión acerca de qué datos de la notaría han de ser respaldados y haber decidido qué modelo de programación de copias de seguridad se va a aplicar en cada caso, es necesario planificar de qué manera se van a proteger los volúmenes de copias resultantes del proceso.

La política de copias de seguridad decidida para la notaría implica, como ya se ha comentado con anterioridad, la instalación de discos duros externos en cada puesto de trabajo que albergarán los volúmenes de respaldo, además se han programado las copias de seguridad de manera que no interfieran en el trabajo diario del empleado, por lo que se realizarán fuera del horario laboral forzando al apagado de los equipos tras su finalización. Consecuentemente los dispositivos de respaldo no pueden ser desconectados de los equipos y almacenados en lugar seguro al finalizar la jornada laboral, ya que no se realizaría la copia de seguridad.

Por consiguiente la seguridad de los volúmenes de respaldo únicamente se podrá garantizar mediante el cifrado de los datos y su duplicación y almacenamiento.

El cifrado de datos se ha conseguido mediante la utilización de la correspondiente utilidad ofrecida por el software de copias de seguridad con el que se han programado las copias. Concretamente se ha configurado el uso del algoritmo de cifrado AES 192 (algoritmo de ***Rijndael***).

En cuanto a la duplicación de datos, se tomarán las siguientes precauciones:

- Una vez al mes, se realizarán copias en soporte óptico (CD o DVD dependiendo del caso) de los archivos correspondientes a las copias totales de respaldo.
- Cada uno de los volúmenes obtenidos se etiquetarán con la siguiente información:
    - Fecha.
    - Hora.
    - Datos que contienen.
    - Tamaño.
    - Persona que efectúa el respaldo.
    - Persona a quién se entrega el respaldo.

- Una vez etiquetados, se entregará al notario o a la persona designada por él, quien los almacenará en una ubicación fuera de la notaría, tomando las medidas adecuadas que salvaguarden tanto su privacidad como su seguridad física.

9.6 PRUEBAS DE OPERATIVIDAD

El último paso en el establecimiento de la política de copias de seguridad de la notaría consiste en la programación de las pruebas de operatividad.

Debido a que por imperativo del notario no se puede interrumpir en ningún momento el trabajo en el despacho notarial, las pruebas de operatividad se han de realizar bien utilizando algún equipo lo más semejante posible a los utilizados por los usuarios, incluyendo un clon del servidor, o bien efectuándolas fuera del horario laboral de la notaría.

Las características de las que han de constar dichas pruebas, vienen especificadas en la sección correspondiente del capítulo dedicado a la metodología de copias de seguridad del presente trabajo. Como recordatorio a continuación se listan las principales:

- Realizar las pruebas de manera realista.
- Realizar pruebas de todo.
- Realizar pruebas de copias de distinto tipo.
- Tomar precauciones al realizar pruebas destructivas.
- Restaurar varios archivos.
- Restaurar el sistema de archivos.
- Simular volúmenes dañados.
- Comprobar la respuesta de la empresa de almacenamiento.
- En caso de respaldo de bases de datos.
    - Simular la restauración completa de la base de datos y comprobar que no se han perdido archivos.
    - Simular la restauración parcial de la base datos, restaurando únicamente determinados datos de la misma.
    - Restaurar la base de datos a partir de un punto concreto en el tiempo anterior a la fecha de la prueba.

10 ANEXOS

10.1 ANEXO I. REAL DECRETO 997/1999

Extracto[42] del *Real Decreto 997/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.*

BOE 13967

Artículo 3. Niveles de seguridad.

1. Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto.

2. Dichos niveles se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

Artículo 4. Aplicación de los niveles de seguridad.

1. Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.

2. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

3. los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.

[42] De los 29 artículos que componen el Real decreto 997/1999, se han incluido únicamente aquellos que se han considerado de interés manifiesto dentro del ámbito del presente trabajo.

Medidas de seguridad de nivel básico.

Artículo 13. Gestión de soportes.

1. Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenados en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

2. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero.

Artículo 14. Copias de respaldo y recuperación.

1. El responsable del fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos.

2. Los procedimientos establecidos para la recuperación de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en el que se encontraba al tiempo de producirse la pérdida o destrucción.

3. Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho periodo no se hubiera producido ninguna actualización de datos.

Medidas de seguridad de nivel medio.

Artículo 20. Gestión de soportes.

1. Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

3. Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él previamente a que se proceda a su baja en el inventario.

4. Cuando los soportes vayan a salir fuera de los locales en que se encuentran ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

Medidas de seguridad de nivel alto.

Artículo 25. Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de datos en un lugar diferente de aquel en que se encuentran los equipos informáticos que los tratan cumpliendo en todo caso las medidas de seguridad exigidas en este Reglamento.

10.2 ANEXO II. COPIAS DE SEGURIDAD CON POSTGRE SQL

Existen fundamentalmente tres métodos para realizar copias de seguridad de los datos en **Postgre SQL**: *SQL dump*, copias de seguridad a nivel de sistema de archivos y copias de seguridad en línea (PostgreSQL).

10.2.1 SQL DUMP

El método ***sql_dump*** genera un archivo de texto con instrucciones SQL que al ser suministradas al servidor, este recrea la base de datos en el mismo estado que estaba en el momento de la copia. Para este propósito Posrgre SQL proporciona la utilidad ***pg_dump***, que tiene como notación más básica: ***pg_dump nombre_bd > archivoSalida***, que devuelve el resultado por la salida estándar.

pg_dump es una aplicación cliente básica de Postgre SQL, lo cual significa que se puede ejecutar desde cualquier host remoto que tenga acceso a la base de datos. Como norma general, y para evitar errores debidos a falta de permisos de lectura o escritura, se deberá utilizar como *superusuario* de la base de datos.

Para especificar a qué servidor de base de datos se debe conectar ***pg_dump*** se han de utilizar las opciones de la línea de comandos ***-h*** (host) y ***-p*** (puerto). El host por defecto es el host local (local host) o aquel que especifique la variable de entorno ***PGHOST***.

Como cualquier otra aplicación cliente Postgr SQl, ***pg_dump*** conectará por defecto con el nombre de usuario de la base de datos que sea igual al usuario actual de la base de datos. Si es necesario sobrescribir este comportamiento, se puede hacer mediante dos vías distintas: especificando la opción ***-U*** o estableciendo la variable de entorno ***PGUSER***.

Las copias creadas con ***pg_dump*** son consistentes internamente, lo cual significa que cualquier actualización que se produzca en la base de datos mientras ***pg_dump*** se esté ejecutando no se reflejará en la copia. Este comportamiento es una consecuencia de que ***pg_dump*** no bloquee otras operaciones en la base de datos mientras se está ejecutando.

10.2.1.1 RESTAURAR LA COPIA

La copia puede ser restaurada mediante la orden ***psql nombre_bd < archivoEntrada***, donde *archivoEntrada* se corresponde con el obtenido al realizar la copia (*archivoSalida*).

La base de datos nombre_bd ha de ser creada previamente a la ejecución de la sentencia ***psql***, ya que esta no la crea.

psql posee las mismas opciones que ***pg_dump*** para controlar la localización del servidor de base de datos y el usuario. Una vez restaurada es conveniente ejecutar ***ANALYZE*** con fin a optimizarla. Una forma sencilla de realizar esta tarea es utilizar: ***vacuumdb -a -z,*** que actualiza todas las bases de datos.

Es posible, gracias a la posibilidad que poseen tanto ***pg_dump*** como ***psql*** de escribir y leer en pipes, realizar la transferencia de una base de datos entre servidores: ***pg_dump -h host1 nombre_bd | psql -h host2 nombre_bd***.

En el caso de realizar copias de seguridad de bases de datos de gran tamaño, es posible comprimirlas, para ello basta con utilizar ***pg_dump nombre_bd | gzip > nombreArchivo.gz***, para luego descomprimirlo con ***cat nombreArchivo.gz | gunzip | psql nombre_bd***.

También es posible seccionar la base de datos en porciones más manejables por el sistema de archivos de la máquina. Por ejemplo, para realizar porciones de 1 Mb, se puede utilizar: ***pg_dump nombre_bd | split -b 1m -nombreArchivo***, para luego unirlos con ***cat nombreArchivo* | psql nombre_bd***.

10.2.2 COPIA DE SEGURIDAD A NIVEL DE ARCHIVO

Una forma alternativa de crear la copia de seguridad consiste en hacer una copia directamente de los archivos que Postgre SQL utiliza para almacenar los datos, para ello se puede utilizar cualquier método estándar de copia de archivos. No obstante existen dos restricciones que se han de tener en cuenta:

1. El servidor de base de datos no puede estar funcionando.
2. La copia de seguridad realizada de esta manera solo será operativa en casos de restauraciones completas de clusters enteros de base de datos.

10.2.3 COPIA EN LÍNEA

En todo momento, Postgre SQl mantiene un archivo log, denominado WAL (*write ahead log*) en el subdirectorio *pg_xlog* del directorio de datos de clusters. El log describe cada cambio que se ha producido en los archivos de la base de datos. Si el sistema se cae, la base de datos puede ser restaurada consistentemente repitiendo las entradas del archivo log creadas desde el último punto correcto.

Por ese motivo la existencia del log hace posible el uso de una tercera estrategia para realizar copias de seguridad de bases de datos combinando el sistema de copias de seguridad basado en sistema de archivos con una copia de seguridad de los archivos ***WAL***. Si es necesaria una restauración, se restaura la copia de seguridad y seguidamente mediante la copia de los archivos ***WAL*** se retorna al momento actual. Este sistema es más complejo de administrar que los métodos anteriores pero ofrece significativos beneficios:

- No es necesario una copia de seguridad perfecta en consistencia como punto de partida. Cualquier inconsistencia interna será reparada mediante los archivos ***WAL***.
- Como es posible encadenar una secuencia indefinida de archivos WAL para ser reconstruidos, copias de seguridad continuas pueden conseguirse simplemente creando copias continuas de archivos ***WAL***.
- No es necesario reconstruir los archivos ***WAL*** hasta el final, sino que se puede interrumpir el proceso en cualquier momento deseado.
- Si continuamente se alimentan de series de archivos ***WAL*** otra máquina con la misma copia de seguridad base, se puede conseguir un sistema de replicado en caliente.

Como en el caso de las copias de seguridad basadas en el sistema de archivos, este tipo de copia únicamente soporta restauraciones de clusters enteros de bases de datos. De la misma manera, requiere grandes cantidades de capacidad de almacenamiento. Es la técnica de copias más utilizada en aquellas situaciones en las que lo importante es la fiabilidad de la copia.

Para realizar una restauración satisfactoria utilizando una copia en línea, es necesario una secuencia continua de archivos WAL que se extiendan hasta el punto de inicio seguro.

10.2.3.1 CONFIGURAR EL ARCHIVADO DE WAL

En un sentido abstracto, un sistema PostgreSQL en funcionamiento, produce una secuencia indefinida de archivos ***WAL*** grabados. El sistema divide físicamente esta secuencia en archivos ***WAL*** segmentados normalmente de 16Mb cada uno. A cada segmento de le asigna nombre numéricos que reflejan su posición en la secuencia WAL abstracta. Si no se utiliza el archivado ***WAL***, el sistema normalmente crea solo unos pocos segmentos y los recicla renombrando los que no son necesarios. Se asume que si un segmento cuyo contenido precede al último punto de control no será nunca más necesario y puede ser reciclado.

Cuando se archiva datos ***WAL***, se persigue capturar el contenido de cada archivo segmento cuando se llena y almacenar los datos antes de que el segmento sea reciclado para ser reutilizado. La forma de salvar esos datos depende de las aplicaciones o el hardware disponible. En este sentido PsotgreSQL no asume nada acerca del método que se utilizará para dicho almacenamiento, en lugar de eso permite al administrador especificar un comando que será ejecutado para copiar un segmento completo de archivo al lugar que se necesite.

Un ejemplo de comando simple puede ser:

```
archive_command = 'cp -i %p /mnt/server/archivedir/%f </dev/null'
```

10.2.4 REALIZACIÓN DE UNA COPIA DE SEGURIDAD BASE

El procedimiento para realizar una copia de seguridad base es relativamente simple y consta de los siguientes pasos secuenciales:

1. Asegurarse de que el archivado ***WAL*** está activado y funcionando.
2. Conectarse a la base de datos como superusuario y utilizar el comando ***SELECT pg_start_backup('etiqueta')***; en donde etiqueta es cualquier cadena para identificar unívocamente esta operación de copia de seguridad.

   pg_start_backup crea una archivo de copia de seguridad denominado etiqueta en el directorio cluster con información acerca de la copia.
3. Realizar la copia de seguridad, utilizando cualquier herramienta de copias de seguridad de sistema de archivos. Aunque no es imprescindible, no es necesario detener la normal ejecución de la base de datos durante la operación.
4. Conectarse de nuevo a la base de datos como superusuario y utilizar ***SELECT pg_stop_backup();***

10.3 ANEXO III. COPIAS DE SEGURIDAD CON MYSQL

Con MySQL se pueden realizar copias de seguridad fundamentalmente mediante cuatro procedimientos (Oracle, 2012):

- copiando los archivos de las tablas
- Copias de seguridad de archivos de texto delimitado
- Copias de seguridad con ***mysqldumo*** o ***mysqlhotcopy***
- Copias de seguridad incrementales activando el log binario

10.3.1 Realizar copias de seguridad copiando los archivos de las tablas

Para motores de almacenamiento que representan cada tabla utilizando sus propios archivos, las tablas pueden ser respaldadas copiando dichos archivos. Por ejemplo, las tablas de ***MylSAM*** son almacenadas como archivos, por lo que es fácil respaldarlas copiando los archivos ****.FRM***, ****.myd*** Y ****.myI***. Es importante que para conseguir una copia de seguridad consistente, se ha de para el servidor o bloquear y terminar todas las transacciones u operaciones pendientes (*flush*): ***LOCK TABLES lista_tablas READ; FLUSH TABLES lista_tablas;***

Únicamente es necesario un bloqueo de lectura; esto permite a otros clientes continuar con las consultas a las tablas mientras se está realizando la copia de seguridad de los archivos en el directorio de las bases de datos. La declaración *FLUSH TABLES* se necesita para tener la seguridad que todos índices de páginas activos son escritos en disco antes de que la copia de seguridad comience.

A continuación figura la sintaxis básica de la instrucción ***LOCK TABLES***:

```
LOCK TABLES
      tbl_name [[AS] alias] lock_type
       [, tbl_name [[AS] alias] lock_type] ...

lock_type:
      READ [LOCAL]
      | [LOW_PRIORITY] WRITE UNLOCK TABLES
```

Se puede crear una copia de seguridad binaria copiando todos los archivos de las tablas mientras el servidor no está actualizando nada. El script ***mysqlhotcopy*** utiliza

este método (se puede encontrar información completa de este script en la dirección *http://dev.mysql.com/doc/refman/5.1/en/mysqlhotcopy.html*

10.3.2 COPIAS DE SEGURIDAD DE ARCHIVOS DE TEXTO DELIMITADO

Para crear un archivo de texto que contenga los datos de la tabla, se puede utilizar la instrucción:

```
SELECT * INTO ARCHIVO_SALIDA 'nombre_archivo' FROM nombre_tabla.
```

El archivo se crea en host servidor de MySQL, no el cliente. Es importante tener en cuenta que el archivo de salida no debe existir ya que el otorgar permisos de sobrescritura constituye un riesgo de seguridad no asumible. Este método funciona con todos los tipos de datos, pero se ha de tener en cuenta que guarda únicamente los datos de las tablas en cuestión, no su estructura.

Otro método que permite crear archivos de texto de datos consiste en utilizar la sentencia **mysqldump** con la opción **--tab** (se puede encontrar detallada explicación de la utilización de la instrucción ***mysqldump*** en la dirección *http://dev.mysql.com/doc/refman/5.1/en/mysqldump-delimited-text.html*)

Para volcar los datos contenidos en un archivo de texto de datos, obtenido por los procedimientos anteriormente explicados, se puede utilizar tanto la sentencia ***LOAD DATA ARCHIVO_ENTADA*** o ***mysqlimport***

10.3.3 COPIAS DE SEGURIDAD CON MYSQLDUMO O MYSQLHOTCOPY

Se pueden realizar copias de seguridad con los scripts ***mysqldumo*** o ***mysqlhotcopy*****.**

El scritp ***mysqldumo*** tiene un carácter más general debido a que es capaz de realizar copia de seguridad de cualquier tipo de tablas. ***mysqlhotcopy*****,** por el contrario únicamente es capaz de trabajar con determinado tipo de motores.

Un archivo de copia generado por la instrucción ***mysqldump*** puede ser utilizado de varias maneras:

- Como copia de seguridad que permita recuperar los datos en caso de pérdida.
- Como una fuente de datos para realizar configuraciones de clonado.
    - Como una fuente de datos de experimentación:
    - Para realizar una copia de la base de datos que se puede utilizar sin hacer cambios en los datos originales.

- Para realizar pruebas de cualquier tipo.

mysqldump genera dos tipos de salidas, dependiendo de la utilización de la opción ***--tab***:

- Sin ***--tab***, ***mysqldump*** escribe instrucciones SQL en la salida estándar. Esta opción consiste en crear instrucciones CREATE para crear objetos copiados e instrucciones INSERT para cargar datos en tablas.
- Con ***--tab***, ***msqldump*** genera dos archivos de salida por cada tabla copiada

10.3.4 COPIAS DE SEGURIDAD INCREMENTALES ACTIVANDO EL LOG BINARIO

MySQL soporta copias de seguridad incrementales. Para ello se ha de arrancar el servidor con la opción ***log-bin*** para activar el log binario (se puede encontrar información detallada del log binario en la dirección *http://dev.mysql.com/doc/refman/5.1/en/binary-log.html*)

El archivo de log binario provee de la información necesaria para replicar cambios en la base de datos que se han producido posteriormente al punto de creación de una copia de seguridad.

En el momento de crear una copia incremental de seguridad se debe rotar el log binario usando ***FLUSH LOGS***. Una vez hecho es necesario copiar en la ubicación de la copia de seguridad todos los archivos log correspondientes desde la última copia de seguridad total o incremental menos uno. Estos archivos binarios de log son la copia incremental.

10.4 ANEXO IV. SOFTWARE LIBRE DE COPIAS DE SEGURIDAD

10.4.1 AMANDA

Página de la aplicación: *http://www.amanda.org/*

Páginas de descarga:

- *http://sourceforge.net/projects/amanda*
- *http://www.amanda.org/download.php*

Amanda (Advanced Maryland Automatic Network Disk Archiver), es una aplicación que permite la configuración de un servidor de un único servidor de copias de seguridad maestro para realzar respaldos en múltiples hosts de una red y almacenarlos en cintas magnéticas, discos duros o discos ópticos. Usa utilidades, y formatos nativos (dump, GNU tar, por ejemplo) y puede respaldar un número elevado de servidores y estaciones de trabajo que corran múltiples versiones de Linux o Unix. Amanda utiliza un cliente nativo de Windows para respaldar equipos y servidores que corran bajo Microsoft Windows.

Las características más importantes de la aplicación se pueden resumir en la siguiente lista:

- Está escrito en C y Perl.
- Su distribución es libre.
- Construido con los más altos estándares de software de respaldo: Unix dump / restore, GNU Tar, y otros.
- Realiza copias de seguridad en máquinas con Windows de 32 y 64 Bits.
- Es capaz de realizar el respaldo de múltiples máquinas en paralelo y volcarlos a un disco de almacenamiento. Una vez que la copia se ha completado, Amanda copia los respaldos finalizados uno a uno a una desde un dispositivo virtual a unidades de cinta magnética o discos.
- Mantiene un catálogo de los archivos copiados y de su localización en los medios de almacenamiento.
- Realiza Mantenimiento de cintas, es decir, nunca sobrescribirá una cinta incorrecta.

- En caso de restauración, facilita listados de las cintas necesarias y encuentra la imagen de copia adecuada para realizarla.
- Soporta comunicación segura entre el servidor y el cliente mediante la utilización de OpenSSH, permitiendo copias de seguridad seguras en un DMZ fuera de internet.
- Se pueden cifrar los archivos de copia tanto en el cliente como en el servidor utilizando GPG o cualquier otro programa de cifrado.
- Es capaz de comprimir los archivos de respaldo, antes de ser enviados o tras ser enviados por la red, con compress, gzip, u otro programa.
- Reporta los resultados en detalle, incluyendo en los informes todos los errores, vía email.
- Ofrece normalización de las copias de seguridad. Amanda programa automáticamente copias de seguridad completas o incrementales, promocionando el nivel de copia en caso necesario, de manera automática, en caso de que determine que es mejor para el resultado final.
- Incluye un programa de chequeo pre-tarea, que reporta vía email los posibles problemas que pudieran ocasionar que el proceso de copia fallara.
- Es compatible con IPv6.
- Expande las cintas magnéticas. Si una copia de seguridad es demasiado grande para ser albergada en una determinada cinta magnética, la aplicación la seccionará y la volcará en múltiples cintas automáticamente.

10.4.2 BACKUP PC

Página de la aplicación: *http://backuppc.sourceforge.net/*

Página de descarga: *http://sourceforge.net/projects/backuppc/*

Página de documentación: *http://backuppc.sourceforge.net/faq/BackupPC.html/*

En la actualidad multitud de pequeñas empresas y redes domésticas, que no se pueden permitir el desembolso que supone la instalación de equipos robotizados, están constituidas por un sinfín de dispositivos de los que es necesario realizar copias de seguridad: ordenadores portátiles, servidores, ordenadores personales, a menudo con una variedad de sistemas operativos. E incluso con equipos portátiles que no pueden estar conectados a la red por la noche, que es cuando generalmente se lanzan

los procesos de copia de seguridad. La mayoría de las aplicaciones libres de copias de seguridad no son capaces de solucionar este tipo de problemas.

BackupPC es una aplicación de alto rendimiento, especializada en la realización de copias de seguridad de ordenadores portátiles y personales con sistemas operativos Windows o Linux, volcándolas discos del servidor. Es altamente configurable y fácil de instalar y mantener.

BackupPC está programado en Perl y extrae copias de seguridad vía SMB utilizando Samba, tar sobre ssh/rsh/nfh, o rsync.

10.4.2.1 CARACTERÍSTICAS PRINCIPALES:

10.4.2.1.1 Soporta cualquier Sistema Operativo cliente:

Por medio de la utilización de herramientas estándar que bien se facilitan con la versión base o pueden ser fácilmente instaladas y añadidas al sistema, es posible soportar una amplia gama de clientes. Como añadidura, no es necesaria la instalación de ningún tipo de software cliente más allá de las utilidades estándar del sistema (tar, ssh, rsync).

10.4.2.1.2 Control de las copias por parte de los usuarios a través de interfaces vía Web

La mayoría de los sistemas operativos disponen de navegador de Internet, por lo que el uso de interfaces Web es una manera de acelerar el proceso de gestionar nuevos sistemas operativos. La interface debería estar diseñada para otorgar el mayor control posible al cliente y además hacerlo de manera segura. Un usuario debería ser capaz de solicitar una restauración sin la necesidad de que interviniera ningún operador. Por otro lado ningún usuario debería poder ver la máquina de otro.

10.4.2.1.3 Soporte para DHCP y clientes desconectados

Mediante el uso de utilidades estándar, BackupPC, soporte clientes DHCP mientras el cliente este registrado con un servicio de nombres como DNS, ACtive Directory o LDPA.

10.4.2.2 OTRAS CARACTERÍSTICAS:

- Un sistema inteligente de gestión de colas minimiza el almacenamiento en disco y la E/S del mismo. Archivos que son idénticos en diferentes copias de seguridad del mismo o diferentes ordenadores son almacenados una única vez, resultando un ahorro considerable de espacio de disco utilizado y de procesos de entrada o salida.
- Compresión opcional que reduce el volumen de almacenamiento.
- Completo grupo de opciones de restauración, incluyendo restauración directa)vía tar o rsync/rsyncd), o mediante la descarga de archivos zip o tar.
- Soporte de entornos móviles en los que los ordenadores portátiles únicamente están conectados de forma intermitente a la red y tienen IP dinámica.
- Parámetros de configuración flexibles que permiten:
    - Múltiples copias de seguridad en paralelo.
    - Especificación de copias de seguridad a compartir.
    - Tomar la decisión de qué directorios respaldar o no
    - Varias programaciones para copias de seguridad totales o incrementales.
    - Programaciones para el envío de recordatorios vía email.
- Recordatorios periódicos a los clientes acerca de la necesidad o no de realizar copias de seguridad.
- Documentación detallada.

10.4.3 BACULA

Página de descarga: http://sourceforge.net/projects/bacula/

Página de la aplicación: http://www.bacula.org/es/

Página de la documentación: http://www.bacula.org/es/?page=documentation

Bacula es un software de código abierto capaz de hacer copias de seguridad y volcar los datos a cualquier combinación de disco, cinta magnética o medios ópticos. El servidor corre en clientes Unix y Linux, versiones de Windows posteriores a la versión

95 y sistemas Mac OS X. Fue originalmente escrito por John Walker y Kern Sibbald en el año 2000.

Está estructurado en una serie de componentes interrelacionados, en los que cada uno de ellos utiliza sockets TCP para comunicarse mediante conexiones de red. El uso de los protocolos TCP/IP es esencial para la filosofía de diseño de la aplicación porque permite a los componentes ser desarrollados en diversas máquinas. El transporte TCP puede ser envuelto con una capa de seguridad de transporte encriptado estándar (TLS) para proteger los datos mientras se produce la transmisión.

10.4.3.1 PRINCIPALES CARACTERÍSTICAS

10.4.3.1.1 Catálogo SQL:

El catálogo contiene una lista de archivos que han sido respaldados, los principales atributos de cada uno de los archivos, incluyendo un checksum, el cliente del que procede cada archivo, y los volúmenes en los que los archivos están almacenados. Debido a la información que contiene, el catálogo se constituye en un elemento vital en los procesos de copia y restauración de datos. Aunque incluye una utilidad que lo repararía en caso de necesidad, el catálogo deberá ser incluido en una copia de seguridad aparte tras cada ciclo de copias.

10.4.3.1.2 Copias de seguridad multivolumen

Una de las características que diferencian a Bacula del resto de software de copias libre, es su excelente soporte nativo a copias de seguridad multivolumen. Cuando se le equipa con un cargador automatizado, la aplicación simplemente expande las cintas magnéticas sin necesidad de la intervención humana. Incluso en máquinas con un único dispositivo de copia, Bacula informa automáticamente, bien mediante mensajes en consola o correos electrónicos, de la necesidad de una nueva cinta de almacenamiento.

10.4.3.1.3 Soporte de medios flexible

Bacula es capaz de volcar los datos de las copias de seguridad en diferentes tipos de medios, utilizando discos o cintas magnéticas con la misma facilidad. Incluye herramientas para transferir de una manera fácil las copias de seguridad a CD o DVD, y el soporte del autocargador permite que se integren silos de alto almacenamiento con un módico esfuerzo.

10.4.3.1.4 Niveles de copias de seguridad

Bacula diferencia entre copias de seguridad totales, diferenciales e incrementales. El nivel de copia deseado se especifica en la definición de la programación de las tareas de respaldo, y puede ser remplazado si un trabajo es realizado manualmente. Si se ha programado una copia de seguridad, pero ninguna copia de seguridad está presente en el catálogo, la aplicación promociona automáticamente una copia diferencial o incremental hasta una copia total.

10.4.3.1.5 Formato de almacenamiento de Bacula

Todos los datos de respaldo de Bacula son almacenados en volúmenes. Un volumen es un simple repositorio para realizar copias de seguridad de datos, puede tratarse de una cinta, un medio óptico o incluso un simple archivo. La aplicación utiliza un formato único en lugar de un estándar como tar o dump. Esta opción de diseño asegura consistencia entre plataformas e implementaciones de Bacula.

Mientras que esta elección de diseño supone distintas ventajas, también implica que son necesarias herramientas especializadas para extraer datos de las copias de respaldo realizadas por la aplicación en el caso de que no esté instalada en el sistema.

10.4.3.1.6 Comprobación de dispositivos de cinta magnética

Aunque el manual de la aplicación recoge un número elevado de dispositivos que se sabe funcionan correctamente con Bacula, es posible utilizar la utilidad *btape* para comprobar directamente si un determinado dispositivo funcionará sin problemas con la aplicación. La utilidad lee la configuración que se ha definido para los dispositivos de almacenamiento en cinta y los utiliza para realizar series exhaustivas de pruebas de compatibilidad, que incluyen lectura, escritura y varias operaciones de búsqueda. Si el resultado de los test es positivo se puede tener la seguridad de que el dispositivo en cuestión se comportará de manera adecuada con la aplicación y además que se encuentra correctamente configurado

Otras características que Bacula ofrece son:

- Soporta múltiples colas.
- Soporta Macintosh HSF.
- Soporta Windows VSS.
- Recuperaciones independientes.

- Documentación amplia y actualizada constantemente.

10.4.4 COBIAN BACKUP

Página de la aplicación: http://www.cobiansoft.com/index.htm

Página de descarga: http://www.cobiansoft.com/cobianbackup.htm

Cobian Backup es una aplicación multi-hilo que se puede utilizar para programar copias de seguridad de archivos y directorios y almacenarlas en otros directorios o dispositivos en la misma máquina o en otras de la red de trabajo.

No se trata de una aplicación normal de copias de seguridad, sino que se ha especializado en la copia de archivos y carpetas, en formato original o comprimidas, creando una copia de seguridad de las mismas y almacenándola en otro destino.

10.4.4.1 PRINCIPALES CARACTERÍSTICAS

- Copias de seguridad vía FTP en las dos direcciones (subida y descarga).
- Ejecutable como aplicación o como servicio: en caso de instalarse como servicio de Windows, se cargará automáticamente al iniciarse el sistema, sin necesidad de realizar ningún tipo de log.
- Consume muy pocos recursos.
- Puede ser ejecutado en segundo plano en el sistema: constantemente comprueba la programación de copias de seguridad y arranca las tareas a la hora especificada por el usuario.
- Soporta varios métodos de compresión: pudiéndose elegir entre los algoritmos zip, zip54 o 7zip.
- Ofrece potentes métodos de cifrado: (**Rijndael**) AES 256, AES 192 y AES 128
- Programación de copias de seguridad totales, incrementales y diferenciales.
- Compatible con múltiples plataformas Windows, incluyendo Windows 2000, 2003, Vista y 7.
- Interfaz gráfica: la interfaz gráfica de Cobian Backup hace que el programa sea simple de utilizar. Se encuentra dividida en dos paneles que muestran la tarea programada con los respectivos atributos, historial y log.

- Filtrado de exclusión o inclusión de archivos: es posible establecer parámetros de exclusión de archivos, que no serán incluidos en la copias de seguridad), o de inclusión (caso contrario).
- historiales: se mantiene un completo informe acerca de los respaldos realizados, sus atributos, éxito o fracaso, etc.

10.4.4.2 HERRAMIENTAS ADICIONALES

A parte de las ya comentadas características y funcionalidades, Cobian Backup ofrece varias herramientas adicionales, a las que se puede acceder mediante el uso de atajos de teclado.

- Descifrador (Decrypter): herramienta diseñada para descifrar archivos que han sido cifrados con Cobian Backup. Se utiliza para versiones antiguas de la aplicación.
- Eliminador (Deleter): un rápido eliminador de archivos y carpetas. Los archivos eliminados a través de esta herramienta no podrán ser recuperados en modo alguno.
- Codificador: Codifica o encripta, una cadena introducida por el usuario y devuelve una salida que puede ser copiada fácilmente. Se utiliza principalmente para codificar a formato binario fechas y horas.

11 TABLA DE ILUSTRACIONES

12 BIBLIOGRAFÍA

Aaronson, L. (Marzo de 2008). *How it works: The sturdiest Solid-State Storage.* Obtenido de popsci.com: www.popsci.com/node/19967

Acens Tecnologies S.A. (s.f.). *Información básica: ¿Qué es la SLA?* Obtenido de acens.com: www.acens.com/file_download/176/acens_que_es_el_sal_baja.pdf

Backup4all. (Agosto de 2011). *Differencial backup.* Obtenido de backup4all: http://www.backup4all.com/kb/differential-backup-117.html

Barker-Plummer, D. (Febrero de 2011). *Turing Machines.* Obtenido de plato.stanford.edu: http://plato.stanford.edu/entries/turing-machine/

Bochner, S. (2958). *John von Neuman, 1903 - 1957. A biographical memoir.* Obtenido de books.nap.edu: http://books.nap.edu/html/biomems/jvonneumann.pdf

Bradbury, C. (Noviembre de 2007). *The IT disaster recobery plan.* Obtenido de continuitycentral.com: http://www.continuitycentral.com/feature0524.htm

Brain, M. (Marzo de 2011). *How CDs Work.* Obtenido de electronics.howstuffworks.com: http://electronics.howstuffworks.com/cd1.htm

Christenson, N. (Agosto de 2004). *Much Ado About Exabyte/8mm Tape Drivers.* Obtenido de jetcafe.org: http://www.jetcafe.org/~npc/articles/exabyte-tape-drives.html

Cibecs. (2012). *2011 Busisness Data Loss Survey.*

Clapperton, G. (Agosto de 2000). *Understanding online backup.* Obtenido de techsupportalert.com: http://www.techsupportalert.com/pdf/r1833.pdf

CodeFX. (2001). *CIFS Explained.* Obtenido de codefx.com: http://www.codefx.com/CIFS_Explained.htm

Comvault Systems. (s.f.). *Synthetic Full Backups.* Obtenido de Commvault.com: http://documentation.commvault.com/dell/release_7_0_0/books_online_1/english_us/features/backup/syn_full.htm

Cook, R. (Septiembre de 2008). *Backup and recovery basics: Testing your backups.* Obtenido de searchdatabasebackup.techtarget.com: http://searchdatabackup.techtarget.com/tip/Backup-and-recovery-basics-Testing-your-backups

Copeland, J. (Julio de 2000). *Turing Archive for the History of Computing.* Obtenido de Alan Turing.net: www.alanturing.net

Da Cruz, F. (Mayo de 2011). *Hollerith & IBM Tabulators and Accounting Machines.* Obtenido de columbia.edu: http://www.columbia.edu/cu/computinghistory/tabulator.html

Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael. AES - The Encryption Standard.* Springer.

De Guise, P. (2009). *Enterprise Systems. Back up and recobery. A corporate insurance policy.* DCD Press.

Farrance, R. (Septiembre de 2006). *Timeline: 50 years of Hard Drives. A look at the history of hard drives.* Obtenido de PcWorld.com: http://www.pcworld.com/article/127105/timeline_50_years_of_hard_drives.html

Goldschmidt, A., & Akera, A. (Abril de 2003). *John W. Mauchly and the Development of the ENIAC Computer.* Obtenido de library.upenn.edu: http://www.library.upenn.edu/exhibits/rbm/mauchly/jwm11.html

IBM Archives. (s.f.). *IBM 726. Magnetic tape reader/recorder.* Obtenido de 03.ibm.com: http://www-03.ibm.com/ibm/history/exhibits/701/701_1415bx26.html

Indiana University. (Mayo de 2009). *What is DHCP?* Obtenido de kb.iu.edu: http://kb.iu.edu/data/adov.html

Jones, D. W. (Julio de 2011). *Punched Cards.* Obtenido de divms.uiowa.edu: http://www.divms.uiowa.edu/~jones/cards/

Kerekes, Z. (2011). *History of Enterprise Disk to Dosk Backup. How the backup market moved from tape to disk - timeline of key events.* Obtenido de storageresearch.com: http://www.storagereseach.com/d2dhistory.html

Kozierok, C. M. (Abril). *The Pc Guide. Hard Disk Operational Overview.* Obtenido de pcguide.com2001: http://www.pcguide.com/ref/hdd/op/over.htm

Leg, C. W. (Marzo de 2009). *History of the Floppy Disk and Associated Hardware.* Obtenido de leggconsulting.com: http://www.leggconsulting.com/Portals/0/Documents/FloppyHistory.pdf

Lubar, S. (Marzo de 2009). *Do not fold, splindle or mutilate. A cultural history of the punched card.* Obtenido de web.archive,org:

http://web.archive.org/web/20061025144334/http:/ccat.sas.upenn.edu/slubar/fsm.html

Maxell. (Mayo de 2010). *About Maxell. New Releases.* Obtenido de biz.maxell.com: http://biz.maxell.com/release/20100514.html

MKM Publicaciones. (Marzo de 2012). *Las empresas pierden hasta 10.000 dólares por cada incidente de pérdida de datos.* Obtenido de mkm-pi.com: http://www.mkm-pi.com/diario-informatico/1las-empresas-pierden-hasta-10-000-dolares-por-cada-incidente-de-perdida-de-datos567/

Oracle. (2010). *System Administration Commands.* Obtenido de docs.oracle.com: http://docs.oracle.com/cd/E19253-01/816-5166/prtvtoc-1m/index.html

Oracle. (2012). *Métodos de copias de seguridad de bases de datos.* Obtenido de dev.mysql.com: http://dev.mysql.com/doc/refman/5.1/en/backup-methods.html

Perenson, M. J. (Septiembre de 2006). *The Hard Drive Turns 50. A look back at where hard drives have been and where they're going.* Obtenido de pcworld.com: http://www.pcworld.com/article/127104/the_hard_drive_turns_50.html

Philips. (s.f.). *Philips Researc: The history of the CD - The CD family.* Obtenido de research.philips.com: http://www.research.philips.com/technologies/projects/cd/cd-family.html

PostgreSQL. (s.f.). *Backup and restore.* Obtenido de postgresql.org: http://www.postgresql.org/docs/8.1/static/backup.html

Preston Curtis, W. (2007). *Backup and Recovery.* O'Reilly Media Inc.

Pugh, E. W. (Mayo de 2005). *RAMAC in Historical Perspective.* Obtenido de magneticdiskheritagecenter.org: http://www.magneticdiskheritagecenter.org/MDHC/MILESTONE/Emerson%20Pugh%20talk.pdf

Rouse, M. (Septiembre de 2005). *Zoned-bit recording (ZBR).* Obtenido de searchstorage.techtarget.com: http://searchstorage.techtarget.com/definition/zoned-bit-recording

Schoenher, S. (Noviembre de 2002). *The History of Magnetic Recording.* Obtenido de homepage.mac.com: http://homepage.mac.com/oldtownman/recording/magnetic4.html

Silberschatz, A., Korth, H. F., & Sudarshan, S. (2006). *Fundamentos del diseño de bases de datos.* Mc Graw Hill.

SNIA. (2012). *Tape Drivers.* Obtenido de snia.org: http://www.snia.org/education/storage_networking_primer/stor_devices/tape_drives

Symantec. (2007). *Symantec Disaster Recovery Research 2007.*

Techweek Informes. (Noviembre de 2011). *El 62% de las empresas europeas pierden datos confidenciales por el extravío de memorias USB.* Obtenido de techweek.es: http://www.techweek.es/seguridad/informes/1009935004801/62-empresas-europeas-pierden-datos.1.html?utm_source=newsletter&utm_medium=email&utm_campaign=20111122

TextosCientíficos.com. (Octubre de 2006). *Cintas Magnéticas.* Obtenido de textoscientificos.com: http://www.textoscientificos.com/informatica/almacenamiento/cintas-magneticas

USB Memory Direct. (Marzo de 2012). *An Overview of USB Flash Drives and Their Future.* Obtenido de usbmemorydirect.com: http://www.usbmemorydirect.com/news/overview_of_usb_flash_drives.htm