UNIVERSIDAD PRIVADA DE TACNA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE SISTEMAS

BACKUP Y RESTAURACION

Integrantes : HUICHI CAPAQUERA HABRAN
GEOVANY HERRERA KENZO
CONDE BEYZAGA WILHELNS
LOPEZ CARPIO EDGARD
AROQUIPA JIMMY

Profesor : PATRICK CUADROS

Curso : BASE DE DATOS 2
Ciclo : VII

TACNA - 2016

Tabla de Contenido

July 12, 2016

1 Introducción

Sobre las estrategias de salvaguarda de datos, o planes de copias de seguridad, hay mucho escrito, sin duda, pero en Expertos en Sistemas se va a tratar de realizar una exposición detallada y completa, recogida en diferentes capítulos. Para ello vamos a comenzar la publicación de una serie de artículos que recojan los diferentes aspectos que hay que considerar en la definición del proceso de respaldo de datos, backups, o copias de seguridad, válidos para cualquier empresa, grandes compañías o usuarios particulares, ya que orientará en la medida de lo posible para que cada cual encuentre su alcance y su casuística particular. Estos artículos irán desde el presente, que incide sobre la necesidad de las mismas, pasando por la confección de un plan de copias de seguridad e incluso llegando a la descripción de herramientas hardware y software específicas.

El plan general de copias de seguridad de cualquier entidad, considerado como un proceso bastante estandarizado, es sin embargo muy dependiente de las peculiaridades de cada empresa o usuario, en función de varios aspectos: presupuéstales, de actividad de negocio, volumen de información, ámbito de restauración necesario, tipos de datos, etc.

2 Marco Teórico

2.1 ¿POR QUÉ SE DEBEN HACER COPIAS DE SEGURIDAD?

Comencemos por enumerar los motivos que nos obligan a su planificación, porque seguro que no todos se conocen lo suficiente, y sin embargo son aspectos que ayudarán a valorar taxativamente hasta dónde se debe llegar, el alcance, y sobre todo el presupuesto, así como a no sustituir el proceso de un verdadero plan de copias de seguridad por otros más simples, como una simple copia de datos en un segundo soporte físico, algo que podría llevarnos a una desagradable sorpresa a la más mínima necesidad de restauración.

Lo obvio, para prevenir una pérdida de datos. Bueno, vale, pero ¿Por qué se puede perder la información alojada en un dispositivo de almacenamiento?
o **Un disco duro**, aunque sea nuevo, **se puede averiar**. Algunos pueden ser recuperados fácilmente, otros también se pueden recuperar, pero a través

de empresas especializadas en estos servicios, a un coste que habitualmente es mayor al daño sufrido; y, por supuesto, en algunas otras circunstancias puede hacerse imposible recuperar la información. Y no, la garantía del fabricante no se hace responsable de la pérdida de datos.

Por error humano también se puede llegar a eliminar o modificar información importante, y necesitar su recuperación.

simplemente por **necesitar recuperar antiguas versiones de documentos** que hayan sido modificados conscientemente, pero que luego cambiamos de opinión o necesitamos consultar estados anteriores de los archivos.

No olvidemos la acción que puede ocasionar sobre la información un , o cualquier otro tipo de malware en general.

La degradación de un sistema operativo o de una base de dato s, simplemente por su uso, o mal uso, puede suponer también una necesidad de restaurar archivos, esta vez de sistemas.

Cualquier otro tipo de sistema de información, no solo un sistema de archivos o bases de datos simple, fácilmente respaldables, sino además, servidores de correo electrónico, sistemas de mensajería más completos como Microsoft Exchange, Blackberry Enterprise Server, servicios de SharePoint, servidores web, etc., que requieren de un plan, un orden en la realización, posibles paradas de los servicios, extracción de instantáneas de volumen, copias de los archivos de transacciones, realización de procesos especiales en las bases de datos relacionales, etc., que sin ellos, el contenido salvaguardado no será más que un conjunto de archivos totalmente inútil, información inconsistente e imposible de restaurar.

El intrusismo El intrusismo, por ejemplo de un hacker, sobre cualquiera de estos sistemas vistos, que pueda provocar la modificación o pérdida de la información. Aunque esto daría para otro tema bastante distinto, comentar tan solo que el mayor enemigo en este sentido en las empresas está dentro de ellas. Un empleado descontento lo tiene muchísimo más fácil para ocasionar una pérdida de información que alguien desde fuera, y sin necesidad de grandes conocimientos técnicos.

Un incendio o un robo.

Catástrofes naturales como inundaciones o terremotos.

No solo por el borrado eventual de los datos, o su modificación, son necesarias las copias de seguridad, sino también **porque alguna ley lo exija** en función del país, la actividad de la empresa u otras circunstancias. La Ley Orgánica de Protección de Datos (LOPD), en España, obliga a la realización de copias de

seguridad cuando se trata con datos de carácter personal, estableciendo además unas pautas concretas a seguir.

Por archivar datos a un medio de almacenamiento más económico Por archivar datos a un medio de almacenamiento más económico. Por ejemplo, si se dispone de una cabina de discos redundantes de alto rendimiento que albergue toda la información de la empresa, el precio de este sistema de almacenamiento por Megabyte de información podría resultar demasiado costoso para una eventual ampliación, de forma que podría ser recomendable, bajo un determinado volumen de información, el archivado de proyectos cerrados o de archivos obsoletos a soportes externos, como cintas LTO (Linear Tape Open), o conjuntos de discos más económicos, cuyo precio por Megabyte es muy inferior.

Porque, en caso de pérdida, **¿En cuánto se podría valorar la información?** Para ello, a su vez, es necesario plantearnos las siguientes cuestiones adicionales:

o**¿Podrías iniciar de nuevo tu actividad en una ubicación distinta, en caso de un gran siniestro, si dispusieras de todos los archivos que residían en tu almacén de información, que ha sido destruido, junto con el resto del edificio (pongamos el caso más extremo)?** Si la respuesta es sí, la vida de tu empresa depende de ello. ¿En cuánto valoras tu empresa? Evidentemente, no basta únicamente con disponer de ese backup, también es necesario un Plan de Contingencias que diga qué hacer con esas copias de seguridad, qué recursos, en cuánto tiempo, cómo, etc., algo que daría para otro artículo de Expertos en Sistemas, y seguro que tendremos. No es tan descabellada la idea de poder resurgir, hay que pensar que un buen seguro lo cubre casi todo, menos la información, claro está.

o**¿En cuánto se podría valorar el tiempo de dedicación de tus empleados?** Esto sí que es algo fácil de cuantificar, aunque evidentemente dependerá de los diferentes perfiles y salarios, pero siempre se puede promediar. Si se eliminan por error los datos de personal que lleva el departamento de RRHH introduciendo las dos últimas semanas, ¿Cuánto cuesta eso? O si se corrompe la información de un proyecto, a causa de un virus, en el que un equipo de desarrollo lleva trabajando 200 horas,**¿En cuánto se podría valorar?** No hay más que multiplicar e ir sumando para calcularlo.

No solo debemos considerar una valoración económica. ¿Y si lo que se pierde es información de clientes, o que su pérdida incida de alguna forma en sus intereses, o simplemente se enteren del traspiés? **¿En cuánto podrías valorar la imagen de tu empresa?**

El caso más grave que podría existir es si además, tenemos**penalizaciones económica?** penalizaciones económicas que cuantificar de cara a clientes, o bien,**responsabilidades legales**, como multas por incumplimiento de LOPD.

A pesar de todo, todavía impresiona la cantidad de empresas que no mantienen una política de copias de seguridad apropiada. Siempre que se habla de cuál es el principal activo de una empresa, es muy habitual oír que su capital humano, y en buena medida es bastante cierto. Pero no olvidemos el dicho de que "nadie es imprescindible", así que incluso los empleados de una compañía pueden ser sustituidos fácilmente por otros distintos que realicen, más o menos, el mismo trabajo. Lo que no se podrá sustituir jamás es la información, por otra. No, la información debe ser exactamente la que es; no nos vale otra, de versiones más antiguas y desactualizada, por ejemplo. Hoy en día, en la era de las tecnologías, las comunicaciones y la informática, es muy difícil encontrar una empresa que sea capaz de soportar la pérdida de toda su información, que pudiese suportar la pérdida de los datos de su cartera de clientes, información de proveedores, datos económicos, RRHH, proyectos, etc.

El principal activo de una empresa es su información.

2.2 ¿CUÁLES SON LOS PRINCIPALES ASPECTOS A TENER EN CUENTA EN LA CONFECCIÓN DE UN PLAN GENERAL DE COPIAS DE SEGURIDAD?

Empresa o particular . Aunque de una forma o de otra, un backup de datos es un backup de datos, uno de los principales factores de riesgo, el económico, que motiva la creación de copias de seguridad, por norma general es mucho más elevado en una empresa que en un particular. Las horas, días, meses o incluso años de trabajo, que se pueden perder en un instante de tiempo ante una contingencia, al traducirlos a coste económico pueden llevar a una empresa a la quiebra, algo que en el entorno privado, por muy importante que sea la información, no es habitual que suponga un daño tan grave. Sin embargo, en un particular, el contenido afectivo que se puede estar respaldando es cada vez mayor, ya que los elementos multimedia incluyen habitualmente muchas fotografías y vídeos familiares, de infancia y ocasiones especiales, además de otros contenidos de interés que también podamos tener en formato electrónico, y que hasta ahora no era habitual, como facturas, información fiscal, libros y otros muchos documentos. La pérdida de todo esta material para un usuario particular, salvando las diferencias que se puedan tener con el ambiente corporativo, nos supondría una pérdida irreparable. Este artículo se centrará bastante más en la elaboración de un plan corporativo, sin embargo siempre será posible extraer ideas y métodos, que gracias al avance en las tecnologías domésticas, podremos aplicar para nuestras copias particulares; sirva como ejemplo la inclusión de las instantáneas de volumen en las últimas versiones de los sistemas operativos de escritorio Microsoft (denominado en Windows 8 como Histórico de archivos), el aporte de los archivos sin conexión, que nos permite mantener sincronizados los

datos entre PC y portátil, y el complemento, de uso obligado, de un plan de copias, que aunque simple, se sirva de backups periódicos en soportes externos, garantizando así la perpetuidad de nuestra información particular.

¿Datos propios o de clientes? Evidentemente, no es lo mismo responsabilizarse de nuestra propia información, que de los datos de clientes, que nos están pagando además por su custodia o gestión, y que habría que recurrir al contrato correspondiente para estimar con suficiente detalle una valoración apropiada. Por supuesto, el tipo de proceso de copias, ámbito de restauración, disponibilidad y el tiempo de respuesta ante contingencias son factores que deben estar recogidos en el mismo, cubriendo todas las posibilidades, y quedando el cliente plenamente informado del más mínimo resquicio que pueda suponer una pérdida de información, del ámbito de restauración, ofreciéndole siempre una alternativa de mejora junto a su coste asociado, así como nuestra recomendación, pero haciéndole partícipe de los pros y contras de su nivel de respaldo. Evidentemente, tanto para el presupuesto de nuestra estrategia de copias de seguridad, como para la valoración de los servicios que vamos a ofertarle, o le estamos ofertando, a nuestros clientes, ya sea en hosting, housing o en sus propias instalaciones, es necesario cuantificar este coste, no solamente para obtener una valoración económica, sino para dimensionar correctamente nuestra estrategia de copias de seguridad. Sin entrar en mucho detalle, estableciendo dos o tres niveles de salvaguarda con ponderaciones económicas, prorrateando costes en los diferentes proyectos, considerando la cantidad de información a respaldar, realizando las estimaciones oportunas sobre el montante de proyectos de este tipo, no es difícil preparar un pequeño análisis sobre los diferentes costes a repercutir, así como los compromisos contractuales con los mismos.

Datos de carácter personal, sujetos a planes específicos, definidos en función del nivel que marque la Ley Orgánica de Protección de Datos (básico, medio o alto), pero que deben formar parte del plan general de copias de seguridad. En España, la LOPD, especifica detalladamente para cada uno de estos niveles, los ámbitos de restauración, la ubicación de las copias, si es necesario aplicar cifrado, etc.

La presencia de sistemas preventivos complementarios, como instantáneas de volumen, discos en espejo o conjuntos de discos redundantes –Redundant Array of Independent Disks- (RAID), o sistemas con alta disponibilidad (en clusters de servidores), e incluso réplicas completas de centros de procesos de datos, pueden influir de alguna manera en el alcance de un plan general de copias de seguridad, pero no debería modificarlo tan drásticamente como se podría pensar, un error bastante común. La existencia de réplicas como las comentadas, puede sin duda, solventar la caída o avería de un disco duro, pero no la acción de un virus en el sistema, por ejemplo; ya que será replicado igualmente en todos los dispositivos redundantes. Lo mismo ocurre con la eliminación o modificación de datos, la copia de una base de datos con datos inconsistentes y otros de los diferentes motivos que nos obligan a la realización de copias de seguridad. No

obstante, estos sistemas complementarios deben ser considerados en el plan, o bien más generalmente en un plan de contingencias o incluso en los análisis de riesgos de cualquier proyecto que se sirva de ellos para el respaldo de sus datos. Un ejemplo de esta influencia sería la mayor rapidez que se obtiene al restaurar un archivo desde las instantáneas de volumen, en lugar de hacerlo desde las copias de seguridad; no olvidemos que el proceso de restauración es parte del plan general de copias de seguridad.

El ámbito necesario de restauración . Es necesario plantear e informar al personal implicado, a los propietarios de los datos, las necesidades ante una posible restauración, proponiendo u ofreciendo diferentes alternativas en base al presupuesto para la estrategia de backup. Es decir, si se necesita restaurar un archivo a una versión anterior, ¿Hasta qué margen de tiempo hacia atrás podría ser necesario llegar? ¿Una semana? ¿Un mes? ¿Un año o más?

Tecnologías y plataformas . Los diferentes sistemas operativos que puedan existir, normalmente Windows y Linux, la diversidad de bases de datos (SQL Server, Oracle, MySQL, etc.), los servicios de mensajería (MS Exchange Server, Open XChange, etc.), sistemas de virtualización (VMware, Citrix, Microsoft), son plataformas que exigen una visión especial de sus respaldos, por diferentes motivos: normalmente necesitan conectores software adicionales para la aplicación de backup que se vaya a utilizar, lo cual conlleva un coste económico asociado, y por otra parte se trata de sistemas que necesitan de métodos especiales de respaldo, en algunos casos es necesario realizar paradas de servicios, realizar operaciones con archivos de transacciones, o utilizar sus propias funciones de restauración, que deben ir conjugadas con la posterior restauración en nuestro sistema global de copias de seguridad. Todo ello debe ser analizado, valorado y contemplado en la estrategia de copias de seguridad.

Horario . Establecer el rango de horario más adecuado, normalmente durante la noche, en el que usuarios y aplicaciones requieren una menor disponibilidad de los datos. En casos puntuales podría ser necesario tener que mantener una disponibilidad 247, en tal caso, deberá considerarse la posibilidad de realizar copias de seguridad “en caliente”, o sea, sin desactivar los servicios. Esta operación se realiza normalmente conjugada con las instantáneas de volumen, siempre que exista compatibilidad, lo que a su vez dependerá del software de copias de seguridad que se esté empleando, de los conectores que estén licenciados y de la naturaleza de los datos.

Un plan de pruebas de restauración . Hay que tener definido un conjunto de pruebas de verificación, que nos permitan asegurar que el plan de copias de seguridad está funcionando correctamente, además de planificar la ejecución periódica del mismo. No sería la primera vez que una empresa lleva años realizando un respaldo de datos erróneos, bases de datos inconsistentes o ficheros corruptos, y posteriormente, cuando llega el problema crítico y se debe echar mano a las copias... digamos que comienzan a rodar cabezas.

Custodia de soportes externos y permisos de acceso . Se deberá establecer una persona responsable, así como los técnicos encargados del proceso, y asignar los permisos adecuados para las diferentes tareas y para el buzón de correos asociado a las alertas y recepción de archivos de registro. Y establecer las cuentas de sistemas que se vayan a utilizar para el acceso por parte de la aplicación de backup a los diferentes sistemas de información comentados anteriormente. Un error muy habitual es utilizar la cuenta del administrador o de root para ello, una práctica muy desaconsejada, que refleja además que no se le cambia la contraseña a esta cuenta con la periodicidad que debería hacerse. Doble error de seguridad.

Continuar garantizando la integridad, confidencialidad y disponibilidad de la información, con las mismas garantías que tenían antes de ser respaldada.

¿Cada cuánto tiempo cambia el contenido de la información a respaldar? Efectivamente, no es lo mismo tener que realizar copias de seguridad de un contenido que evolucione constantemente, y lo más importante, cuyo coste evolutivo sea muy alto. Es decir, por ejemplo, un equipo grande de desarrollo, en unas pocas horas de trabajo estaría generando una enorme cantidad de información digna de ser respaldada cuanto antes; mientras que también podríamos tener el caso contrario, de un repositorio de información cuyas modificaciones se realicen a muy largo plazo. Evidentemente, el tipo de copias, su periodicidad, e incluso el tamaño de los soportes externos, podrían ser totalmente distintos, al igual que otros factores.

Ubicación de las copias . Las copias de seguridad no se deben almacenar en el cajón de la mesa "del informático". Desde una caja fuerte, pasando por

una cámara ignífuga o aún mejor, una ubicación fuera del edificio donde residan los almacenes de información. Como siempre, si existen datos de carácter personal, la LOPD tiene mucho que decir, ya que por ejemplo, en caso de sacarse información fuera de la empresa, nos añadirá el hándicap de tener que ir cifrada.

Presupuesto. Lo más lógico es que en base a todos los factores, y tras la confección de la estrategia de copias de seguridad, uno de los resultados sea el presupuesto necesario. Pero no nos engañemos, lo habitual es conocer el presupuesto, o al menos hasta donde podemos llegar, antes de confeccionar el plan, pudiendo adaptarlo en cierta medida en base al mismo. Conocer el presupuesto con el que contamos es muy importante, ya que de él dependen todos y cada uno de los puntos comentados.

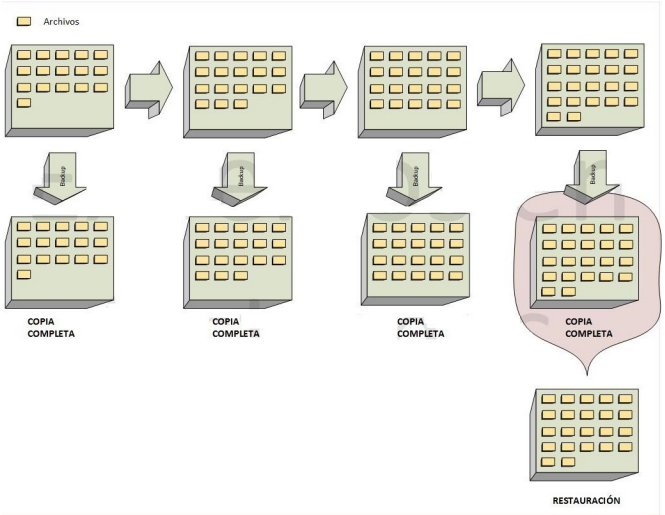
Elaborar y mantener un plan de operaciones. Es muy habitual llegar a elaborarlo, pero eso de mantenerlo... Un documento de este tipo debe ser algo vivo, y el responsable del proceso de copias de seguridad debe ocuparse de que la información que en él se refleje esté actualizada. En este documento se detallarán las acciones, responsables, nombres y ubicación de dispositivos, tiempos de respaldo y restauración necesarios, etc.

Todos estos puntos y puede que alguno más, son factores clave a la hora de diseñar una estrategia apropiada de copias de seguridad. En los próximos capítulos se afinará aún más en otros aspectos que abordan de forma más directa los procesos de backups.

2.3 DIFERENTES TIPOS DE COPIAS DE SEGURIDAD

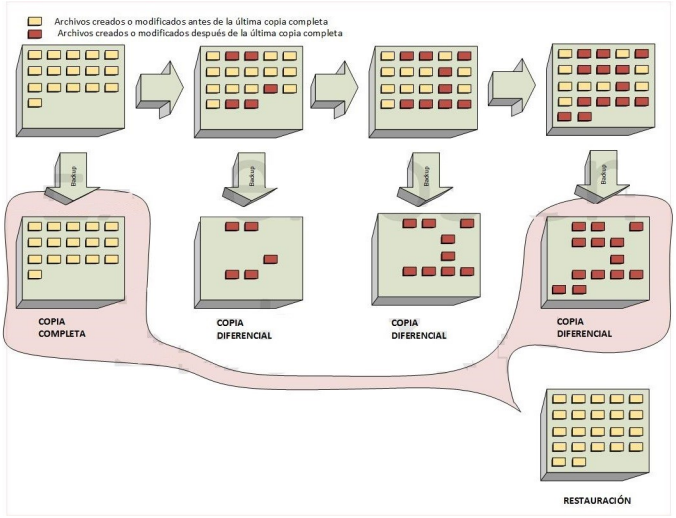
2.3.1 Copia de seguridad completa o normal

Una copia normal no es más que un backup completo de todos los archivos seleccionados en el plan de copias. Cada vez que se realiza una copia normal, el sistema operativo pone el bit de copia del archivo salvaguardado (también llamado bit de modificación) a 0, para identificar que se le ha realizado un respaldo, o que el archivo no ha sido modificado desde la última copia de seguridad que se le realizó. Este bit volverá a 1 en el momento en que el archivo sea modificado.



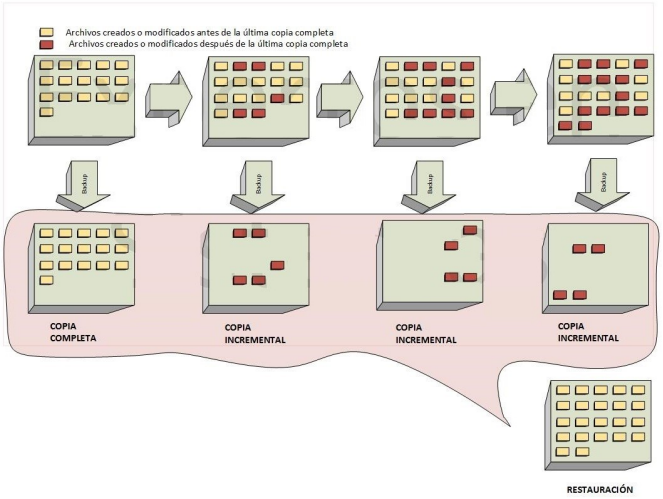
2.3.2 Copia de seguridad diferencial

Una copia diferencial es un proceso de backup en el que se salvaguardan solamente los datos que han sido modificados desde la última copia de seguridad completa que se realizó. O sea, el proceso se fija en el estado del bit de modificación, y solo copia el archivo en caso de que éste se encuentre a 1. De esta forma, en cada medio, o conjunto de medios de backup que se creen, solo existirá una información parcial del almacén de datos. Por este motivo, para poder realizar una restauración completa para esa fecha, será necesario disponer de este medio diferencial más el medio en el que se realizó la copia completa o de referencia. Para ello, el propio software que utilicemos para realizarlas se encargará de demandarnos que insertemos ambos medios, y él mismo obtendrá el conjunto final de información con la totalidad de los datos respaldados, en caso de necesitarse una restauración.



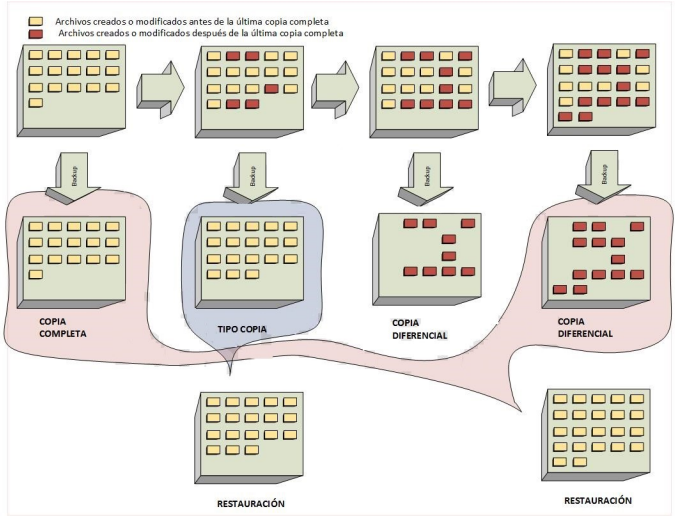
2.3.3 Copia de seguridad incremental

Se trata del tipo de copia que menos capacidad necesita, por volumen de copia, ya que solo almacenará la información que haya sido modificada desde la última copia de seguridad realizada, ya sea completa, diferencial o incremental, da lo mismo. Además, evidentemente, también se trata del proceso de backup más rápido en realizarse. El principal inconveniente que tiene este mecanismo es que para lograr una restauración en un momento determinado, se necesitarán todos los conjuntos de medios incrementales hasta llegar a la última copia diferencial o completa realizada, además de éstas últimas. Igualmente, será el propio software de backup el que nos pida los diferentes volúmenes y los catalogue antes de proceder a su restauración, por lo que el proceso será bastante transparente para el administrador, antes de disponer de nuevo de toda la información.



2.3.4 Copia de seguridad de tipo copia o sin restaurar el bit de archivado.

En Ntbackup de Windows Server, y en otras plataformas, existe un cuarto tipo de backup, denominado tipo copia, a veces disponible como opción de configuración para las copias de tipo completo. Éste no es más que un backup completo, pero en el que no se restaura el bit de copia a 0, sino que se mantiene a 1. De esta forma, en caso necesario de pretender obtener puntualmente un backup completo de información, sin que se modifique el calendario de nuestro plan de copias, podremos obtenerlo. Por ejemplo, si nuestro plan de copia se basa en la realización de backups completos los domingos por la noche, e incrementales de lunes a viernes; y ante una instalación importante en nuestros sistemas, queremos realizar el miércoles una copia de seguridad previa de todos los repositorios de información, pero sin modificar la estrategia de copias de seguridad utilizada, podremos hacerlo utilizando este método.



Para garantizar la correcta utilización de los diferentes tipos de copias de seguridad, evitando los errores, se deberá establecer un sistema de nomenclatura de los medios y etiquetado acorde al plan de copias que se haya implementado.

Evidentemente, los plantes de copias que se utilizan son combinaciones de los diferentes tipos de copias mencionados y dependen en gran medida del volumen total de información a respaldar, las ventanas de tiempo que dispongamos para ello, etc.

Pero, ¿Cuántos medios necesitamos para generar un plan de copias de seguridad? Si nuestros medios son cintas LTO, por ejemplo, ¿Cuántas cintas se necesitan para implementarlo? Si para cada copia de seguridad se necesita al menos una cinta, ¿Vamos a ir utilizando cintas indefinidamente? Está claro que las cintas, o en general los medios utilizados, deberán ir rotando, sobrescribiéndose periódicamente, aunque por otra parte, nuestra política de copias de seguridad también deberá considerar el almacenamiento indefinido o a muy largo plazo de algunos medios, en función de las directrices marcadas, por ejemplo por la LOPD, o simplemente porque esa sea nuestra estrategia.

2.4 ROTACIÓN Y ARCHIVADO DE MEDIOS

A continuación se muestra un ejemplo de plan de copias que podría ser válido para muchas empresas de tamaño medio y necesidades tipo, donde los contenidos, el volumen de datos y la capacidad de restauración sean de lo más común.

Durante la noche, a menudo, aunque irá en función del hardware utilizado,

podría no dar tiempo suficiente para la realización de todo el backup completo, por este motivo, es habitual dejar las copias completas para los fines de semana.

De esta forma, una planificación tipo podría ser la siguiente:

Sábados 11:00 PM: Copia completa. Medios: S1, S2, S3, S4, S5 (*)

Lunes 11:00 PM: Copia diferencial. Medio: L

Martes 11:00 PM: Copia diferencial. Medio: M

Miércoles 11:00 PM: Copia diferencial. Medio: X

Jueves 11:00 PM: Copia diferencial. Medio: J

Viernes 11:00 PM: Copia diferencial. Medio: V

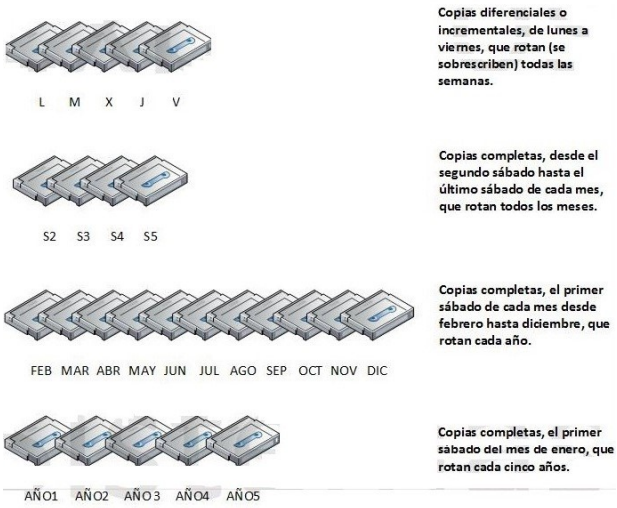
(*) S5 solo se utilizará en los meses que coincidan 5 sábados.

Cada medio de copia completa Sn, en función del volumen de datos, podría estar formado por dos o más cintas LTO, por ejemplo, aunque debido a su alta capacidad, podría ser también de una sola cinta LTO. Sin embargo, lo más normal será que los medios diferenciales e incrementales sí que tengan suficiente con una única cinta LTO, ya que normalmente ocupan poco volumen. En tal caso, podríamos estar hablando de un total de 10 cintas LTO para empezar.

De esta forma, con tan solo 10 cintas podremos tener un plan de copias que permitirá restaurar todo el contenido hasta un mes hacia atrás. Como esto es poco, deberemos recurrir al archivado de medios por más tiempo, de forma que si sustituimos el medio S1 por uno que lleve el nombre del mes, estaremos guardando el contenido del primer sábado de cada mes durante un año:

ENE FEB MAR ABR MAY JUN JUL AGO SEP OCT NOV DIC

Con esta modificación, podremos restaurar toda la información hasta un año hacia atrás, pero si además sustituimos el medio ENE (enero) por cinco nuevos medios de rotación que se sobrescriban anualmente, podremos recurrir a un backup de la información hasta 5 años hacia atrás. Con este último cambio, el conjunto de medios resultante sería el siguiente:



Conjunto de medios para el Plan de Copias de Seguridad

En definitiva, con un conjunto de medios finito (25 cintas LTO), hemos podido definir un plan de copias de seguridad que nos permite recuperar la siguiente información:

Datos perdidos cualquier día de la semana anterior..

En caso de necesitar datos más antiguos de una semana, se podrán recuperar de sábado en sábado, ya que los medios diarios habrán sido sobrescritos.

En caso de necesitar datos más antiguos de un mes, se podrán recuperar de mes en mes (primer sábado de cada mes, que corresponde a las cintas etiquetadas con el nombre de cada mes).

En caso de necesitar datos más antiguos de un año, se podrá recurrir a las cintas LTO etiquetadas como AÑOn, que contendrán un backup completo del primer sábado de cada año.

En función de las necesidades de cada empresa, modificando el número de cintas, el calendario de backup y los horarios, se traducirá en un cambio en el ámbito de restauración, permitiendo el **ajuste personalizado del plan de copias de seguridad**. Una opción bastante recomendable es adquirir una cinta LTO cada año, o bien, el número de cintas LTO que conformen el medio completo, y almacenar estas copias indefinidamente, etiquetándolas con el año en curso. De esta forma se obtiene un plan de copias de seguridad bastante completo con un número de medios moderadamente reducido.

Aunque en los ejemplos se han empleado medios basados en soportes LTO, su

finalidad ha consistido en la exposición de casos fieles a la realidad que se ofrecen en las empresas TIC, pero realmente son extrapolables a cualquier otro tipo de soportes, ya sean discos duros, CDs o DVDs, otros tipos de cintas magnéticas, etc., aunque como veremos en próximos artículos, cada cual tendrá sus ventajas e inconvenientes, que irán en relación a las **características y necesidades particulares de cada empresa**.

2.5 SOLUCIONES DE COPIAS DE SEGURIDAD

2.5.1 CD (Compact Disk) y DVD (Digital Versatile Disk) grabables o regrabables.

Aunque muy cerca de ni tan siquiera haberse tenido en consideración, se ha incluido este punto pensando fundamentalmente en las copias de recuperación del sistema y en usuarios particulares.

Se trata del elemento más económico, tanto por el propio dispositivo hardware como por sus soportes (CDs y DVDs). Sus capacidades no son muy elevadas: 650 o 700 Mb de datos en el caso de los CDs y 4,7 o 8,5 Gb básicamente para los DVDs. El principal problema que presentan es su escasa durabilidad, al contrario de lo que afirman los propios fabricantes, incluso en la serigrafía que muestran sus cajas -lifetime (toda la vida)-, pero que al cabo de algunos meses, o en pocos años, muchos terminan siendo unos bonitos posavasos. Y no hay que olvidar la obligación que tienen muchas empresas de almacenar la información por un período de tiempo mayor.

Sin embargo, a nivel doméstico sí que puede ser una buena opción, siempre que los procesos de backups se reciclen con frecuencia, y que, por supuesto, no se deposite toda la confianza exclusivamente en esta vía de salvaguarda de datos.

CD

DVD

2.5.2 Unidades de cintas magnéticas

Se trata del sistema más utilizado en empresas de tamaño medio y pequeño, así como del método proporcionalmente más económico, no solo como dispositivos de respaldo, sino también como almacenamiento a bajo coste y altamente fiable orientado al archivado definitivo de datos. Se utilizan en conjunción con una aplicación de administración del dispositivo y gestión de los medios, que a veces viene incluida en el propio sistema operativo, ya sea Windows o Linux, y en otras ocasiones, se recurre a la adquisición de una aplicación de terceros, que nos permite una mayor facilidad de uso, así como mayores posibilidades en la gestión y restauración.

Cintas magnéticas DDS

Aconsejable para grandes volúmenes de datos, gracias a las posibilidades que nos ofrece en conjunción con las librerías robóticas, permitiendo el cambio automático de cintas, algo que conlleva multiplicar con creces sus capacidades de almacenamiento, minimizando la intervención del administración de sistemas y permitiendo la programación calendarizada del cambio de medios.

Unidad de cinta LTO con lectura de códigos de barra

2.5.3 Copias de seguridad basadas en discos duros

Gracias al abaratamiento de estos dispositivos, generalmente utilizados en exclusividad para alojar el sistema operativo, aplicaciones y datos, ahora cabe también la posibilidad de realizar los backups en arrays formados por unidades de discos duros.

Su coste puede variar, en función del tipo de discos empleados, desde los baratos SATA, pasando por los SCSI, hasta los rápidos discos en fibra óptica, cuyas velocidades van en consonancia a sus precios. De esta forma, podemos considerar para uso doméstico, o para pequeñas empresas y autónomos, la posibilidad de realizar las copias en discos USB externos o en pequeños dispositivos NAS (Network Attached Storage), también con interface USB:

Dispositivo NAS económico

Para PYMES y grandes empresas existen soluciones de los principales fabricantes, como la StoreOnce Backup Family, de HP:

HP StoreOne Backup Family

Este tipo de dispositivos, manteniendo las altas capacidades que ofrecían las cintas, consiguen unas velocidades de acceso y escritura impensables con los dispositivos secuenciales. Sin embargo, y a pesar del abaratamiento comentado anteriormente, no llegan en ningún caso a ofrecer la buena relación prestaciones/precio que ofrecen las cintas, lo cual lo hacen aconsejable tan solo para soluciones de salvaguarda donde deba primar la velocidad por encima de todo, o para utilizarlo conjuntamente con algún otro método, como veremos más adelante.

2.5.4 Backups en la nube

Se trata de uno de los primeros servicios en la nube que ofrecieron algunos proveedores a través de Internet, con una gran evolución desde sus primeras soluciones, situados actualmente a la vanguardia entre los distintos métodos de respaldo y darían sin duda para un artículo bastante extenso.

Los backups en la nube gozan de numerosas ventajas, sin estar carentes de inconvenientes, como cualquier otra solución.

Entre sus ventajas destaca la clara reducción en la necesidad de disponer de una infraestructura local, disminución de los costes operativos, de hardware, de software, incluso de recursos técnicos, y coste basado en el almacenamiento utilizado.

Pero conlleva una serie de inconvenientes que no hemos de obviar, entre los que reside la necesidad de ancho de banda debido a la latencia, y mucho, en principio. Además, el más que evidente problema en la seguridad es la razón fundamental por la que muchas empresas no terminan de emplearlos. Y es natural, no olvidemos el reciente caso PRISM, de espionaje de la información por parte del gobierno norteamericano, donde los proveedores de servicios reconocen la vulneración de la privacidad en la información almacenada por sus clientes. Adicionalmente, la restauración y la integración con los sistemas de información utilizados por cada empresa son también algunos de los obstáculos que hay que salvar.

Aunque, sin lugar a dudas, su principal ventaja es la externalización de la información fuera de la propia empresa, algo que podría garantizar su supervivencia en caso de un desastre importante. Las estrategias de copias de seguridad y la recuperación de desastres van muy de la mano, aunque esta última exige medidas bastante más estrictas para garantizar su éxito ante una eventual contingencia, y claramente la externalización de la información es una de ellas.

Se trata de una solución muy adecuada para la realización de copias de seguridad de dispositivos móviles y oficinas remotas, de las que en caso contrario, debamos realizar los backups directamente desde la central, con lo que esta situación conlleva. Por este motivo, es habitual el uso de soluciones mixtas en algunas empresas, realizándose backups en la nube únicamente de los dispositivos utilizados para teletrabajo, portátiles, tablets, oficinas externas, etc., que además disponen de un volumen de datos pequeño, eliminando la necesidad de tal infraestructura de salvaguarda remota desde la oficina central, que tan solo se encargará de realizar los backups locales, donde reside el mayor volumen de información.

Existen además una serie de requerimientos fundamentales, sin los cuales se deberá descartar cualquier proveedor de servicios que no los proporcione: si se trata, como es lo más probable, de una comunicación a través de Internet, se deberá disponer de un canal cifrado por SSL para el transporte de la información. Esta deberá permanecer cifrada en su almacén de datos, mediante algún algoritmo con suficientes garantías, como puede ser el AES de 256 bits. Y, por supuesto, deberemos contar con un sistema de autenticación eficaz y seguro, como por ejemplo basado en dos factores o una autenticación OTP (One Time

Password) – Contraseña de un solo uso.

Otros requerimientos para minimizar el impacto sobre el ancho de banda son la deduplicación y compresión en origen, y el initial seeding cada vez más utilizado, o posibilidad de envío en un dispositivo físico con el volumen total de datos, por ejemplo un disco duro USB, de forma que se evite la masiva puesta en funcionamiento del plan de copias, tras la cual, tan solo se realizarán los backups continuos o incrementales, con la información que se vaya modificando. Esta última opción también es interesante en caso de necesitar una restauración importante.

Los proveedores de servicios de este tipo se las van ingeniando cada vez mejor para solventar los múltiples problemas que plantean estas soluciones de almacenamiento en la nube. Otra opción importante es la salvaguarda granular de la información, no a nivel de archivo, sino por debajo de estos. Veamos un ejemplo para clarificarlo: supongamos un archivo de Access (.mdb) de varios gigas de información, o cualquier otro archivo pesado; primero se deberá subir completamente para su primer respaldo, y posteriormente, cada vez que se realice una pequeña modificación se volverá a subir de nuevo por completo, ya que la mayoría de los sistemas de backup interpretarán que el archivo ha sido modificado, y tanto si se trata de copias diferenciales como incrementales, el sistema lo volverá a subir completamente. Para evitar esto, es fundamental un reconocimiento granular de los datos que hay que respaldar, a través de una capa de abstracción intermedia.

Así que hay que tener cuidado, ya que todas estas opciones no siempre están incluidas en los distintos proveedores de servicios de backup en la nube.

Además de asegurarnos que se cumplen estos requisitos, deberemos informarnos sobre determinados aspectos del proveedor: sus garantías de servicio, disponibilidad, capacidad y tiempo de respuesta ante situaciones de contingencias, cumplimiento de la normativa legal, etc.

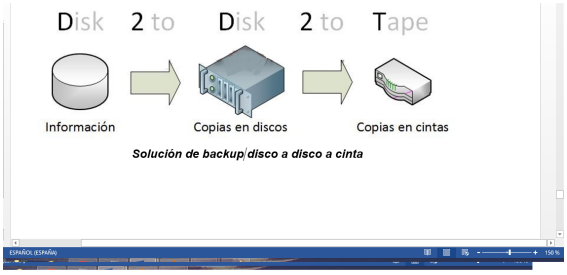
No olvidemos que en caso de una emergencia, de ellos dependerá la rápida recuperación de nuestra información.

2.5.5 Soluciones mixtas

Gracias a la variedad de opciones de distinta naturaleza, prestaciones, ventajas e inconvenientes, una buena forma de aproximar en la mayor medida la solución adoptada a nuestras necesidades, consiste en utilizar una solución de backup mixta, basada en la unión de varias de ellas.

Desde hace bastante tiempo se vienen utilizando soluciones del tipo D2D2T –disk to disk to tape- (disco a disco a cinta); es decir, nuestro sistema de copias

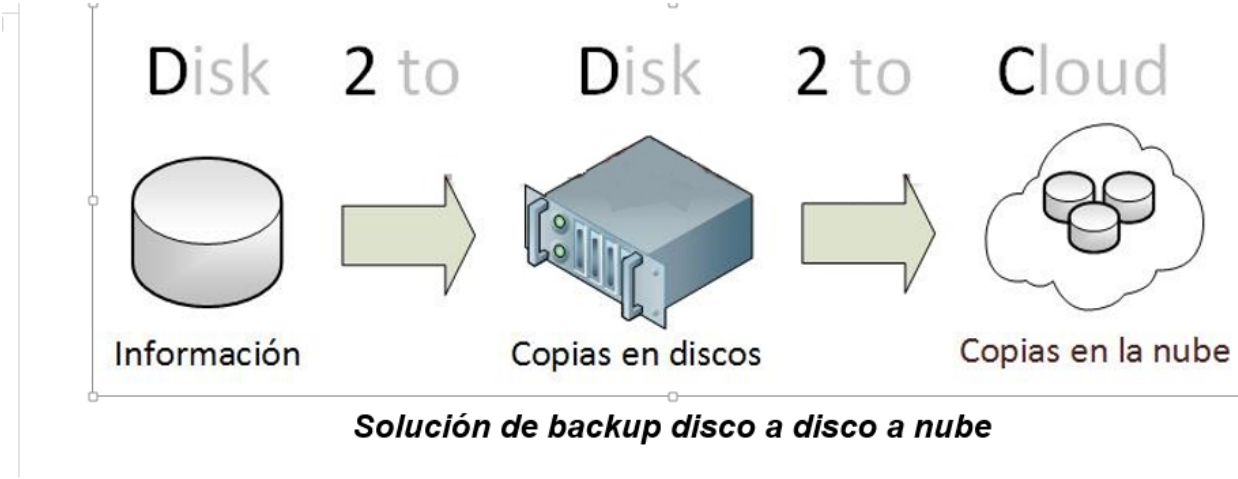
de seguridad realiza un primer backup sobre un conjunto de discos de tipo NAS, SAN, etc., de forma rápida, continua y eficaz, que incluso puede ser programado para realizarse varias veces al día, para minimizar la probabilidad de una posible pérdida de información. A su vez, este contenido, conforme esté completo, es salvaguardado a cinta, de forma más lenta, naturalmente. Esta última operación es más lenta, sin duda, pero no influirá en la disponibilidad de los datos originales, bases de datos o cualquier otro sistema de información cuyos servicios deban ser parados para su respaldo, ya que se estará haciendo desde una ubicación que lo que almacena es una copia previa en un conjunto de discos duros independiente.



Solución de backup disco a disco a cinta

Las ventajas de este sistema son obvias. Algunos inconvenientes que anteriormente habíamos encontrado en la realización de las copias de primer nivel, desde el almacén de datos original, se minimizan: el tiempo que se tarda en realizar el backup es muy inferior, ya que su salvaguarda en discos duros se realiza a mayor velocidad. Por otra parte también se minimiza el coste de los discos, ya que como posteriormente los datos se pasarán a cinta, no es necesario llenar y adquirir indefinidamente estos costosos dispositivos, sino que una vez respaldados a cinta, podrán ser sobrescritos. El archivado definitivo a cintas resulta bastante económico, además de permitir la flexibilidad de poder almacenarlo en sitios físicos diferentes a la oficina.

Más recientemente, y con la aparición de los backups en la nube, también se pudo optimizar este sistema a través de la implementación de soluciones mixtas. La estrategia D2D2C –disk to disk to cloud– (disco a disco a nube), añade algunas ventajas frente a la solución D2D2T, ventajas ya mencionadas anteriormente, que consisten principalmente en el alojamiento externo de la información, eliminando la necesidad del transporte de las cintas, previo cifrado de las mismas, controles de seguridad, etc.



Solución de backup disco a disco a nube

Evidentemente, el coste económico de este servicio en la nube deberá someterse a análisis y contrastarse con el resto de posibilidades. Como hemos podido ver, hay soluciones para todos los presupuestos y necesidades.

2.6 Aplicaciones

Independientemente de los dispositivos hardware que se utilicen, las copias de seguridad deben estar gestionadas por un software. En función de la calidad y alcance de éste, controlará, no solo el dispositivo, sino también todo el conjunto de medios, calendarios, planes de copias, credenciales, catálogos, acceso web, etc., integrados en una base de datos y disponible incluso vía web. Una de las aplicaciones más extendidas es Backup Exec, adquirida hace algunos años por Symantec y antes más conocida como Veritas. Esta aplicación no solo permite diseñar un mejor plan de copias de seguridad, sino que también hace viable la conectividad a distintos almacenes de información, además de a los archivos de datos, como pueden ser bases de datos SQL Server, Microsoft Exchange, servidores Windows adicionales, Linux, etc. Su coste lo hace recomendable únicamente para empresas.

Adicionalmente, existen aplicaciones de mucho más alto nivel, y precio, orientadas a grandes sistemas de información, como pueden ser Netbackup (también de Symantec), CA ArcServer, CommVault, EMC Networker, IBM TSM (Tivoli Storage Manager), etc., todas ellas compatibles con las distintas soluciones comentadas, incluida la D2D2C.

En algunos casos, al adquirir un hardware de backup, podremos encontrar que nos suministran una distribución gratuita de una de estas aplicaciones, como puede ser el propio Backup Exec, lo que nos servirá para la implantación de un plan de copias muy básico, ya que conforme vayamos integrando distintos servidores y servicios de nuestra red, observaremos que deberemos licenciar paquetes adicionales del producto, algo que evidentemente tiene costes añadidos.

Para empresas pequeñas, usuarios particulares y autónomos existen herramientas software más económicas, algunas gratuítas o integradas en el sistema operativo, como puede ser el mítico ntbackup, o de más reciente aparición e incluido en las últimas versiones de los sistemas operativos de Microsoft, wbadmin, que permite la realización de copias de seguridad incluso a través de las instantáneas de volumen.

Recuperar Base de Datos usando RMAN Voy a explicar en esta entrada, de forma sencilla y resumida, los pasos a seguir para recuperar una base de datos Oracle haciendo uso de la herramienta RMAN.

Supongamos que se produce cualquier error accidental del tipo de borrar algún datafile. La forma inmediata de recuperar la base de datos es haciendo uso de RMAN. Para ello, este es el procedimiento:

Parar la base de datos.

SQL¿ SHUTDOWN IMMEDIATE;

Entrar a RMAN.

rman target=/ catalog

rman$_{u}ser@cadena_{c}onexión$

RMAN¿ STARTUP MOUNT;

RMAN¿ RESTORE DATABASE;

RMAN¿ RECOVER DATABASE;

RMAN¿ ALTER DATABASE OPEN RESETLOGS;

RMAN¿ EXIT;

Bajar la base de datos, desde SQLPLUS.

SQL¿ SHUTDOWN IMMEDIATE;

Levantar la base de datos.

SQL¿ CONN / AS SYSDBA

SQL¿ STARTUP;

2.6.1 Introducción al Backup y a la Recuperación

Planear y comprobar los procedimientos de backup del sistema es la única garantía que existe contra fallos del sistema, del SO, del software o cualquier otro tipo de circunstancias.

Las causas de error en una sistema de BD pueden agruparse en las siguientes categorías:

• **Físicas** son causadas por fallos del hardware, como por ejemplo del disco o de la CPU.

• **e Diseño**
son agujeros en el software, ya sea en el SO o en el SGBD.

•**De Funcionamiento** de Funcionamiento
son causadas por la intervención humana, debidos a fallos del DBA, configuraciones inapropiadas o mal planteamiento de los procedimientos de backup.
•**Del entorno**
como por ejemplo desastres naturales, fallos de corriente, temperatura excesiva.
De entre todas estas posibilidades, el DBA sólo puede influir y prever los errores de funcionamiento, ya que el resto habitualmente no está dentro de sus responsabilidades y capacidades.
Dada la complejidad de los sistemas actuales y las necesidades cada vez más críticas en la disponibilidad de los sistemas, donde una BD caida puede causar pérdidas millonarias, puede ser interesante considerar los mecanismos de protección hardware y de redundancia que la tecnología nos proporciona:

• UPS o fuentes de corriente ininterrumpida,

• espejado de disco, o tecnología RAID,

• Componentes duplicados,

• Sistemas redundantes.

Una de las más importantes decisiones que un DBA debe tomar es decidir si arrancar la BD en modo ARCHIVELOG o no. Esta decisión tiene sus ventajas

e inconvenientes:

- Ventajas:

o Aunque se pierdan los ficheros de datos, siempre se puede recuperar la BD con una copia antigua de los ficheros de datos y los ficheros de redo log archivados.

o Es posible realizar backups en caliente.

- Inconvenientes:

o Se necesitará más espacio en disco.

o El trabajo del DBA se incrementa al tener que determinar el destino del archivado de los redo log.

Presentación del Backup Los backups se pueden clasificar en físicos y lógicos. Los físicos se realizan cuando se copian los ficheros que soportan la BD. Entre estos se encuentran los backups del SO, los backups en frío y los backups en caliente.

Los backups lógicos sólo extraen los datos de las tablas utilizando comandos SQL y se realizan con la utilidad export/import.

Backups del SO
Este tipo de backup es el más sencillo de ejecutar, aunque consume mucho tiempo y hace inaccesible al sistema mientras se lleva a cabo. Aprovecha el backup del SO para almacenar también todos los ficheros de la BD. Los pasos de este tipo de backup son los siguientes:

1. Parar la BD y el SO

2. Arrancar en modo superusuario.

3. Realizar copia de todos los ficheros del sistema de ficheros

4. Arrancar el sistema en modo normal y luego la BD.

Backups de la BD en Frio
Los backups en frio implican parar la BD en modo normal y copiar todos los ficheros sobre los que se asienta. Antes de parar la BD hay que parar también todos las aplicaciones que estén trabajando con la BD. Una vez realizada la copia de los ficheros, la BD se puede volver a arrancar.

Backups de la BD en Caliente
El backup en caliente se realiza mientras la BD está abierta y funcionando en modo ARCHIVELOG. Habrá que tener cuidado de realizarlo cuando la carga de la BD sea pequeña. Este tipo de backup consiste en copiar todos los ficheros correspondientes a un tablespace determinado, los ficheros redo log archivados y los ficheros de control. Esto para cada tablespace de la BD.

Backups Lógicos con Export/Import
Estas utilidades permiten al DBA hacer copias de determinados objetos de la BD, así como restaurarlos o moverlos de una BD a otra. Estas herramientas utilizan comandos del SQL para obtener el contenido de los objetos y escribirlos en/leerlos de ficheros Una vez que se ha planeado una estrategia de backup y se ha probado, conviene automatizarla para facilitar así su cumplimiento.

Presentación de la Recuperación Oracle proporciona diferentes modos de recuperar un fallo en la BD, y es importante que el DBA conozca cómo funciona cada uno de ellos para determinar cuándo ha de ser utilizado.
Una de las mayores responsabilidades del DBA consiste en tener la BD a punto, y prepararla ante la posibilidad de que se produzca un fallo. Así, ante un fallo el DBA podrá recuperar la BD en el menor tiempo posible. Los procesos de recuperación dependen del tipo de error y de las estructuras afectadas.

Así, los tipos de error que se pueden producir son:
Errores de Usuario
Como por ejemplo un usuario borrando una fila o eliminando una tabla. Estos errores se solucionan importando una tabla de una copia lógica anterior. Si no se dispone de la copia lógica, se puede recuperar la BD en una instancia auxiliar, exportar la tabla en cuestión de la instancia auxiliar e importarla en la instancia operativa.

Fallos de Sentencias
Se definen como la imposibilidad del SGBD Oracle de ejecutar alguna sentencia SQL. Un ejemplo de esto se produce cuando se intenta una selección de una tabla que no existe. Estos fallos se recuperan automáticamente mediante unrollback de la transacción que contenía la sentencia fallida. El usuario necesitará volver a ejecutar otra vez la transacción cuando se haya solucionado la causa del problema.
Fallos de Procesos
Es una terminación anormal de un proceso. Si el proceso era un proceso de usuario, del servidor o de una aplicación el PMON efectuará la recuperación del proceso. Si el proceso era alguno de los de background, la instancia debe de ser parada y arrancada de nuevo, proceso durante el cual se recupera la caida efectuando un roll forward y un rollback de las transacciones no confirmadas.

Fallos de Procesos Fallos de la Red
Algunas veces los fallos en la red producen fallos de proceso, que son tratados

por el PMON. Si en el error de red se ve envuelta una transacción distribuida, una vez que se reestablece la conexión, el proceso RECO resuelve los conflictos automáticamente.

Fallos de Instancia
Pueden deberse a fallos físicos o de diseño del software que hacen que algún proceso background caiga y la instancia con él. La recuperación es automática cuando se levanta la BD, tomandose más o menos tiempo en la recuperación.

Fallos del Sistema
Son los fallos más peligrosos, no sólo porque se pueden perder datos, sino porque se tarda más tiempo en recuperar que los otros fallos. Además se depende mucho de la experiencia del DBA para levantar la BD rápidamente y sin pédida (o casi) de datos. Existen tres tipos de recuperación en Oracle: a nivel de bloque, de thread y física.

Recuperación de bloques
Es el mecanismo de recuperación más simple, y se realiza automáticamente. Se produce cuando un proceso muere justo cuando está cambiando un bloque, y se utilizan los registros redo log en línea para reconstruir el bloque y escribirlo en disco.

Recuperación de threads
Se realiza automáticamente cuando Oracle descubre que una instancia muere dejando abierto un thread, entonces se restauran los bloques de datos modificados que estaban en el cache de la instancia muerta, y cerrando el thread que estaba abierto. La recuperación se efectua automáticamento cuando la BD se levanta.

Recuperación física
Se realiza como respuesta a un comando RECOVER. Se utiliza para convertir los ficheros de backup en actuales, o para restaurar los cambios que fueron perdidos cuando un fichero de datos fue puesto offline sin un checkpoint, aplicando los fichero redo log archivados y en línea.

2.6.2 Principios de Backup

Un backup válido es una copia de la información sobre la BD necesaria para reconstruir la BD a partir de un estado no utilizable de la misma. Normalmente, si la estrategia de backup se basa en la copia de los ficheros de datos y en el archivado de los ficheros redo log, se han de tener copias de los ficheros de datos, de los ficheros de control, de los ficheros redo log activos y también de los archivados. Si se pierde uno de los ficheros redo log archivados se dice que se tiene un agujero en la secuencia de ficheros. Esto invalida el backup, pero permite a la BD ser llevada hasta el principio del agujero realizando una recuperación incompleta.

Diseño de la BD y Reglas Básicas de Backup Antes de nada, es muy importante entender ciertas reglas que determinan la situación de los ficheros y otras consideraciones que afectarán al esquema de backup:

• Es recomendable archivar los ficheros redo log en disco, y luego copiarlos a cinta, pero siempre en un disco diferente del que soporta los ficheros de datos y de redo log activos.

• Los ficheros copias no deben estar en el mismo dispositivo que los originales. No siempre hay que pasar las copias a cinta, ya que si se dejan en disco se acelera la recuperación. Además, si se copian las copias a cinta y se mantienen en el disco, se puede sobrevivir a diversos fallos de dispositivo.

• Se deberían mantener diferentes copias de los ficheros de control, colocadas en diferentes discos con diferentes controladores.

• Los ficheros redo log en línea deben estar multiplexados, con un mínimo de 2 miembros por grupo, residiendo cada miembro en un disco distinto.

• Siempre que la estructura de la BD cambie debido a la inclusión, borrado o renombrado de un fichero de datos o de redo log, se debe copiar el fichero de control, ya que almacenan la estructura de la BD. Además, cada fichero añadido también debe ser copiado. El fichero de control puede ser copiado mientras la BD está abierta con el siguiente comando:

• SVRMGR¿ alter database backup controlfile to 'destino';
Teniendo en cuenta las reglas anteriores, los siguientes puntos pueden considerarse un ejemplo de estrategia de backup:

1. Activar el modo ARCHIVELOG.

2. Realizar un backup al menos una vez a la semana si la BD se puede parar. En otro caso, realizar backups en caliente cada día.

3. Copiar todos los ficheros redo log archivados cada cuatro horas. El tamaño y el número de ellos dependerá de la tasa de transacciones.

4. Efectuar un export de la BD semanalmente en modo RESTRICT.

Backups Físicos Los backups físicos son aquellos que copian físicamente los ficheros de la BD. Existen dos opciones: en frío y en caliente. Se dice que el backup es en frio cuando los ficheros se copian con la BD esta parada. En caliente es cuando se copian los ficheros con la BD abierta y funcionando.

Backup en Frío
El primer paso es parar la BD con el comando shutdown normal. Si la BD se tiene que parar con inmediate o abort debe rearrancarse con el modo RESTRICT y vuelta a parar en modo normal. Después se copian los ficheros de datos, los de redo log y los de control, además de los redo log archivados y aún no copiados.
Una buena idea es automatizar todo este proceso con los scripts correspondientes, de modo que no nos olvidemos de copiar ningún fichero.
Como este tipo de backup es una copia de los ficheros de la BD, si estos contienen algún tipo de corrupción, la traspasaremos a la copia de seguridad sin detectarla. Por esto es importante comprobar las copias de seguridad.

Backup en Caliente
Si la implantación de BD requiere disponibilidad de la misma 24h. al día, 7 dias a la semana no se pueden realizar backups en frio. Para efectuar un backup en caliente debemos trabajar con la BD en modo ARCHIVELOG. El procedimiento debackup en caliente es bastante parecido al frio. Existen dos comandos adicionales: begin backup antes de comenzar y end backup al finalizar el backup. Por ejemplo, antes y después de efectuar un backup del tablespace users se deberían ejecutar las sentencias:

SVRMGR¿ alter tablespace users begin backup;
SVRMGR¿ alter tablespace users end backup;
Así como el backup en frio permitía realizar una copia de toda la BD al tiempo, en los backups en caliente la unidad de tratamiento es el tablespace. El backup en caliente consiste en la copia de los ficheros de datos (por tablespaces), el actual fichero de control y todos los ficheros redo log archivados creados durante el periodo de backup. También se necesitarán todos los ficheros redo log archivados después del backup en caliente para conseguir una recuperación total.

Backups Lógicos Este tipo de backups copian el contenido de la BD pero sin almacenar la posición física de los datos. Se realizan con la herramienta export que copia los datos y la definición de la BD en un fichero en un formato interno de Oracle.
Para realizar un export la BD debe estár abierta. Export asegura la consistencia en la tabla, aunque no entre tablas. Si se requiere consistencia entre todas las tablas de la BD entonces no se debe realizar ninguna transacción durante el proceso deexport. Esto se puede conseguir si se abre la BD en modo RESTRICT.
Entre las ventajas de efectuar un export están las siguientes:

• Se puede detectar la corrupción en los bloques de datos, ya que el proceso de export fallará.

• Protege de fallos de usuario, por ejemplo si se borra una fila o toda una tabla por error es fácil recuperarla por medio de un import.

• Se puede determinar los datos a exportar con gran flexibilidad.

• Se pueden realizar exports completos,
incrementales y acumulativos.

• Los backups relizados con export son portables y sirven como formato de intercambio de datos entre BDs y entre máquinas.

Una de las desventajas de realizar backups lógicos con export es que son mucho más lentos que los backups físicos.

Modos de Export
Existen tres modos de realizar una exportación de datos:
Modo Tabla

Exporta las definiciones de tabla, los datos, los derechos del propietario, los índices del propietario, las restricciones de la tabla y los disparadores asociados a la tabla.

Modo Usuario
Exporta todo lo del modo de Tabla más los clusters, enlaces de BD, vistas, sinónimos privados, secuencias, procedimientos, etc. del usuario.

BD Entera
Además de todo lo del modo Usuario, exporta los roles, todos los sinónimos, los privilegios del sistema, las definiciones de los tablespaces, las cuotas en los tablespaces, las definiciones de los segmentos de rollback, las opciones de auditoría del sistema, todos los disparadores y los perfiles.

El modo BD entera puede ser dividido en tres casos: Completo, Acumulativo e Incremental. Estos dos últimos se toman menos tiempo que el completo, y permiten exportar sólo los cámbios en los datos y en las definiciones.

Completo

Exporta todas las tablas de la BD e inicializa la información sobre la exportación incremental de cada tabla. Después de una exportación completa, no se necesitan los ficheros de exportaciones acumulativas e incrementales de la BD anteriores.

exp userid=system/manager full=y inctype=complete constraints=Y

file=full$_{e}xport_{f}ilename$

Acumulativo

Exporta solo las tablas que han sido modificadas o creadas desde la última exportación Acumulativa o Completa, y registra los detalles de exportación para cada tabla exportada. Después de una exportación acumulativa, no se necesitan los ficheros de exportaciones incrementales de la BD anteriores.

exp userid=system/manager full=y inctype=cumulative constraints=Y

file=cumulative$_{e}xport_{f}ilename$

Incremental

Exporta todas las tablas modificadas o creadas desde la última exportación Incremental, Acumulativa o Completa, y registra los detalles de exportación para cada tabla exportada. Son interesantes en entornos en los que muchas tablas permanecen estáticas por periodos largos de tiempo, mientras que otras varían y necesitan ser copiadas. Este tipo de exportación es útil cuando hay que recuperar rápidamente una tabla borrada por accidente.

exp userid=system/manager full=y inctype=incremental constraints=Y
file=incremental$_{e}xport_{f}ilename$
$Lapolíticadeexportaciónpuedeserlasiguiente : realizarunaexportacióncompletaeld$ía1($porejemploeldomingo$)

2.6.3 Principios de la Recuperación

Para entender los principios de la recuperación, se necesita entender las estructuras de datos subyacentes utilizadas en la recuperación.

2.6.4 Definiciones y Conceptos

Los ficheros redo log contienen los cambios realizados sobre la BD. Conviene presentar algunos conceptos relacionados con ellos.

Vector de Cambio
describe un cambio simple en un bloque de datos de la BD. Entre otros datos, contiene el número de versión, el código de la transacción, y la dirección del bloque afectado.
Registro Redo log

Es un conjunto de vectores de cambio que describen un cambio atómico sobre la BD. La transacción es también la unidad de recuperación.
Evolución de Redo log por día

se puede calcular ejecutando el comando archive log list en dos días consecutivos y calculando la diferencia del número de secuencia de los ficheros redo

log, multiplicado por el tamaño de un fichero redo log:

SVRMGR¿ archive log list;
Database log mode No Archive Mode
Automatic archival Disabled
Archive destination /opt/app/oracle/admin/demo/arch/arch.log
Oldest online log sequence 3
Current log sequence 5
System Change Number, SCN
Es un dato que define la versión confirmada de la BD en este instante de tiempo. Cuando una transacción es confirmada, se le asigna un SCN que la identifica unívocamente. Los ficheros redo log son marcados con dos SCN. Cuando se abre un nuevo fichero redo log se le marca con un SCN, low SCN, que es uno mas que el SCN mayor del anterior fichero redo log; y su high SCN es puesto a infinito. Los SCN también se asocian al fichero de control, ya que cuando se para una BD, un tablespace o fichero de datos, se almacena para cada fichero de datos su stop SCN en el fichero de control.

Cambio de redo log
es el proceso mediante el cual se deja de utilizar un fichero redo log y el LGWR combia al siguiente fichero redo log disponible. Se puede hacer con el comando alter system switch logfile;.
Checkpoints
son activados automáticamente durante el funcionamiento normal de la instancia, pero pueden ser activados manualmente con el comando alter system checkpoint local o alter system checkpoint global dependiendo si nos referimos a la instancia en la que estamos, o si queremos que afecte a todas las instancias activas, respectivamente. Cada checkpoint lleva implicito un SCN, y Oracle asegura que todos los cámbios con un SCN menor que el del checkpoint dado han sido escritos en el disco.

Métodos de Recuperación Existen varios métodos de recuperación, pero todos ellos se basan en la aplicación de los registros de redo log.
Aplicación de Redo Log
Cuando una BD se arranca con el comando startup, la BD pasa por los estados nomount, mount y open. En este tercer estado, se verifica que se pueden abrir todos los ficheros de log y de datos. Si la BD se arranca por primera vez después de una caida, se necesitará efectuar una recuperación que consiste en dos pasos: avanzar la BD hacia adelante aplicando los registros redo log, deshacer las transacciones no confirmadas.
Cada fichero de datos tiene en su cabecera el último checkpoint efectuado, así como el fichero de control también lleva esa cuenta. El checkpoint lleva incluido el SCN. Este es conocido como SCN de inicio de fichero. Asociado a cada fichero de datos el fichero de control tiene el SCN de final, puesto inicialmente a infinito. El SCN de inicio se incrementa con cada checkpoint.
Cuando la BD se para en modo normal o inmediato iguala el SCN de parada

para cada fichero de datos al SCN almacenado en cada fichero de datos. Cuando se abre otra vez la BD se realizan dos comprobaciones. La primera es mirar si el contador de checkpoints en la cabecera de los ficheros de datos coincide con el correspondiente del fichero de control. Si es así, se compara el SCN de inicio de cada fichero de datos con el SCN de final almacenado en el fichero de control. Si son iguales no se necesita recuperación en este fichero de datos. Como parte de la apertura se pone a infinito el SCN de final para ese fichero de datos.
Si la BD se paró con en modo abort no se ejecutó el checkpoint y el SCN de fin para los fichero de datos está a infinito. Así, durante la BD se abre, y suponiendo que el contador de checkpoints coincide, se comparan los SCN de inicio y de final, y como el último es infinito se efectura una recuperación aplicando los cambios almacenados en los ficheros redo log en línea para avanzar la BD, y los registros de roll back de los segmentos de roll back para deshacer las transacciones no confirmadas.
Si después de parar la BD se reemplaza un fichero de datos por su copia de seguridad, al arrancar la BD Oracle detecta que el contador de checkpoints del fichero de datos no coincide con el almacenado en el fichero de control. Así, se tendrá que echar mano a los ficheros redo log archivados, empezando por aquel cuyo número de secuencia aparece en la cabecera del fichero de datos.

Recuperación Física La utilización de una copia de backup de ficheros de datos siempre necesita de una recuperación física. También es así cuando un fichero de datos se pone offline sin un checkpoint.
Oracle detecta que se necesita una recuperación física cuando el contador de checkpoints de la cabecera del fichero de datos no coincide con el correspondiente contador de checkpoints del fichero de control. Entonces se hace necesario el comando recover. La recuperación comienza en el SCN menor de los ficheros de datos en recuperación, aplicando los registros de redo log a partir de él, y parando en el SCN de final mayor de todos los ficheros de datos.
Existen tres opciones para realizar una recuperacion física. La primera es una recuperación de BD donde se restaura la BD entera. La segunda es una recuperación de tablespace donde, mientras una parte de la BD está abierta, se puede recuperar un tablespace determinado. Esto significa que serán recuperados todos los ficheros de datos asociados al tablespace. El tercer tipo es la recuperación de un fichero de datos específico mientras el resto de la BD está abierta.
Requisitos para Utilizar Recuperación Física
La primera condición que se ha de poner para poder recuperar físicamente una BD es que ésta se esté utilizando en modo ARCHIVELOG. De otro modo, una recuperación completa puede que no sea posible. Si trabajamos con la BD en modoNOARCHIVELOG, y se hace una copia semanal de los ficheros de la BD, se debería estar preparado para perder, en el peor de los casos, el trabajo de la última semana si sucede un fallo. Ya que los ficheros de redo log contendrían un agujero y no se podia avanzar la BD hasta el intante anterior al fallo. En este caso el único medio para reconstruir la BD es hacerlo desde un export completo, recreando el esquema de la BD e importando todos los datos.

Recuperación de la BD
La BD debe estar montada pero no abierta. El comando de recuperación es el siguiente:

RECOVER [AUTOMATIC] [FROM 'localizacion'] [BD]
[UNTIL CANCEL]

[UNTIL TIME fecha]

[UNTIL CHANGE entero]

[USING BACKUP CONTROLFILE]

Las opciones entre corchetes son opcionales:

• AUTOMATIC hace que la recuperación se haga automáticamente sin preguntar al DBA por el nombre de los ficheros redo log. También se puede utilizar para este cometido el comando set autorecovery on/off. Los ficheros redo log deben estar en la localización fijada en $\mathrm{LOG}_{A}RCHIVE_{D}ESTyelformatodelnombredelosficherosdebeserelfij$

• FROM se utiliza para determinar el lugar donde están los ficheros redo log, si es distinto del fijado en $\mathrm{LOG}_{A}RCHIVE_{D}EST$.

• UNTIL sirve para indicar que se desea realizar una recuperación incompleta, lo que implica perder datos. Solo se dará cuando se han perdido redo log archivados o el fichero de control. Cuando se ha realizado una recuperación incompleta la BD debe ser abierta con el comando alter database open resetlogs, lo que produce que los redo log no aplicados no se apliquen nunca y se inicialice la secuencia de redo log en el fichero de control. Existen tres opciones para parar la recuperación:

UNTIL CANCEL permite recuperar un redo log cada vez, parando cuando se teclea CANCEL.

o UNTIL TIME permite recuperar hasta un instante dado dentro de un fichero de redo log
o UNTIL CHANGE permite recuperar hasta un SCN dado.
o USING BACKUP CONTROLFILE utiliza una copia de seguridad del fichero de control para gobernar la recuperación.

Recuperación de un tablespace
La BD debe estar abierta, pero con el tablespace a recuperar offline. El comando de recuperación es el siguiente:

RECOVER [AUTOMATIC] [FROM 'localizacion']

TABLESPACE nombre$_{t}ablespace[, nombre_{t}ablespace]$

Recuperación de un Fichero de Datos

La BD debe estar abierta o cerrada, dependiendo del fichero a recuperar. Si el fichero a recuperar es de un tablespace de usuario la BD puede estar abierta, pero con el fichero a recuperar offline. Si el fichero es del tablespace SYSTEM la BD debe estar cerrada, ya que no puede estar abierta con los ficheros del SYSTEM offline. El comando de recuperación es el siguiente:

RECOVER [AUTOMATIC] [FROM 'localizacion']
DATAFILE nombre$_{f}ichero[, nombre_{f}ichero]$

Creando un Fichero de Control
Si el fichero de control ha resultado dañado y se ha perdido se puede utilizar una copia de seguridad del mismo o crear uno nuevo. El comando de creación de un nuevo fichero de control es CREATE CONTROLFILE. Este comando se puede ejecutar sólo con la BD en estado nomount. La ejecución del comando produce un nuevo fichero de control y el montaje automático de la BD.

Un comando interesante que ayuda a mantener los ficheros de control a salvo es el siguiente:

SVRMGR¿ alter database backup controlfile to trace; que produce un script que puede ser utilizado para generar un nuevo fichero de control y recuperar la BD, en caso necesario. El fichero de traza generado es el siguiente:

Dump file /opt/app/oracle/admin/demo/udump/demo$_{o}ra_{5}15.trc$
$Oracle7ServerRelease7.3.2.3.0 - ProductionRelease$
$Withthedistributed, replicationandSpatialDataoptions$
$PL/SQLRelease2.3.2.3.0 - Production$
$ORACLE_{H}OME = /opt/app/oracle/product/7.3.2$
$Systemname : SunOS$
$Nodename : cartan$
$Release : 5.5$
$Version : Generic$
$Machine : sun4m$
$Instancename : demo$
$Redothreadmountedbythisinstance : 1$
$Oracleprocessnumber : 7$
$Unixprocesspid : 515, image : oracledemo$

Fri May 15 11:41:19 1998
Fri May 15 11:41:19 1998

*** SESSION ID:(6.2035) 1998.05.15.11.41.19.000
The following commands will create a new control
file and use it
to open the database.
No data other than log history will be lost.
Additional logs may
be required for media recovery of offline data files. Use this
only if the current version of all online logs are available.
STARTUP NOMOUNT

CREATE CONTROLFILE REUSE DATABASE "DEMO" NORESETLOGS
NOARCHIVELOG
MAXLOGFILES 16
MAXLOGMEMBERS 2
MAXDATAFILES 30
MAXINSTANCES 1
MAXLOGHISTORY 100
LOGFILE
GROUP 1 '/export/home/oradata/demo/redodemo01.log' SIZE 2M,
GROUP 2 '/export/home/oradata/demo/redodemo02.log' SIZE 2M,
GROUP 3 '/export/home/oradata/demo/redodemo03.log' SIZE 2M
DATAFILE
'/export/home/oradata/demo/system01.dbf',
'/export/home/oradata/demo/rbs01.dbf',
'/export/home/oradata/demo/rbs02.dbf',
'/export/home/oradata/demo/rbs03.dbf',
'/export/home/oradata/demo/temp01.dbf',
'/export/home/oradata/demo/tools01.dbf',
'/export/home/oradata/demo/users01.dbf'
;
Recovery is required if any of the datafiles are restored backups,
or if the last shutdown was not normal or immediate.
RECOVER DATABASE
Database can now be opened normally.
ALTER DATABASE OPEN;

Recuperación Lógica Oracle dispone de la herramienta import para restaurar los datos de una BD a partir de los ficheros resultados de un export. Import lee los datos de los ficheros de exportación y ejecuta las sentencias que almacenan creando las tablas y llenándolas de datos.
Para importar un export incremental se puede efectuar la siguiente secuencia de pasos:
1. Utilizar la copia más reciente del import para restaurar las definiciones del sistema:
2.
3. imp userid=sys/passwd inctype=system full=Y file=export$_{f}ilename$

4.$Ponerlossegmentosderollbackonline.$
5.$Importarelficherodeexportacióncompletamásreciente$:
6.7.$impuserid = sys/passwdinctype = restorefull = Yfile = filename$
8.$Importarlosficherosdeexportaciónenmodoacumulacióndesdelaexportacióncompletamásreciente, enordenc$
9.
10.$impuserid = sys/passwdinctype = restorefull = Yfile = filename$
11.$Importarlosficherosdeexportaciónenmodoincrementaldesdelaexportacióncompletaoacumulativamásreci$

12.
13.$impuserid = sys/passwdinctype = restorefull = Yfile = filename$

3 REFERENCIAS

• http://www.expertosensistemas.com/estrategias-de-copias-de-seguridad-i/
• http://www.expertosensistemas.com/estrategias-de-copias-de-seguridad-ii/
• http://www.expertosensistemas.com/estrategias-de-copias-de-seguridad-iii/
• http://www.expertosensistemas.com/estrategias-de-copias-de-seguridad-iv/
• http://soportealpcsac.blogspot.pe/2016/01/estrategias-de-copias-de-seguridad.html
• http://www.oracle.com/technetwork/articles/servers-storage-admin/dbappliancebackupstrategies-519664.pdf/
• https://es.sharelatex.com/learn/Inserting$_I magesPosicionar_l a_i magen$/
ffl$http : //es.slideshare.net/gabrieldesimone549/tutorial - share - latex/$