# Plan de continuidad de la actividad

Las empresas utilizan la informática para almacenar datos que pueden contener información confidencial. Por ello, es importante garantizar su protección tanto durante el almacenamiento como en la entrega de datos.

La disponibilidad permite garantizar el servicio en cualquier circunstancia y para ello se requiere la implementación de soluciones que hagan más fiables los servicios y los medios de almacenamiento.

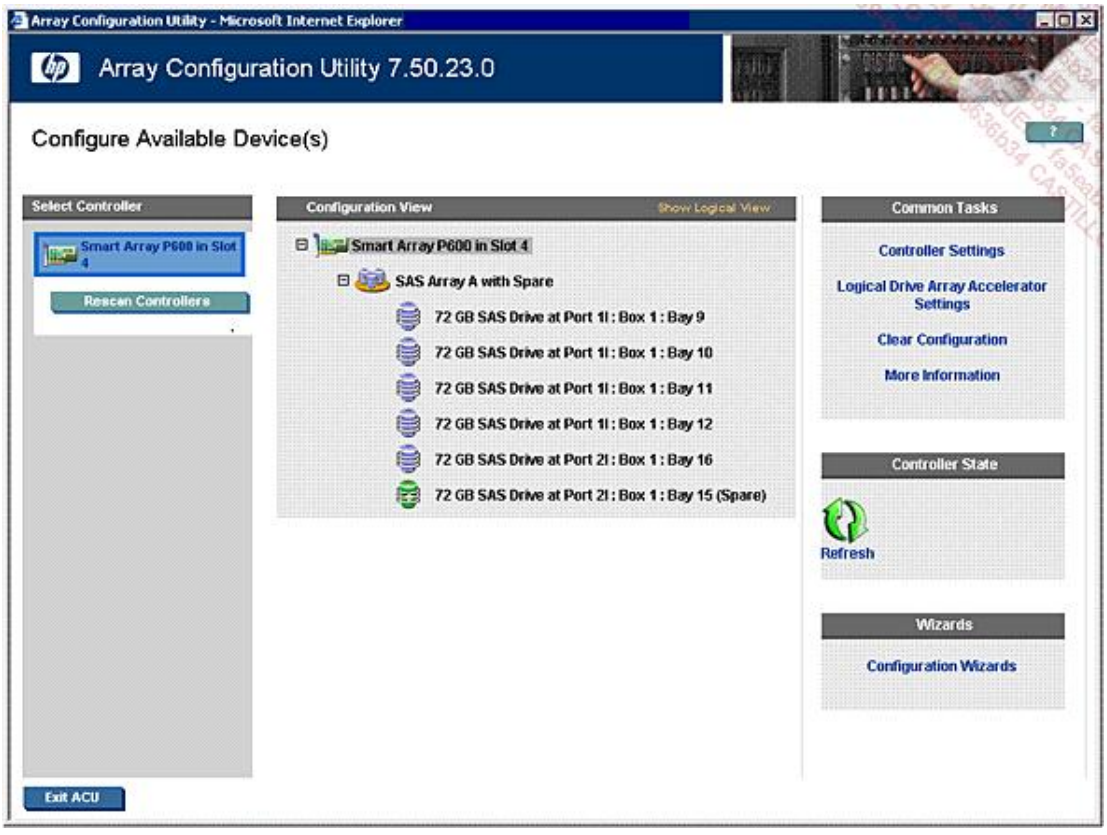
Los principios de confidencialidad también son importantes, ya que protegen la visibilidad de los datos. Los cálculos de integridad permiten, por su parte, prevenir pérdidas de información. Sobre estos conceptos volveremos más tarde en el capítulo Principios de protección de una red.

## 1. Disponibilidad

### a. La fiabilización del sistema de almacenamiento

#### Redundancia de los datos

Es posible implementar una redundancia de medios para garantizar una buena tolerancia a fallos a través de la duplicación de datos en dos o más discos duros. Algunas soluciones *Redundant Array of Inexpensive Disks* (RAID), o conjunto redundante de discos independientes, permiten esta alternativa.




*Utilidad de configuración HP*

#### Protección eléctrica

A veces, también es necesario proteger eléctricamente las máquinas imprescindibles de una red (servidores, equipos de conexión...) contra las subidas de tensión o los cortes eléctricos. Con este fin, los Sistemas de Alimentación Ininterrumpida (SAI) o (UPS - *Uninterruptible Power Supply*) actúan como filtro de tensión. Permiten también compensar la alimentación principal del hardware conmutando la fuente de alimentación con una batería.

*Sistema de alimentación ininterrumpida*

### Sistema transaccional de archivos

Este sistema de transacción se establece explícitamente en el sistema de archivos (en el caso de Novell Netware), o implícitamente como en el caso de Linux (Ext4) y Windows (NTFS).

Igualmente se puede hablar de JFS (*Journaled File System*), disponible en IBM AIX o ZFS (*Z File System*), de Sun Solaris.

### Integridad de datos y CRC

Los sistemas de archivos ejecutan un mecanismo de cálculo de integridad de los datos almacenados, a través de códigos de redundancia cíclicos (CRC - *Cyclic Redundancy Check*).

El inicio de un cálculo de CRC es un polinomio generador, cuyo valor binario es conocido, por ejemplo los 17 bits 10001000000100001 para un CRC de 16 bits. Se efectúa un cálculo a partir de este polinomio y de los bits que deben comprobarse. Cuando se repiten las mismas operaciones, el resultado se compara con el anterior para comprobar que no hay error. El sistema está diseñado para detectar tanto los errores repartidos aleatoriamente como los secuenciales, de longitud inferior al tamaño del polinomio. La mayoría de los tramos de errores superiores o iguales al polinomio también pueden identificarse.

## b. La fiabilización de los intercambios

### Soporte físico fiable

Una manera sencilla de garantizar una fiabilidad en el intercambio de información es utilizar un soporte de transmisión fiable, por ejemplo la fibra óptica, insensible a cualquier perturbación electromagnética.

### Puntos de sincronización

En el intercambio de información crucial, como la que permite la actualización de bases de datos, es necesario poder efectuar una recuperación del contexto antes del incidente, estableciendo estas protecciones de contexto o puntos de sincronización.

Guardando periódicamente las modificaciones, es posible recuperar el contexto inmediatamente anterior al incidente. De hecho, es importante saber exactamente cuáles fueron las modificaciones que se tuvieron en cuenta

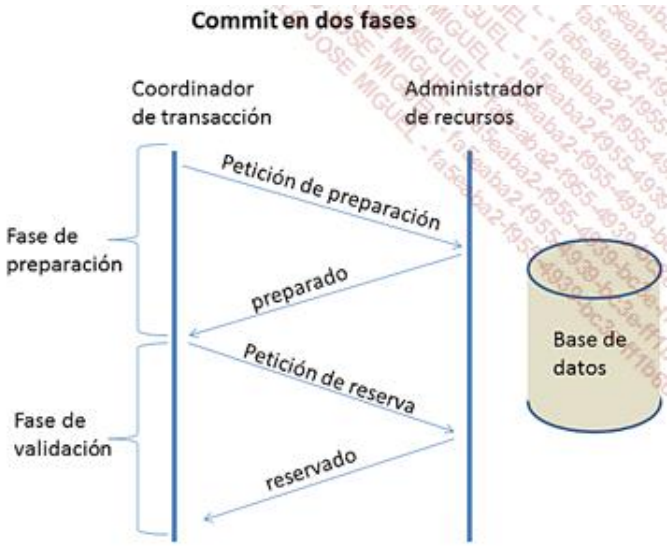
durante la última transacción anterior al incidente.

### Protocolos en modo conectado

Los protocolos conectados aseguran fiabilidad en los intercambios gracias a los acuses de recibo y a los códigos de redundancia cíclicos.

### Transacciones a nivel de aplicación

Cuando, por ejemplo, se realizan actualizaciones importantes en bases de datos, es esencial hacer operaciones unitarias, incluso si hay problemas. Para esto, uno de los mecanismos más conocidos es el **«commit» (validación) de dos fases**.




## 2. Confidencialidad

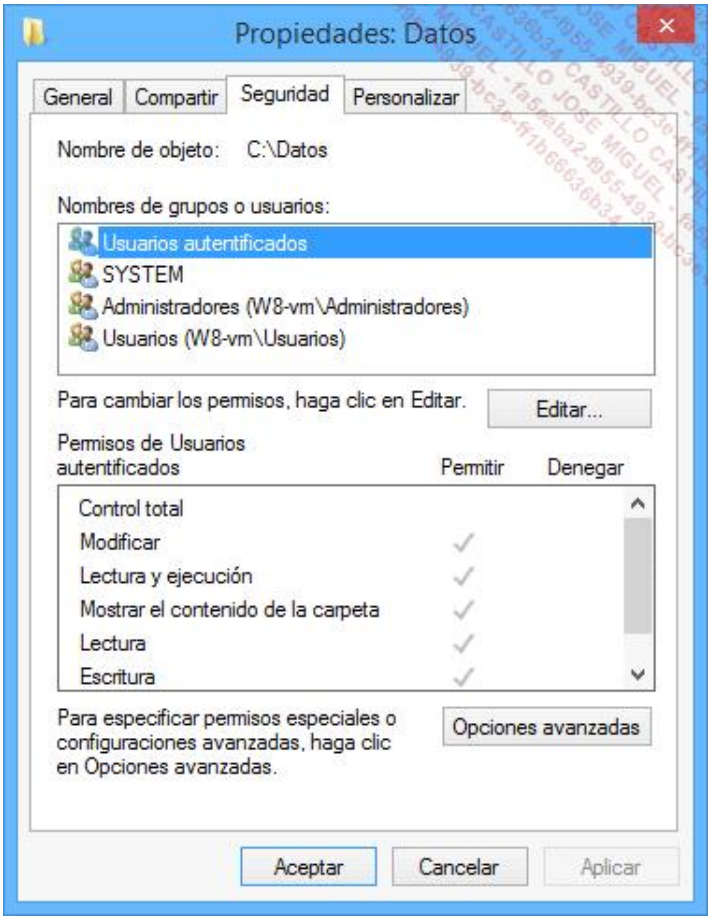
### a. La seguridad del sistema de archivos

La primera solución para garantizar la confidencialidad de los datos puede ser aportada por el sistema de archivos que utiliza el sistema operativo.

Para poner en marcha la seguridad local, es necesario poder identificar cada acceso.

Para poder identificar, ante todo es necesario autentificar los usuarios. Por ello, en un sistema de archivos seguro, es necesario basarse en la autentificación inicial.

Un sistema de archivos seguro tiene en cuenta a los usuarios del sistema para administrar reglas de seguridad personalizadas a nivel de los archivos.




*Administración de permisos locales en Windows 8*

Por ejemplo: los sistemas Windows ofrecen NTFS (*New Technology File System*). Linux utiliza el sistema de archivos Ext4, que muestra los permisos elementales (RWX) para tres tipos de usuario (el usuario propietario, el grupo propietario y el resto). Los sistemas operativos Unix utilizan sistemas de archivos diferentes pero que emplean los mismos conjuntos de permisos.

## b. La protección de los intercambios

### Autentificar

El establecimiento de una conexión a menudo está precedido por una autentificación que valida el acceso a los recursos remotos.

De hecho, todos podemos marcar un número de teléfono para conectarnos con un módem remoto o introducir la dirección de un servidor público. Para ello es necesario validar el acceso a la red en primer término y después el acceso a la información.

### El cifrado

La confidencialidad de la información es necesaria a menudo durante la transmisión de datos en distintos y variados soportes. De hecho, tomando como principio que es imposible impedir a alguien interceptar las tramas en una red y que resulta incluso menos posible saber si nuestras tramas han sido leídas, es preferible procurar que la información transmitida no sea legible para cualquiera.

Para convertir esta información en confidencial, se debe codificar mediante un cifrado, también llamado encriptado. De esta manera solo el emisor y el receptor pueden leerlo.

Las herramientas de análisis de tramas permiten la lectura y la interpretación de los flujos que circulan si no están cifrados. Microsoft proporciona, con las versiones de servidor de sus sistemas operativos, un programa de este tipo, el monitor de red, en una versión limitada.

Igualmente podemos encontrar herramientas gratuitas, WireShark y TCPDump, disponibles para varios sistemas operativos y que pueden descargarse de Internet.

Los sitios web www.wireshark.org y www.tcpdump.org permiten obtener información sobre estas herramientas, así como acceder a su descarga.

#### Internet y confidencialidad

Un dato confidencial que viaja por Internet, como el número de una tarjeta de crédito, puede ser interceptado por personas mal intencionadas si este no está encriptado.

Por ello recurrimos al cifrado de la información confidencial (nombre y contraseñas) o incluso de la totalidad de los datos.

También la legislación al respecto ha evolucionado en España. Los métodos de cifrado pueden superar los 128 bits en ciertas condiciones.

## 3. Redundancia de datos

### a. La tolerancia a fallos

La tolerancia a fallos se puede definir como una configuración de hardware o software que permite prevenir uno o más tipos de averías susceptibles de perjudicar el buen funcionamiento del sistema, de retrasar o afectar un proceso o un usuario.

Para los discos duros, aunque existen soluciones de software, se utiliza especialmente la tolerancia a fallos por hardware. Esta permite la sustitución en caliente (*hot plug*), es decir, sin apagar el ordenador. Entre las soluciones que ofrecen tolerancia a fallos, encontramos:

- RAID 1, o espejo (*mirroring*), en el cual las operaciones de lectura y escritura tienen lugar simultáneamente en dos discos.
- RAID 2, otro dispositivo de espejo que no necesita un segundo disco en las operaciones de lectura (obsoleta).
- RAID 3, bloques de intervalo con paridad hacia un disco dedicado.
- RAID 5, bloques de intervalo con paridad distribuida conectados a un ensamblaje de discos.
- RAID 5 + 1, combinación de bloques de intervalo con paridad, puestos en espejo.
- RAID 0 + 1, combinación de *stripping* (bloques de intervalo) y espejo...

Ninguna de las soluciones RAID incluye la tolerancia a fallos. Por ello, el modo RAID 0, calificado de bloques de intervalo (stripping) sirve principalmente para acelerar las operaciones de escritura, ya que distribuye los datos entre varios discos y de manera transparente para el usuario.

Dentro de un servidor, los componentes como la alimentación y los ventiladores también disponen de mecanismos

de tolerancia a fallos.

*Servidor 2U con alimentación redundante*

Los tradicionales, completos y autónomos servidores en forma de torre se han visto reemplazados hoy día por versiones integrables en estantes (*racks*). Su tamaño es más pequeño debido a que se han quitado algunos componentes. Se les llama servidores pizza, aunque incorporan discos duros o placas (*blade*), tarjetas muy simples que integran un mínimo de componentes.

*Placas en chasis*

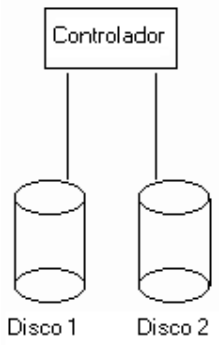
De esta manera, resulta mucho más sencillo duplicar los servidores e implementar mecanismos de tolerancia a fallos a este nivel. Los datos puede traspasarse entre dispositivos llamados bahías de discos, que también se colocan en *racks*.

*Sistema de almacenamiento de discos IBM*

### b. El espejo de discos

En el modo espejo, se conectan dos o más discos duros al mismo bus de datos. Los bloques de datos grabados en el disco primario también se graban en el disco secundario.

Los discos funcionan en tándem. Graban y actualizan los mismos archivos. En caso de fallo de uno de los discos, el otro continúa funcionando ininterrumpidamente y sin pérdida de datos.



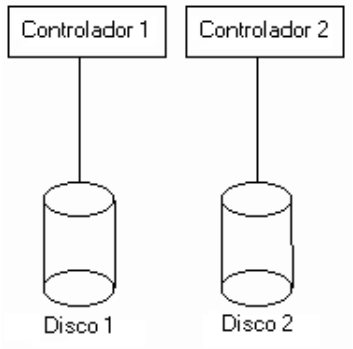

El modo espejo no es suficiente para garantizar la protección de los datos. De hecho, si los dos discos duros sufren una avería al mismo tiempo, o si el propio ordenador presenta algún defecto, se pierden los datos. Contra esto, se recomienda hacer copias de seguridad regularmente.

En caso de fallo de uno de los discos, el sistema operativo envía un mensaje para reportar el incidente y para que la protección en modo espejo se restablezca cuanto antes. Como este modo duplica los datos de los discos que se encuentran conectados al mismo bus de datos, no puede garantizar la protección entre los discos duros y el servidor en caso de avería del bus de datos. Un incidente de este tipo implicará un fallo de los dos discos a la vez.

### c. El espejo de controladores y discos

Este método de duplicación de datos permite garantizar la protección de los datos. Consiste en copiar los datos en dos discos distintos, utilizando dos buses de datos distintos.

Así se protegen los datos en caso de fallo de un disco duro o del bus de datos que conecta el disco duro con el servidor (este bus de datos incluye la controladora de discos y el cable de interfaz). Si uno de los elementos de un bus de datos está defectuoso, el otro disco sigue funcionando, ininterrumpidamente y sin pérdida de datos, puesto que se transmiten por otro bus de datos. En este caso, el sistema operativo enviará un mensaje de advertencia para indicar que una unidad está defectuosa.




Tampoco basta con el modo duplicado para garantizar la protección de los datos. De hecho, si los dos buses de datos de los discos sufren una avería en el mismo momento o si el propio ordenador presenta algún defecto, se pierden los datos. En este caso, también se recomienda hacer copias de seguridad regularmente.

En modo duplicado los mismos datos se registran simultáneamente en todos los discos. Para los discos que están conectados a buses diferentes, la transferencia de datos es mucho más rápida que en el modo espejo, donde los datos se transmiten sucesivamente hacia los discos y a través del mismo bus de datos.

Este modo también posibilita las búsquedas distribuidas que envían solicitudes de lectura hacia varios discos y esperan una respuesta más rápida. Si varias solicitudes llegan al mismo tiempo, se distribuyen entre los discos

duplicados y, en consecuencia, son tratadas simultáneamente.

## d. Bloques de intervalo con paridad

### Bloques de intervalo

El modo de escritura en bloques de intervalo (*stripping*) ejecuta simultáneamente varios discos con el fin de acelerar los procesos. Además de no permitir la tolerancia a fallos, disminuye el tiempo de lectura.

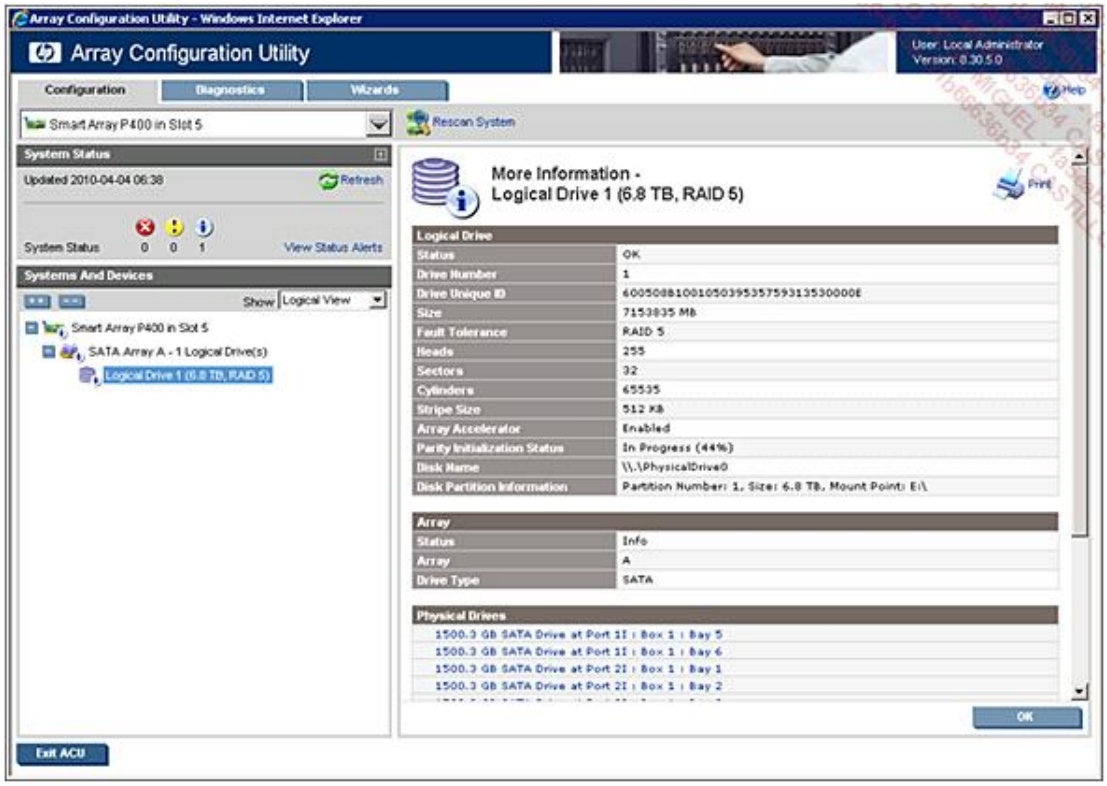
Cada uno de los soportes está dividido en bloques pequeños de igual tamaño. La escritura de un archivo podrá abarcar una serie de bloques repartidos en varios discos duros.

El bloque de intervalos está estandarizado con el nombre RAID 0.

### RAID 3, RAID 5 y RAID 6

Los bloques de intervalo con paridad representan el sistema más utilizado para concebir una estrategia de tolerancia a fallos de disco.

RAID 3 es una solución en la que la paridad se almacena en un disco dedicado. Con RAID 5, la información de paridad se distribuye en un disco diferente en cada intervalo.




*Configuración RAID 5*

La técnica RAID 6 es una evolución de RAID 5. Las soluciones 3 y 5 solo permiten un fallo de disco en la serie. Si se produce el fallo en dos unidades, se pierden los datos almacenados y hay que restaurarlos. Aquí, las operaciones de paridad se duplican y se vuelven más complejas, lo que permite el fallo conjunto de dos discos duros sin incidencia para el usuario. Con la disminución de costes, esta solución, que no es nueva, se utiliza cada vez más.

## Paridad

Además de escribirse en el bloque de intervalos, la información de paridad se registra en un disco con el fin de recuperar los datos en caso de fallo de uno de ellos, cualquiera que sea.

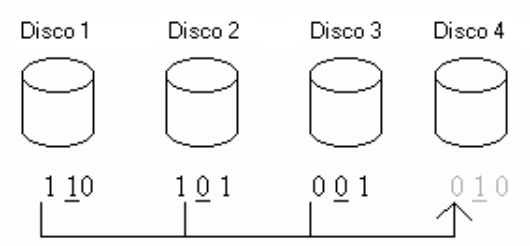
Para una solución que implique n discos, la información que debe escribirse se divide para ser distribuida entre los n-1 discos.

Por ejemplo, para escribir '110 101 001', se reparte en el bloque de intervalos constituido por cuatro discos.

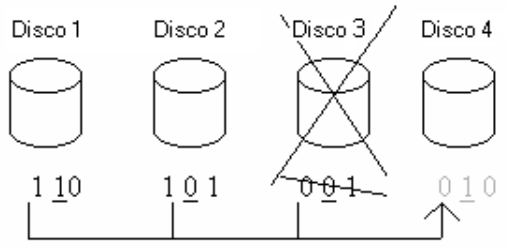
Para cada símbolo en enésima posición de cada disco, se calcula la información de paridad: lo que equivale a calcular el número de '1' para una posición dada y asignarle el enésimo intervalo, donde se almacenará la paridad, para que la determinación del número global de '1' sea par (paridad uniforme).

Así, si tomamos el primer símbolo de cada uno de los tres discos, obtendremos: '1 1 0'. Se determina el primer símbolo del disco 4 eligiendo '0', de modo que el número '1' sea par. De esta manera hay dos símbolos '1' entre los cuatro discos.

De la misma manera, para los símbolos que se encuentran en segunda posición, es decir, '1 0 0', se elige '1' como segundo símbolo en el último disco. Se obtiene así '0 1 0' como información de paridad para el disco 4. En caso de fallo de uno de los discos, por ejemplo el segundo, se recalcula la información perdida de la misma manera que si se tratara de información de paridad.




A partir de los discos 1, 2 y 4, se seleccionan los primeros símbolos de cada uno: '1 1 0' Se calcula el símbolo necesario para obtener un número par de '1', es decir '0'.




Se efectúa la misma operación para los segundos símbolos y luego para los terceros. Se localizan '0 0 1', lo que nos permite reconstruir la información global representada como '110 101 001', y todo esto a pesar de que uno de los discos duros esté defectuoso.

El cálculo de paridad en el nivel más bajo es efectuado por una UO (Unidad Organizativa) exclusiva (XOR). De esta manera, la paridad del disco 4 es d4 = 110 XOR 101 XOR 001, o sea, 010. De este modo es más fácil obtener cualquier información, por ejemplo d3, a partir de los tres discos restantes. Por ejemplo, d3 = 110 XOR 101 XOR 010.

La UO exclusiva se basa en la lógica siguiente: 0 XOR 0 = 0, 0 XOR 1 = 1, 1 XOR 0 = 1, 1 XOR 1 = 0. Podemos entender la UO exclusiva como una suma binaria con posible pérdida de retención. En el lenguaje oral, podemos

asociarlo con «Queso o postre» en un menú de restaurante, donde solo uno de los dos es una elección válida.

### e. La neutralización de los sectores defectuosos

Este método permite garantizar el almacenamiento correcto de los datos en caso de sectores defectuosos. De hecho, todos los datos se escriben en segundo plano y luego son verificados. Cuando no se consigue escribir después de algunos intentos (es decir, cuando los datos que deben escribirse en la RAM no son los mismos que los escritos en el disco), el sector se marca como defectuoso y los datos se redirigen hacia un espacio reservado del disco. Y se deja de utilizar el sector marcado.

## 4. Soluciones de redundancia en servidor

Las soluciones de redundancia en servidor permiten dos funcionalidades que es necesario distinguir:

- La tolerancia a fallos.
- La distribución de carga.

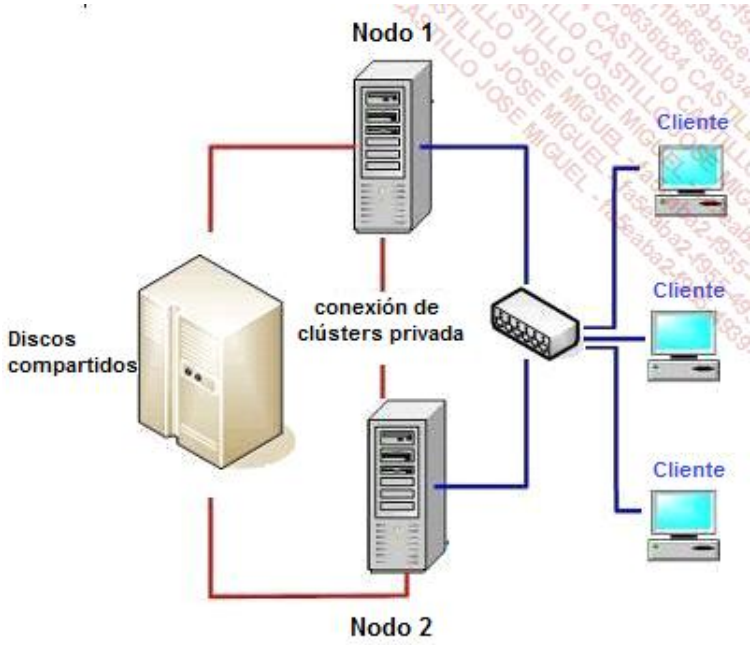
Estas dos funciones pueden ejecutarse simultáneamente.

Este tipo de soluciones posibilita lo que se conoce como alta disponibilidad, ya que ofrece un servicio continuo a los usuarios, incluso en caso de problemas de sobrecarga.

### a. La tolerancia a fallos

En este caso, varios procesos de un sistema operativo de servidores adaptado se ejecutan en distintos servidores. Esta tecnología se conoce como clúster de n nodos y define una solución que ejecuta n procesos de un mismo sistema operativo.

Como ejemplo, en el siguiente recuadro esquematizamos la ejecución de un clúster de dos nodos.




*Esquema de un clúster de dos nodos*

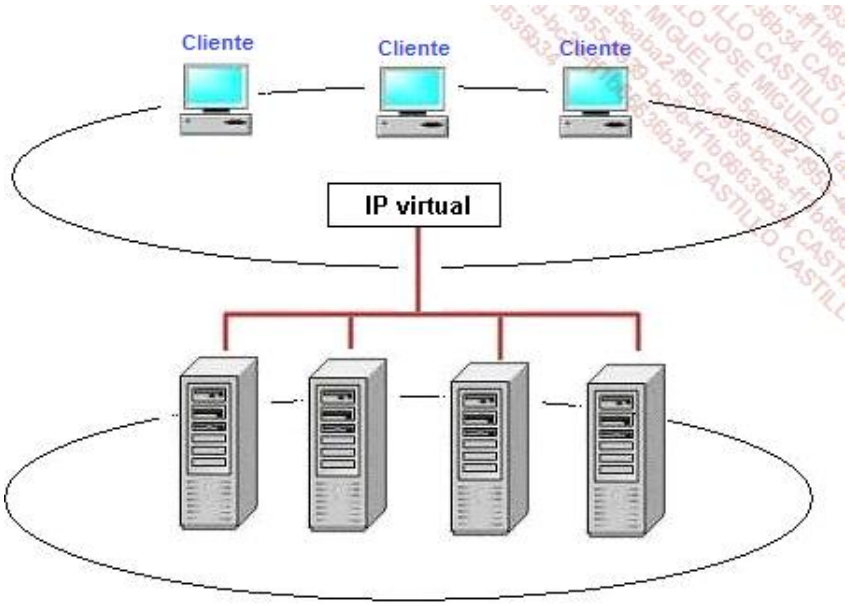
Esta tolerancia a fallos permite mantener el servicio para los usuarios. Por otra parte, es necesario que los datos se mantengan disponibles y actualizados, sea cual sea el servidor que falle.

Si estos datos se mantienen en los discos duros locales de los servidores, se puede poner en marcha una sincronización continua (replicación). Si no, es posible desviar los datos a un pool de almacenamiento compartido (infraestructura NAS).

En este sistema de redundancia de servidores, no todos responden obligatoriamente a las demandas de los usuarios. Este funcionamiento se reserva a las soluciones más evolucionadas. A menudo, un solo servidor ofrece de forma permanente sus servicios a los usuarios (servidor activo) y un segundo permanece preparado para tomar el relevo en caso de fallo del primero (servidor pasivo).

### b. La distribución de la carga de red

El *Network Load Balancing* (NLB) no corresponde en realidad a una solución de hardware, en el sentido que se pueden utilizar ordenadores no dedicados al rol de servidores. Esta labor también es posible realizarla con PC que estén puestos en red.




*Clúster de carga de red equilibrada*

A pesar de que esta solución no es forzosamente la más fiable (con respecto a la utilización de verdaderos servidores), permite disminuir considerablemente los costes de adquisición y además puede constituir una solución interesante para el sector pyme.

El equilibro de carga de red permite proporcionar una solución de alta disponibilidad avanzada. Es perfecta, por ejemplo, para servir sitios web.

Una funcionalidad como esta permite adaptar los resultados vinculados a la aplicación, distribuyendo las peticiones de clientes entre los servidores que forman el clúster. Así pues, cuando el tráfico aumenta, es posible añadir servidores suplementarios al clúster.

Se puede implementar una funcionalidad de «Teaming» en un servidor cuando este posee varias interfaces de red. Ofrece una tolerancia a fallos e incluso una distribución de carga y simula, igual que el NLB, una interfaz virtual con

un punto de entrada único. En este caso se trata de duplicar las tarjetas de red, y no los servidores.

### La virtualización como solución en sí misma

La virtualización es, sobre todo, una solución de consolidación, pero, además, un argumento que nos puede llevar a su implementación es la posibilidad de ofrecer fácilmente altos niveles de disponibilidad.

Una infraestructura virtual puede actuar a varios niveles para mejorar la disponibilidad de la solución:

- reduciendo considerablemente las interrupciones de servicios programados;
- evitando las interrupciones de servicios no programados;
- permitiendo un restablecimiento rápido después de una parada.

De hecho, las soluciones de virtualización en la actualidad permiten mover dinámicamente máquinas virtuales hacia diferentes servidores físicos, y esto, sin interrumpir el servicio. Así, para operaciones de mantenimiento del hardware, no es necesario implementar «ventanas de mantenimiento» correspondientes a periodos de interrupción de servicio, a menudo difíciles de planificar.

La virtualización propone igualmente numerosas ventajas ofreciendo un «teaming» de las interfaces de red o incluso de las rutas de acceso múltiples a los recursos SAN.

También es posible ofrecer una solución que cambie automáticamente cuando haya una incidencia, sin tener ninguna dependencia del hardware específico dedicado, ya que el usuario trabaja en las máquinas virtuales, independientes del hardware.

Las soluciones de software de servicios de clúster permiten igualmente una verdadera configuración de alta disponibilidad.

## 5. Política de respaldo

Para cada archivo creado o modificado, el sistema operativo asigna un bit de archivo o actualiza la fecha de la última modificación. A partir de ahí, es posible determinar qué archivos deben respaldarse.

Los productos Microsoft y Novell se basan en un atributo de archivo. Los sistemas Unix y Linux trabajan con las fechas de los archivos.

Una empresa determinará su política de respaldo para poder responder a varias cuestiones:

- ¿Cuáles son los archivos que deben respaldarse?
- ¿Con qué tipo de respaldo?
- ¿Cuándo efectuar las copias de seguridad?
- ¿En cuántos soportes?
- ¿Es más importante respaldar rápidamente o restaurar rápidamente?
- ¿Cuántas cintas se deben utilizar, de qué manera (rotación de las cintas)?

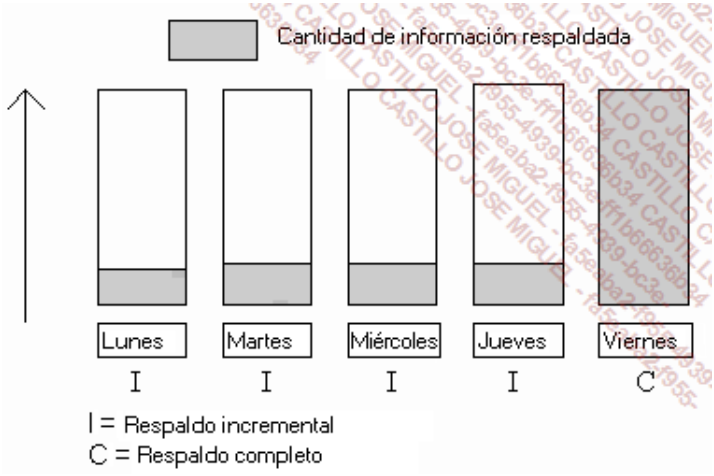
### a. El respaldo completo

En un respaldo completo, los atributos de archivo se reinicializan para almacenar el hecho de que se ha grabado. Si se utiliza la fecha, se debe utilizar la del último respaldo que se guarda, de tal modo que se puedan diferenciar los archivos que se respaldaron de los que aún no (fecha de la última modificación).

### b. El respaldo incremental

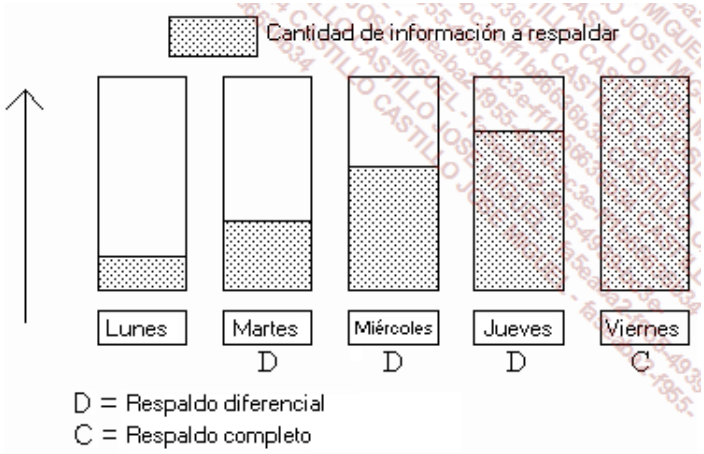
Esto tipo de respaldo marca los archivos como ya grabados. Se realiza, en general, diariamente, y tiene en cuenta las modificaciones del día anterior. Una política semanal consiste, por ejemplo, en efectuar un respaldo completo los viernes y una copia incremental el resto de los días.

Esta política minimiza la duración de la copia diaria. En contraposición, en una restauración completa hasta el último jueves, por ejemplo, sería necesario restaurar la cinta del viernes anterior, más las cuatro cintas correspondientes a cada uno de los días de esa semana.




### c. El respaldo diferencial

Este tipo de respaldo (a menudo diario) no necesita reinicializar los atributos de los archivos para indicar que ya se registraron. Por lo tanto, para cada nuevo respaldo diferencial, se tienen en cuenta las modificaciones anteriores y las del mismo día.




Esta política minimiza el tiempo de restauración, puesto que solo requiere dos cintas (la completa más la última diferencial). Aunque tiene el inconveniente de que la copia diaria es cada vez más larga.

Podemos citar como principales soluciones de copias de seguridad: ARCserve (CA), Backup Exec o Netbackup (Symantec), Networker (EMC), Time Navigator alias TiNa (Atempo), Tivoli Storage Manager alias TSM (IBM).

## 6. Continuidad y reanudación de la actividad en caso de siniestro

### a. Principios

El sistema de información de una empresa no está exento de incidentes, que pueden afectar a uno o más equipos, o incluso de un accidente o problema grave, por ejemplo en la sala de servidores. El coste implicado puede tener consecuencias desastrosas. Se pueden poner en práctica planes y métodos de seguridad para garantizar la continuidad o la reanudación de la actividad en tales casos.

La reacción después de un daño debe ser proporcional a este. Se deberá prever con anterioridad una serie de medios que sucesiva y escaladamente vayan actuando. El primer punto consiste en la redacción de un balance de impacto en la actividad (BIA), que contenga:

- el análisis de los costes financieros;
- la identificación de las aplicaciones críticas;
- la determinación del tiempo necesario para la reanudación de la actividad;
- el detalle de la infraestructura del sistema de información;
- la lista de los usuarios críticos.

El BIA está destinado a facilitar las distintas decisiones que se deban tomar, siempre difíciles después de un accidente. Pueden completarse con:

- soluciones de emergencia y su activación;
- el nombramiento de un departamento de crisis, con especialistas de cada sector, cuyo peritaje se solicitará en ese momento;
- la puesta en marcha de un plan de continuidad de la actividad (PCA) o de un plan de reanudación de la actividad (PRA);
- protocolos y pruebas necesarios.

### b. El plan de continuidad de la actividad (PCA)

El PCA (o BCP - *Business Continuity Plan*) define el conjunto de acciones que garantizan la continuidad de la empresa después de un incidente grave. Debe acompañarse de medidas urgentes; es un plan a corto plazo.

Permite cuantificar las necesidades para poder continuar la actividad, incluso en un estado degradado del sistema, después de una interrupción corta, de algunos segundos a decenas de minutos. Se compone de:

- medidas preventivas;
- redistribución de las principales tareas;
- contractualización con los proveedores y aseguradoras;
- degradación previsible del sistema;
- procedimientos y pruebas.

## c. El plan de reanudación de actividad (PRA)

El plan de reanudación de actividad (o BRP - *Business Recovery Plan*) es el conjunto de los procedimientos que permiten la reanudación de la actividad en un sitio de emergencia después del incidente. La interrupción se calcula desde algunas horas hasta algunos días, hasta que sea posible la aplicación del PCA.

Cada actor del sistema y cada actividad de la empresa es objeto de reanudaciones específicas. Debe haber un PRA por sistema, por entorno, por aplicación, por ámbito de actividad o por sitio, según la política de seguridad definida.

El PRA está constituido por distintos procedimientos.

### Plan de preparación

El plan de preparación determina el entorno necesario para la reanudación. Describe la estructura física del lugar provisional (medios informáticos, red, telecomunicaciones, logística...). Describe también el mapeado lógico de las aplicaciones y los medios humanos que deben solicitarse.

### Plan de ejecución

La definición y la planificación de las etapas de reanudación están en este plan de ejecución, que incluye una descripción de las actividades y responsabilidades de los participantes, así como las acciones que deben emprenderse.

### Plan de recuperación

Este procedimiento prevé la reinstalación de las aplicaciones y la restauración de los datos. Debe incluir una estimación del tiempo necesario para restablecer el funcionamiento.

### Validación y actualización

Las pruebas de validación de procedimientos tampoco deben olvidarse. Así pues, se puede realizar una prueba completa al finalizar la ejecución del PRA.

Y, por supuesto, a todo cambio importante dentro del sistema de información debe corresponder una actualización de estos procedimientos.