Diseñando Sistemas de Alta Disponibilidad y Tolerantes a Fallos

(Versión 1.3)
Puedes descargar la última versión de este documento de:
http://jo.morales0002.eresmas.net/fencasa.html

José María Morales Vázquez

Métodos y Tecnología (MTP). Agastia nº 44-46
28027 Madrid, Spain
josemaria.morales@hispalinux.es

Resumen. La tolerancia a fallos, tal y como la conocemos hoy en día, se basa fundamentalmente en un concepto: redundancia. La mejor forma de asegurar la disponibilidad de nuestros equipos y los servicios que ellos suministran de manera fiable y sin interrupción las 24 horas del día durante siete días a la semana, es la duplicación de todos sus elementos críticos y la disposición de los elementos software y hardware necesarios para que los elementos redundantes actúen cooperativamente, bien sea de forma activa-activa o activa-pasiva, pero siempre de forma transparente para el usuario final. En el presente documento repasaremos los principales elementos de riesgo de un sistema informático, estudiaremos la forma de evitarlos o reducirlos y aplicaremos esta solución a un caso real.

1 Introducción

Siguiendo la taxonomía dada por el grupo de trabajo WG10.4, perteneciente al comité técnico TC-10 de la IFIP (International Federation for Information Processing), la disponibilidad es una medida relativa a la preparación para su utilización de un sistema informático, mientras que la fiabilidad es una medida relativa a su capacidad para mantenerse operativo en el tiempo. Ambas propiedades están englobadas dentro de una propiedad mucho más amplia, la confiabilidad, que también incluye aspectos de seguridad, confidencialidad e integridad de datos.

Todas ellas conllevan un elevado aumento del coste invertido en *hardware* y *software*. Al igual que ocurre en el mundo del deporte, realizar una carrera de 100 metros en menos de 11 segundos es relativamente fácil para un deportista de élite. A partir de aquí, cada décima de segundo de menos será fruto de duras horas de entrenamiento. En el caso que nos ocupa, eligiendo correctamente los componentes de nuestro sistema es relativamente fácil alcanzar un sistema disponible el 98% del tiempo. El paso del 98 al 99 por ciento, y de aquí al 99,999% (lo que los

estadounidenses llaman los cinco nueves del tiempo de funcionamiento) es una tarea compleja que lleva aparejado un aumento exponencial del coste total del sistema.

Las métricas comúnmente utilizadas para medir la disponibilidad y fiabilidad de un sistema son el tiempo medio entre fallos o MTTF (*mean time to failure*) que mide el tiempo medio transcurrido hasta que un dispositivo falla, y el tiempo medio de recuperación o MTTR (*mean time to recover*) que mide el tiempo medio tomado en restablecerse la situación normal una vez que se ha producido el fallo. El tiempo en el que un sistema está fuera de servicio se mide a menudo como el cociente MTTR/MTTF. Lógicamente, nuestro principal objetivo es aumentar el MTTF y reducir el MTTR de forma que minimicemos ese tiempo.

En el presente documento discutiremos la solución adoptada ante un caso real. Se trataba de reconstruir la arquitectura informática de una importante cadena empresarial de nuestro país, con cerca de 100 establecimientos de diferentes tamaños (entre 5 y 50 usuarios en cada uno de ellos) distribuidos por toda la geografía española, y dos grandes centros corporativos: uno con 100 usuarios y el otro con mas de 300 repartidos entre dos edificios distantes entre sí por, aproximadamente, un kilómetro, con el objetivo de hacerlo altamente disponible. El cliente exigía que la solución estuviera basada en productos Microsoft.

2 Estudio de la Solución

La solución que aquí defendemos, por diversos motivos, difiere ligeramente de la que se implantó en la realidad. No obstante, aquí se presentará aquella que nosotros creemos que hubiese sido la solución óptima para el proyecto que nos ocupa dividiéndola en cinco grandes capítulos: infraestructura, servidores, mensajería, arquitectura Web y seguridad. Antes de exponer la solución adoptada en cada uno de estos apartados se discutirán las ventajas e inconvenientes de las diferentes opciones disponibles.

2.1 Infraestructura

La línea de división entre la infraestructura y la arquitectura de un sistema informático es, a menudo, muy difícil de ver. Sobre todo porque si nos planteamos la arquitectura de una organización desde un punto de vista evolutivo, los elementos que en un momento dado se consideran como propios de la arquitectura pasan a ser posteriormente parte de la infraestructura. Esto, por ejemplo, ha ocurrido ya con las redes locales y está empezando a ocurrir con los sistemas de mensajería. Aquí trataremos dentro de este apartado exclusivamente los problemas derivados del suministro eléctrico y los sistemas de comunicaciones.

Suministro Eléctrico. La primera causa de fallos que debemos subsanar en nuestro sistema es la provocada por interrupciones o anomalías en el suministro eléctrico. Si, por el motivo que sea, nuestros equipos se quedan sin energía o ésta les llega alterada nuestro sistema no funcionará en absoluto o no lo hará correctamente. Tres son los posibles problemas que se nos pueden presentar en este aspecto:

- Fallos en las fuentes de alimentación locales de los equipos.
- Fluctuaciones de tensión en el suministro eléctrico.
- Cortes totales de suministro eléctrico.

Fallos las fuentes de alimentación locales de los equipos. Las partes mas débiles de los sistemas informáticos, y las que fallan mas a menudo son las fuentes de alimentación. Todos los filtros, generadores externos y sistemas de alimentación ininterrumpida no nos valen de nada si lo que falla es la fuente de alimentación local de uno de nuestros equipos. Afortunadamente, la mayoría de los servidores de gama alta y elementos críticos de un sistema informático se fabrican hoy en día con una fuente de alimentación redundante o con la posibilidad de instalársela. Si algunos de los equipos vitales para nuestro sistema no disponen de esta opción deberíamos de encargar a sus respectivos fabricantes una fuente de repuesto, mantenerlas todas correctamente etiquetadas para poder identificarlas rápidamente y practicar sus sustitución para estar seguros de poder hacerlo correctamente y en el menor tiempo posible cuando sea necesario.

Fluctuaciones de Tensión. Incluso en las mejores áreas de suministro la corriente eléctrica sufre variaciones. Cuando éstas son pequeñas pueden pasarnos inadvertidas, aunque a la larga fatigan y acortan la vida útil de nuestros equipos. Si estas fluctuaciones son mayores pueden ocasionarnos graves daños materiales. Podemos hablar de cuatro fenómenos distintos englobados dentro de esta categoría: picos de tensión (*spikes*), sobretensiones (*surges*), caídas (*sags*) y bajadas de tensión (*brownouts*).

Los **picos de tensión** son grandes incrementos de la misma de duración infinitesimal. Es posiblemente, de todos los fenómenos que aquí discutiremos, el más peligroso y más difícil de tratar. La mayoría de las veces son ocasionados por factores externos que están totalmente fuera de nuestro control (como el arranque en las proximidades de un gran motor eléctrico o la recuperación después de un corte de suministro de la central eléctrica) y los efectos suelen ser devastadores: estamos hablando de puntas que pueden rondar los 1.000 voltios que, momentáneamente, llegan a equipos diseñados para trabajar a sólo 220.

A la hora de elegir nuestro protector contra estos fenómenos debemos de tener en cuenta fundamentalmente dos parámetros: que la velocidad de reacción del elemento ante los picos sea lo mas elevada posible y que, ante las puntas más severas, el protector se autodestruya a sí mismo aislando nuestro sistema de la red eléctrica como última medida de salvaguarda.

Existen en el mercado diferentes soluciones de propósito general para protegernos de este fenómeno: transistores de sacrificio, arrays de transformadores, transformadores de tensión constante, etc. El coste de las mismas suele ser

directamente proporcional a la verdadera protección que nos proporcionan. Existen protectores mas especializados (y también mas caros) diseñados específicamente para salvaguardar elementos informáticos y que trabajan creando un camino eléctrico alternativo para derivar esos picos de tensión sin que lleguen a afectar a nuestros equipos.

Muchas de las nuevas UPS (*Uninterruptible Power Supply*) también proporcionan protección contra los picos de tensión proporcionándonos un suministro de tensión constante, pero no olvidemos que, como última opción, el protector debe de autodestruirse como medida de seguridad y es mucho mas barato reemplazar o reparar un protector que una UPS.

Las **sobretensiones** son ocasionadas por causas similares a las que generan los picos de tensión, pero suelen ser de mayor duración (unos cientos de milisegundos) y de menor intensidad. La protección contra las sobretensiones es bastante más sencilla que contra los picos: una buena UPS con protección y suministro de tensión constante, o cualquiera de las soluciones antes mencionadas, nos solucionará fácilmente nuestro problema.

Las **caídas de tensión** son el fenómeno opuesto a los picos. No llegan a ser cortes efectivos del suministro, sino meramente descensos muy bruscos de duración infinitesimal que, sin la protección adecuada, puede causar el reseteo de nuestros equipos. Un transformador de tensión constante podría solucionarnos el problema de las caídas menos severas, pero sólo una buena UPS nos proporcionará una protección total contra este fenómeno.

Por último, las **bajadas de tensión** son descensos de alrededor de un 5 o 10 % de la tensión de suministro que, para defenderse de las sobrecargas, las compañías eléctricas realizan deliberadamente. Una buena UPS nos puede proporcionar una protección ocasional, pero si la bajada de tensión es especialmente prolongada, tan sólo un buen transformador de tensión constante podrá aislarnos de este fenómeno.

Cortes totales del suministro Eléctrico. Dentro de los cortes totales de suministro podemos distinguir tres casos: los que duran unos milisegundos (micro-cortes), aquellos que duran unos minutos y los que duran desde una hora hasta varios días.

Los **micro-cortes** pueden provocar, en el mejor de los casos, que los equipos se reinicien y, en el peor, fallos inesperados e imprevisibles de memoria, lectura o escritura en disco, etc. Tienen un efecto particularmente perjudicial cuando se reproducen continuadamente varios de estos cortes, lo que provoca una gran fatiga a los componentes electrónicos de nuestros equipos. No es raro tampoco que uno o varios microcortes vayan acompañados, seguida o intercaladamente, de picos de tensión. La solución a este problema, no obstante, es bien sencilla y basta para solventarlo disponer de una UPS con un protector adicional contra picos de tensión.

Los **cortes** que duran entre unos minutos y una hora pueden solventarse con una UPS de gama media, teniendo siempre en cuenta que debemos de dimensionar adecuadamente la duración de las baterías de la misma en función de la carga de nuestro sistema. No está de más contar, asimismo, con una protección contra picos.

Los cortes de corriente durante tiempos mas prolongados son provocados por problemas mas graves: inundaciones, incendios, catástrofes naturales y similares. Su tratamiento va más allá de la tolerancia a fallos y debería de estudiarse en el plan de

recuperación ante desastres de la compañía. Aquí nos limitaremos a apuntar que, básicamente, debemos decidir qué hacer ante esta eventualidad: podemos mantener nuestro sistema durante un número determinado de horas (dimensionando adecuadamente las baterías de nuestra UPS) y luego detenerlo de forma controlada hasta el restablecimiento de la situación o por el contrario, si necesitamos mantener nuestra organización funcionando aún ante estas circunstancias precisamos de una combinación de UPS más un generador de corriente que también debe de estar adecuadamente dimensionado.

Como anticipamos en la introducción, en la realidad siempre tenemos que alcanzar un compromiso entre la disponibilidad que pretendemos y el coste del sistema.

En el caso que nos socupa, uno de los criterios discriminatorios a la hora de escoger los elementos críticos de la red (servidores, cabinas externas de discos y routers) fue la posibilidad de que incluyesen fuentes de alimentación redundantes.

Se utilizaron, en casi todos los casos, UPS con protección contra picos y estabilizador de salida de tensión constante de la casa CENER. En los centros corporativos se instalaron además sendos generadores de tensión y en uno de ellos, enclavado en una zona industrial (mucho mas propensa a los picos de tensión) se colocaron además protectores específicos contra estos fenómenos. La capacidad de las UPS de las dependencias situadas en zonas propensas a cortes de suministros frecuentes y prolongados se sobredimensionaron ampliamente con respecto al resto.

Infraestructura de comunicaciones. Dividiremos este punto en dos apartados: el primero relativo a la infraestructura de comunicaciones local y el segundo en el que estudiaremos los medios de comunicaciones inter-centros.

En lo referente a las **comunicaciones locales**, la utilización generalizada de redes usando par trenzado y concentradores de cableado (ya sean *hubs* o *switchs*) ha solucionado muchos problemas de falta de disponibilidad ocasionados por el uso de redes con cable coaxial, en las que el fallo en uno de los segmentos (ocasionado por un roedor, un usuario descuidado o cualquier otra causa) provocaba el corte de las comunicaciones en toda la red local. Actualmente, la interrupción en uno de los segmentos aisla de la red exclusivamente al equipo o equipos que están conectados a él, con lo que nos basta con tener algunos segmentos de *backup* para los equipos críticos de nuestro sistema y un concentrador de reserva por si tuviésemos la necesidad de sustituirlo.

En cuanto a las **comunicaciones inter-centros**, la mejor opción sería poder disponer de dos medios alternativos de distintas tecnologías e incluso, ahora que es posible, de dos operadores de comunicaciones diferentes en cada uno de ellos. De nada nos vale disponer de dos líneas de RDSI para nuestra operativa normal y otras dos de *backup* puesto que, por ejemplo, si la avería ocurre precisamente en la centralita del operador que nos proporciona dichas lineas, las cuatro quedarán inoperativas.

En lo referente a tecnologías, contamos fundamentalmente con cuatro opciones:

- *Frame Relay* o Red de Retransmisión de Tramas.
- RDSI o Red Digital de Servicios Integrados.

- ADSL o *Asymmetric Digital Subscriber Line*.
- Redes ATM o de Transferencia Asíncrona.

La elección de unas u otras depende del uso que vayamos a darle y de las necesidades de nuestro sistema y no es un tema que corresponda tratar en este documento.

En cuanto al manejo de las mismas, en la actualidad existen diversos modelos de *routers* de gama media-alta que son capaces de gestionar el uso de dos interfaces de red diferentes, de cualquiera de los medios antes enumerados, y realizar una conmutación transparente entre el medio principal y el secundario en caso de falta de disponibilidad en las comunicaciones. Obviamente, el uso de un solo *router* introduce un punto único de fallos en nuestro subsistema de comunicaciones que deberíamos de solventar en un verdadero sistema de alta disponibilidad, a pesar de que los *routers* suelen ser aparatos muy robustos y que rara vez presentan averías.

En nuestro caso, usamos en cada una de las oficinas de esta organización un *switch* para los servidores, *routers* y equipos críticos, y concentradores *hubs* para el resto de los puestos de trabajo e impresoras de la red. Las bocas disponibles de estos dispositivos estaban sobredimensionadas para que, en el caso de que uno de ellos se averiase, pudiésemos recomponer sin problemas y en pocos segundos la topología de nuestra red. Los segmentos de cable de los servidores y equipos críticos estaban duplicados, no así los de las estaciones de trabajo. En cuanto a la WAN, se usaron dos medios diferentes aunque del mismo operador: *Frame Relay* como medio principal de comunicaciones y RDSI como *backup*. El ancho de banda de las líneas contratadas difiere en los distintos centros entre 64 Kbps y 128 Kbps, dependiendo del número de usuarios de los mismos. Los *routers* eran CISCO 4400 con interfaces RDSI *y Frame Relay* y no se duplicaron. En cuanto a la estuctura física, se pensó en dos grandes estrellas. El centro de cada una de ellas estaría en cada uno de los dos grandes centros departamentales. Ambos estarían unidos por una línea *Frame Relay* de 2 Mbps con seis líneas RDSI como *backup*. En el caso del centro corporativo separado en dos edificios distantes por un kilómetro de distancia, se unieron ambos mediante un radio enlace de 2 Mbps con otras seis líneas RDSI como *backup*.

2.2 Servidores

El *hardware* básico que incluyen los servidores de las principales marcas es muy fiable y está lejos de toda duda. No obstante, puesto que una de las exigencias del cliente era que la arquitectura estuviese basada en productos Microsoft, no está mal consultar la lista de compatibilidad HCL (*Hardware Compatibility List*) de Microsoft (http://www.microsoft.com/hcl). Al margen de cuestiones comerciales, el hecho de que un servidor sea incluido en las HCL, nos garantiza que ha pasado unas duras pruebas de compatibilidad y disponibilidad. En el caso de la HCL de Datacenter (los servidores de gama más alta certificados por Microsoft) la inclusión en la lista exige que el servidor se ejecute sin problemas durante 14 días y que el nivel de disponibilidad del mismo durante ese periodo sea del 100%. Según Microsoft, esto equivale a un nivel de disponibilidad continua del 99,99%.

Teniendo esto en cuenta se decidió, fundamentalmente por razones empresariales, usar servidores de la gama Netfinity de IBM con una configuración en cluster de dos vías. Enumeraremos, en cualquier caso las características fundamentales y deseables a tener en cuenta a la hora de elegir el *hardware* y la configuración de nuestros servidores:

- Usar una configuración en cluster de dos nodos.
- Dos fuentes de alimentación por servidor.
- Tres tarjetas de red por servidor.
- Dos tarjetas SCSI por servidor.
- Usar una cabina de discos externa a los servidores.
- Usar un esquema adecuado de tolerancia a fallos con los dispositivos de almacenamiento (RAID).
- Sistema de protección de memoria.
- Disponer de *software* (y a ser posible *hardware*) de administración de sistemas.
- Posibilidad de cambiar las tarjetas del equipo en caliente.

Clusters. Un *cluster* de ordenadores es, básicamente, un sistema distribuido en paralelo que consiste en dos o mas servidores interconectados compartiendo sus recursos y que son vistos como si se tratase de uno solo. Esta medida incrementa enormemente la disponibilidad de un sistema, no sólo ante fallos, sino también contemplando las necesarias actualizaciones periódicas del sistema que nos obligan a sacarlos momentáneamente de producción.

Imaginemos, a muy grandes rasgos, un caso en el que tenemos un servidor realmente malo con un porcentaje de disponibilidad de sólo el 95%. Esto significa que el servidor no estará disponible durante, aproximadamente, 1 hora y 12 minutos al día. La probabilidad de que el servidor no esté disponible en un momento dado es, por tanto, del 5%. Si, simplemente, sumamos otro servidor de iguales características, la probabilidad de que ambos se encuentren simultáneamente fuera de servicio es del 0,25% y la disponibilidad del sistema aumenta hasta el 99,75%, esto es, hemos reducido el tiempo de no disponibilidad a una media de tan solo 3 minutos y 36 segundos diarios.

RAIDs. A pesar de que los avances en la tecnología nos proporcionan discos cada vez mas fiables (y de mayor capacidad), siguen siendo uno de los principales puntos débiles de nuestros sistemas, especialmente durante los primeros meses de uso. La tecnología RAID (*Redundant Array of Independent Disks*) nos permite, mediante *hardware* o *software*, combinar dos o más discos de forma que sean vistos como una única unidad lógica. La información se almacena en ellos de forma redundante proporcionando distintos niveles de tolerancia a fallos. Existen, lógicamente, algunas contrapartidas: algunos esquemas de RAID penalizan la escritura en disco, otros la lectura, y todos, en mayor o menor medida, ocasionan una considerable reducción en el espacio disponible para almacenamiento. En cualquier caso, ahora que la tecnología nos ofrece canales SCSI cada vez mas rápidos y *megabytes* mas baratos, son costes fáciles de pagar considerando la alta disponibilidad con que dotan a nuestros sistemas.

Un esquema RAID puede ser controlado por el propio sistema operativo, por *software* especializado o por un adaptador *hardware* específico que usa un procesador dedicado para aligerar la carga de la CPU del servidor. Usando un buen *hardware* tendremos mayor tolerancia a fallos, mejor rendimiento de lectura y escritura (gracias a *caches* dedicadas) y funcionalidades extras como el *hot-swap* y el *hot-spare* de las que hablaremos más adelante. No perdamos de vista que, al incluir la controladora de RAID por *hardware*, estamos introduciendo otro punto de fallo: ella misma. Los errores en las controladores son más infrecuentes que en los propios discos, pero ocurren. Los mejores sistemas RAID basados en *hardware* son aquellos que disponen de dos o más controladores totalmente independientes.

A continuación, discutiremos brevemente los distintos esquemas RAID existentes con las principales características de cada uno de ellos:

- **RAID 0.** De todos los esquemas RAID, éste es el único que no proporciona tolerancia a fallos. Se utiliza exclusivamente cuando necesitamos altos rendimientos, la cantidad de espacio disponible es crítica y la disponibilidad nos la deben de proporcionan otros esquemas. Permite que múltiples discos sean vistos como una única unidad lógica mediante una técnica denominada *drive spanning*, de forma que la capacidad de la unidad lógica es igual a la suma de las capacidades de todas las unidades físicas. Se puede usar con cualquier número de discos físicos (de dos en adelante) limitados sólo por la capacidad de nuestra controladora. Para distribuir los datos entre los diferentes discos físicos se usa otra técnica denominada *drive striping* que maximiza el rendimiento de las operaciones de entrada/salida. Para ello, se divide el disco lógico en bloques de datos denominados bandas (*stripes*), las cuales se distribuyen entre los discos físicos. Durante las operaciones de lectura y escritura los discos operan simultáneamente.
- **RAID 1.** Emplea la técnica denominada *drive mirroring*, mediante la cuál creamos un único disco lógico usando para ello dos (y sólo dos) discos físicos. Todos los datos que escribimos en el disco lógico son escritos en ambos discos físicos, de forma que ambos son, en todo momento, gemelos. El espacio real disponible se reduce, pues, al 50%. El rendimiento en la lectura de datos se incrementa, pero empeora en la escritura. RAID 1 nos proporciona un buen nivel de tolerancia a fallos y de rendimiento, pero la peor eficiencia en cuanto al espacio de almacenamiento disponible. Cuando usamos RAID 1 con dos controladoras de disco independientes, la técnica resultante se denomina *drive duplexing* y nos proporciona uno de los máximos niveles de tolerancia a fallos que podemos lograr en este aspecto.
- **RAID 1E** o **RAID 6.** El RAID 1E (*enhaced*) combina las técnicas de *mirroring* y *striping* de forma que nuestro disco lógico es igualmente dividido en bandas, de forma que cada una de ellas está escrita en dos discos distintos. De esta forma podemos permitir cualquier número de discos físicos y no sólo dos como en el RAID 1. El espacio útil sigue reducido al 50% de la capacidad total y todo lo dicho en cuanto al rendimiento de lecturas y escrituras del RAID 1 es válido también para este esquema.
- **RAID 10** o **RAID 1+0.** Combina también, aunque de distinta forma, las técnicas de *mirroring* y *striping*. Es el resultado de realizar un *mirroring* de dos volúmenes

de disco con RAID 0. El número de discos usados ha de ser par, la capacidad de espacio útil es del 50% y tenemos rendimientos de lectura y escritura similares a los proporcionados por RAID 0.

- **RAID 3.** RAID 3 requiere al menos tres discos físicos. Uno de ellos está dedicado exclusivamente a almacenar la paridad de los datos de todos los demás. Los datos se encuentran, al igual que en esquemas anteriores, divididos en bandas. Usando paridad en lugar de *mirroring* estamos reduciendo considerablemente el espacio necesario para la redundancia de datos. Proporciona un alto rendimiento en operaciones de lecturas de grandes bloque y, como contrapartida, ocasiona un cuello de botella en las operaciones de escritura. RAID 3 está recomendado exclusivamente en las aplicaciones que requieran uso intensivo de lectura de datos y escasas escrituras. Este esquema y el siguiente (RAID 4) prácticamente no se usan en la actualidad, habiendo sido desplazados por RAID 5.
- **RAID 4.** Es similar a RAID 3 con la única diferencia de que utiliza bandas mas grandes para mejorar algo el rendimiento en las operaciones de escritura.
- **RAID 5.** Este esquema usa bandas para almacenar los datos y paridad para proporcionar tolerancia a fallos. La principal diferencia respecto a RAID 3 y RAID 4 es que no dedica un disco en exclusiva para la paridad, sino que almacena ésta en bandas intercaladas entre los datos de todos los discos. Requiere un mínimo de tres discos y su eficacia en cuanto a espacio de almacenamiento es idéntica a la proporcionada por los dos RAID's anteriores. La distribución de las bandas de paridad entre todos los discos elimina el cuello de botella existente en las escrituras.

Como puede apreciarse en la descripción de todos ellos, es necesario introducir nuevas variables a la hora de elegir cuál es el esquema RAID que más se ajusta a nuestras necesidades. Ya no nos basta con saber la disponibilidad que necesitamos y el coste que podemos asumir, tenemos que estudiar también el uso que harán nuestras aplicaciones de los discos. Por ejemplo, si necesitamos hacer un uso intensivo de los discos para escritura el mejor esquema es el RAID 1. Si fundamentalmente vamos a realizar lecturas de grandes bloques de forma secuencial, RAID 3 o RAID 4 son los esquemas más apropiados. Sin embargo, si necesitamos hacer uso intensivo de lectura de bloques de tamaño variado y de forma fundamentalmente aleatoria, obviamente los mejores esquemas son RAID 5 o RAID 10. Ante la duda, estos dos últimos esquemas son los mas flexibles y los que nos ofrecen un mejor comportamiento medio ante cualquier situación.

Otro punto a tener en cuenta es la elección de los discos. Salvo en RAID 1, el resto de los esquemas nos proporcionan mayor velocidad de acceso y escritura y menor pérdida de capacidad utilizando discos pequeños en mayor cantidad, frente al uso de menor número de discos de mayor tamaño.

Otro punto importante a estudiar es el comportamiento de los distintos esquemas de RAID ante un estado crítico, es decir, tras haber perdido uno de los discos físicos. En RAID 1, ya sea *mirroring* o *duplexing*, si perdemos un disco el otro tiene una copia íntegra de todos los datos. Perdemos el beneficio adicional de lectura conjunta de ambos discos, pero no apreciaremos una sensible degradación del sistema. En RAID 3 o RAID 4, si uno de los discos de datos falla, su contenido será reconstruido

a partir de la información almacenada en el disco de paridad, con lo que apreciaremos una sensible degradación del rendimiento. Si el disco que falla es el de paridad, el rendimiento del sistema no sufrirá ningún cambio apreciable. En RAID 5, la pérdida de cualquiera de los discos ocasionará una sensible pérdida de rendimiento. En todos ellos, la tolerancia a fallos desaparece hasta que no hemos reemplazado el disco dañado y éste ha sido reconstruido.

Cuando hablamos de las mejoras aportadas por un esquema RAID soportado por *hardware*, debemos mencionar dos funcionalidades llamadas *hot-swap* y *hot-spare*. Ambas tienen que ver con la forma de actuar cuando hemos perdido un disco. Si nuestro esquema RAID no está soportado por hardware específico, para reemplazar uno de ellos debemos necesariamente de apagar la máquina, reemplazar el disco, volver a arrancar la máquina e iniciar la reconstrucción. Si nuestro *hardware* de RAID soporta *hot-swap* podemos reemplazar el disco 'en caliente' sin necesidad de apagar la máquina. Una vez que hemos introducido el nuevo disco inmediatamente comienza la reconstrucción del mismo. Durante todo el proceso de reconstrucción, sea cual sea el esquema de RAID que usemos, el rendimiento del sistema se verá sensiblemente degradado.

Hot-spare va un paso mas allá. Si nuestro *hardware* soporta está técnica, podemos tener un disco adicional de reserva en nuestra cabina de discos. Cuando el *hardware* de RAID detecta que ha perdido uno de los discos útiles lo reemplaza inmediatamente por el de reserva e inicia la reconstrucción, de forma que el tiempo que permanecemos sin tolerancia a fallos es mínimo (únicamente mientras dure la reconstrucción del disco de reserva) y no se requiere en ningún momento una intervención manual para restablecer las condiciones de fiabilidad iniciales.

Aún tenemos un nivel mas de disponibilidad: los llamados *arrays de RAID arrays*. Éstos nos permiten la pérdida de un disco manteniendo la tolerancia a fallos y sin apreciar visiblemente ninguna degradación en el rendimiento del sistema, y la pérdida de dos discos simultaneamente manteniendo la disponibilidad del sistema. Además, estos esquemas tienen una excelente respuesta tanto en escritura como en lectura. Los principales inconveniente son el elevado coste de implementación de los mismos y que estamos hablando de sistemas propietarios de diversos fabricantes de *hardware* sin ningún tipo de normalización al respecto.

Por último, en un nivel mas alto y mas cercano a la filosofía de *backups*, están soluciones como el SRDF (*Simmetrix Remote Data Facility)*, distribuido por la casa EMC^2 y que consiste básicamente en una replicación a distancia de la totalidad o parte de nuestros dispositivos de almacenamiento. No precisa de CPU's dedicadas, es totalmente independiente de las máquinas, sistemas operativos y bases de datos que usemos en nuestra red, admite replicaciones síncronas o asíncronas configurables dinámicamente y casi cualquier medio de comunicación disponible en el mercado (Frame Relay, RDSI, ATM...).

Sistemas de protección de memoria. Otro de los grandes quebraderos de cabeza de los administradores de sistemas son los problemas con la memoria de los servidores. Más a menudo de lo que nos gusta reconocer compramos bancos de memoría exclusivamente por su precio sin preocuparnos de la calidad de los *chips* o los controles a que han sido sometidos. Dos son los tipos de errores que pueden sufrir los

bancos de memoria: los denominados ***"soft errors"*** que se deben habitualmente a subidas inesperadas de tensión de las que ya hemos hablado y que desaparecen en cuanto que se actualiza la menoria, aunque pueden provocar el malfuncionamiento de alguna aplicación o del sistema operativo, y los llamados ***"hard errors"*** que son averías mucho mas graves e irreparables que sólo se solucionan sustituyendo el banco de memoria por uno nuevo, con la correspondiente parada del servidor para realizar esta sustitución. Muchas de las marcas de servidores de gama media-alta incluyen algún tipo de protección de memoria que evitan que se produzcan errores *soft* y/o *hard*. Las tecnólogía mas usadas en estos aspectos son la denominada ECC (*Error Correcting Code)* incluida en la mayoría de los servidores Compaq y la tecnología Chipkill, incorporada en las placas bases de los equipos Netfinity de IBM. Ambas protegen nuestros servidores de los dos tipos de errores antes mencionados. Existen soluciones similares proporcionadas por otros fabricantes de servidores.

Software **de administración de sistemas.** Otra característica deseable es que nuestros servidores sean compatibles con alguno de los estándares de administración de sistemas disponibles, tales como DMI (*Desktop Management Interface*) o CIM (*Common Information Model*) que les permita suministrar información a alguna herramienta de administración de sistemas, como por ejemplo OpenView de Hewlett-Packard, Unicenter de Computer Associates o Tivoli de Tivoli Networks.

Estas herramientas nos proporcionaran la información necesaria para conocer en todo momento el rendimiento y estado de nuestros servidores, y poder realizar un mantenimiento preventivo de los mismos antes de que sea necesario realizar un mantenimiento correctivo. Permiten monitorizar parámetros tales como el funcionamiento de los ventiladores, el voltaje del sistema en diversos puntos, la temperatura y la detección de determinados tipos de fallos del *hardware*, mostrándonos en todos los casos mensajes de advertencia o alarma, y pudiendo en algunos de ellos actuar de forma autónoma como, por ejemplo, activando un ventilador auxiliar en caso de detectar el funcionamiento defectuoso de alguno de los mismos o el aumento anormal de la temperatura del equipo.

El siguiente paso sería la inclusión en nuestros equipos de una tarjeta opcional de administración de sistemas *hardware*. IBM posee las denominadas *Advanced System Management Processor,* Compaq comercializa un par de versiones de un producto denominado *Remote Insight Board* y Dell ha desarrollado una tarjeta denominada *Remote Assistant Card*. El resto de los fabricantes de servidores de gama alta comercializan productos muy similares. La funcionalidad de estas tarjetas complementa y potencia las características antes descritas de los programas de administración de sistemas, pudiendo incluso realizar llamadas de alerta a buscapersonas de servicios técnicos y permitiéndonos conectar en control remoto al servidor fallido para diagnosticar e intentar solventar el error. El uso de estos dispositivos nos permite realizar en remoto desde cualquier equipo toda la operativa necesaria sobre los servidores, permitiéndonos eliminar de los mismos el ratón y el teclado que, no lo olvidemos, también pueden constituir un punto de fallo.

Sustitución de tarjetas en caliente. La posibilidad de cambiar las tarjetas PCI sin necesidad de apagar el servidor es otra característica deseable pero reservada a los servidores de última generación. Dichas tarjetas se comercializan con distintas denominaciones propietarias de los distintos fabricantes y son pocos aún los controladores que nos permiten utilizarlas, ya que requieren que el sistema sea capaz de detener y reinicar la tarjeta de forma dinámica. No obstante, es una característica muy a tener en cuenta en equipos de alta disponibilidad y que poco a poco se va abriendo camino entre los distintos fabricantes de servidores.

En nuestra instalación se tomó la determinación de, a pesar de las diferencias existentes entre las distintas dependencias de la organización, instalar siempre el mismo tipo de máquina variando unicamente la capacidad de almacenamiento de la misma. Esta homogeneización facilitaría el posterior mantenimiento de la instalación. Como servidores se escogieron dos IBM Netfinity 5500-M20 con dos discos internos de 9 *Gigabytes* cada uno en configuración *cluster* con una cabina de discos externos EXP200 con capacidad para 10 discos. Para la configuración de los RAIDs se optó por una opción *hardware* mediante las tarjeta IBM ServeRaid 3HB Ultra2 SCSI con funcionalidad de *hot-swap.* Los discos internos de cada servidor se configuraron con un esquema RAID1-duplexing. La cabina de discos externas alojaría 10 discos en tres volúmenes con esquema RAID5 en cada uno de ellos. El décimo disco sería reservado como *hot-spare*. Los equipos trabajaban con el *software* de administración de sistemas de Tivoli y eran controlados de forma remota mediante Netfinity Software Management.

2.3 Sistema de mensajería Electrónica

Los sistemas de mensajería se están convirtiendo en uno de los puntos vitales de las nuevas empresas. Estamos, además, ante el caso de una empresa que apuesta fuertemente por las nuevas tecnologías y que quiere introducir a sus clientes un servicio de reservas vía e-mail. Partiendo de la infraestructura física de comunicaciones que se discutió anteriormente, aquí se comentaran las características fundamentales del servicio de mensajería.

Como servidor se pensó en Microsoft Exchange Server 5.5 Enterprise Edition. La versión Enterprise de este servidor añade dos características fundamentales sobre la versión básica: el tamaño de su base de datos está limitado exclusivamente por el espacio físico de que disponemos en disco y es posible su instalación en modo activo/pasivo en una configuración en *cluster*. Como estructura lógica se pensó en una doble estrella. El centro de cada estrella se situaría en cada uno de los grandes centros corporativos y los brazos serían las delegaciones que dependen de cada uno de ellos. Estas delegaciones tienen definidas dos rutas de encaminamiento lógico de los mensajes: una principal con el centro de la estrella que le corresponde y otra secundaria (definida con un mayor coste para que no sea utilizada salvo error o saturación en la primaria) con el centro de la otra estrella. En cada uno de los centros corporativos instalamos dos servidores de correo: uno, formado por un *cluster* de dos vías, dedicado como servidor propiamente dicho de los usuarios de dichos centros y el

otro, un servidor sencillo, que tiene como función hacer de conector y encaminador de mensajes. El servicio de entrada y salida de mensajes a Internet se configuró asimismo en estos dos servidores de correo adicionales. La necesidad de contar con una zona desmilitarizada (DMZ) para esta función y la estructura planteada en la misma se tratará con más detalle en el apartado de seguridad.

Restricciones. Un sistema de mensajería electrónica sin ningún tipo de restricción puede ser muy peligroso: el mal uso de los usuarios puede ocasionar que las líneas se colapsen y dejar a nuestro sistema fuera de servicio durante prolongados períodos de tiempo. Invertir en educación es una buena opción: la mayoría de los usuarios no son conscientes de que enviarle ese video de 60 *megabytes* a las 30 personas que tiene en su libreta de direcciones puede ocasionar un desastre: el simplemente le da al boton de “Enviar” y el mensaje desaparece de su vista y puede seguir trabajando con normalidad.

No obstante, la mejor opción es una adecuada política de restricciones. La práctica totalidad de los servidores de correo electrónico actuales permite limitar el tamaño máximo de los mensajes enviados y aceptados por cada usuario o grupo de estos e incluso hacer una diferenciación entre los mensajes que provienen de Internet y los que son enviados a través de la red empresarial. Otra buena costumbre es acotar el tamaño máximo que cada usuario puede emplear en su buzón personal. Un crecimiento desmedido de las bases de datos de nuestro servidor puede acabar degradando su rendimiento en el mejor de los casos o hacerlo inoperativo en el peor de ellos. No se pueden poner normas en estos aspectos. Depende mucho del número de usuarios que tengamos, la calidad y ancho de banda de nuestra red local y líneas de comunicaciones y, sobre todo, el uso que se le dé en nuestra empresa al correo electrónico. Para comprender correctamente este último aspecto es necesario realizar un detallado estudio hablando con los diferentes usuarios e intentando comprender sus hábitos y costumbres.

En nuestro caso, la infraestructura de comunicaciones interna es en la mayoría de los casos antigua (10 *Mbps*) y tan sólo en algunas de las oficinas modernas existen redes a 100 *Mbps*. Las líneas de comunicaciones externas también son de escaso ancho de banda (entre 64 y 128 *Kbps*). Los usuarios realizan un uso intensivo de los sistemas de mensajería tanto interna como externamente, llegando a registrar una media diaria de entre 40 y 50 mensajes por persona y día. Los mensajes suelen ser habitualmente de texto plano y a menudo con archivos adjuntos de Word o Excel de pequeño tamaño. Sólo ocasionalmente se envían grandes archivos, sobre todo por parte de los cargos directivos y a finales de cada mes.

Distinguiremos dos tipos de usuarios: los cargos directivos y personal técnico por un lado y el resto de usuarios por otro. Llamaremos a los primeros usuarios tipo A y a los segundos usuarios tipo B. Limitaremos los buzones de los usuarios tipo A a 400 *megabytes* y los de los usuarios tipo B a 200 *megabytes*. Los mensajes enviados y recibidos a través de Internet fueron limitados en ambos casos a 1 *megabyte*. Por último, los mensajes internos fueron limitados para los usuarios tipo B en 1 *megabyte* y para los usuarios tipo A en 5 *megabytes*.

2.4 Arquitectura Web

La estrategia comunmente usada para diseñar una sede Web o de servidores FTP de alta disponibilidad es lo que se denomina una granja de servidores (*Web Farm*) con algún sistema de balanceo de carga entre los servidores que componen la granja. Con ello conseguimos, aparte de una alta disponibilidad, un sistema fácilmente escalable. Mediante el sistema de balanceo de carga las peticiones entrantes de los distintos clientes son repartidas de distintas formas, según el método que empleemos, entre los servidores que compongan la granja. Existen varias formas de implementar esta distribución de la carga. Aquí discutiremos las ventajas e inconvenientes de tres de los métodos más usados:

- *Round Robin Domain Name System* (RRDNS).
- *Load Balancing Switches.*
- *Microsoft Network Load Balancing* (NLB).

Round Robin DNS. Es el metodo más simple y económico de implementar el balanceo de carga para cualquier servicio basado en TCP/IP, siendo una característica base de los sistemas operativos más populares. La norma 'de facto' que define la implementación de esta técnica es conocida como BIND (*Berkeley Internet Name Domain*). RRDNS permite que un grupo de servidores aparezca ante los clientes como si se tratase de uno solo, distribuyéndose el tráfico de éstos entre todos los servidores. El funcionamiento es muy sencillo: cuando un cliente interroga a un servidor DNS en busca de un determinado servicio, este le devuelve la dirección IP del servidor que lo proporciona. En una implementación de RRDNS, el servidor DNS proporciona una dirección diferente cada vez que es requerido por un cliente. Estas direcciones son las de los servidores que constituyen nuestra granja. Cada dirección IP pertenece a un servidor diferente capaz de gestionar estas peticiones, de forma que la carga de trabajo es repartida entre las diferentes máquinas proporcionándonos un método primitivo de balanceo de carga. La principal ventaja de este método es su bajo coste: no requiere *hardware* ni *software* adicional. No obstante, presenta varios grandes inconvenientes a tener en cuenta. En primer lugar, no todos los clientes obtienen la dirección directamente del servidor DNS, ya que éstos implementan un sitema de *cache* para la resolución de nombres. Esta *cache* puede deshabilitarse, pero esto empobrecerá el rendimiento de nuestro servidor ya que le obligará a resolver todas las direcciones que le lleguen. En segundo lugar, el servidor DNS no obtiene en ningún momento información del estado de los servidores de la granja, de forma que si alguno de ellos está sobrecargado de trabajo seguirá enviándole peticiones de servicio hasta saturarlo, a pesar de que los otros están libres. Por último, si uno de los servidores falla quedando fuera de servicio y no lo eliminamos manualmente del servidor DNS, este continuará enviándole peticiones. El cliente tendrá que esperar a que el time-out correspondiente concluya antes de ser remitido a otro servidor de la granja.

Load Balancing Switches. Es una solución *hardware* proporcionada por diferentes fabricantes, tales como Cysco Systems o Alteon Websystems. Es una solución robusta y muy escalable. Los *switches* se colocan entre la conección a Internet y la granja de

servidores. Todas las peticiones de los clientes llegan al *switch* usando la misma dirección IP y es éste, en base a diferentes algoritmos implementados en él, quien dirige el requerimiento de servicio a uno de los servidores de la granja. El switch dirige periódicamente un *ping* a cada uno de los servidores que componen la granja de forma que puede determinar en cada momento cuales están activos y cuales no. Asimismo, usa el tiempo de respuesta de los mismos para determinar la carga de trabajo de cada uno y utilizar este parámetro en sus algoritmos de encaminamiento, proporcionándonos de esta forma un balanceo de carga inteligente. Su principal inconveniente es el elevado coste de estos mecanismos. Además, si pretendemos construir un sistema de alta disponibilidad no podemos contentarnos con uno sólo de estos aparatos, convirtiéndolo en el talón de Aquiles de nuestro sistema: deberíamos de contar con, al menos, dos de ellos, elevando aún más el coste de esta solución.

Microsoft NLB. Se trata de una solución propietaria de la empresa de Redmon, disponible en algunas de las versiones de sus sistemas operativos NT 4.0 y 2000. Este sistema utiliza una dirección IP virtual para el *cluster* de servidores, distribuyendo la carga de los clientes entre los servidores reales de forma transparente para los clientes. NLB se implementa usando un *driver* de red situado logicamente entre el nivel más alto del protocolo TCP/IP y el adaptador de red del servidor. Todos los servidores que componen el *cluster* reciben la totalidad de las peticiones de los clientes. El driver de red de NLB actúa como filtro y permite que el servidor procese únicamente parte del tráfico que recibe.

Viendo el mecanismo utilizado por las tres soluciones vistas podemos comprender fácilmente que, si queremos implementar un servicio de muy alta disponibilidad, podemos combinar fácilmente dos de ellas colocando, por ejemplo, un sistema de RRDNS en un primer nivel que redirija el tráfico a dos *switches* de balanceo de carga, cada uno de los cuales encamina el tráfico a 8 servidores diferentes.

En nuestro caso se optó por usar NLB para el reparto de carga, combinado con Microsoft Cluster Service para aumentar la disponibilidad y escalabilidad del sistema. El *front-end* estaría conformado por cuatro servidores Web con reparto de carga mediante NLB que atacarían a una pareja de servidores en *cluster* con una cabina de discos externas como almacen de información compartido, en los que se ejecuta un gestor de bases de datos de Oracle para dar servicio a nuestros servidores Web. En la siguiente figura se puede ver un esquema de la instalación.

2.5 Seguridad

La seguridad física y lógica de nuestro sistema es el último punto de este documento, aunque no el menos importante. Si buscamos construir un sistema confiable y altamente disponible debemos de hacerlo seguro. De nada vale todo lo visto anteriormente si permitimos que por sabotaje, ataques de piratas informáticos o por causa de un desastre natural nuestros servidores sean irremediablemente dañados. Este problema es mucho más extenso de lo que podemos ver aquí y debería de estudiarse en el entorno de la preparación para la recuperación ante desastres totales.

No obstante, veremos someramente los principales puntos susceptibles de ser atacados en un sistema informático, algunas formas de minimizar los riesgos de ataque e intrusismo y unas nociones sobre sistemas confiables de copias de *backup*.

Seguridad física. La mayoría de las discusiones sobre seguridad actuales se centran en los graves daños ocasionados por los virus y en la seguridad en la red. Sin embargo, algo que suele pasarse por alto es que los servidores son más vulnerables a los ataques físicos que a los remotos. Si asaltan un servidor de nuestra red de forma remota siempre se puede reiniciar, reconfigurar o reinstalar, pero si ha sido dañado fisicamente el problema puede ser más serio y costoso en tiempo de disponibilidad. Los principales puntos a tener en cuenta son los siguientes:

- Ubicación de los servidores y elementos críticos de nuestra red.
- Contraseñas de BIOS y de consola.
- Seguridad general del hardware.

Los servidores deben de estar ubicados en un espacio aislado, de acceso controlado y bien diferenciado del resto de la oficina. Deben de poseer un ambiente refrigerado y libre de emisiones de polvo, humos y cualquier otro agente agresivo para los mismos. Las salas y los pasillos de acceso deben de ser totalmente opacos y sin puertas de cristal. Las puertas de acceso deben de tener una cerradura de seguridad. Sería deseable en casos extremos la vigilancia mediante circuito cerrado de TV.

Los servidores deben de estar protegidos mediante contraseñas de BIOS y de cónsola. Dichas contraseñas deben de ser conocidas exclusivamente por las personas indispensables, cumplir ciertas normas de seguridad (combinaciones sin sentido de símbolos, números y letras en mayúsculas y minúsculas), guardarse en un sobre lacrado para emergencias, cambiarse periódicamente y nunca jamás dejar las contraseñas por defecto que el fabricante o distribuidor proporcione.

Otra amenaza es el robo, tanto del sistema entero como de componentes individuales. No es necesario que se lleven el servidor completo: los equipos de alta disponibilidad están construidos de forma que muchos de sus componentes son fácilmente accesibles y extraibles ‘en caliente’. Esto, que es una ventaja a la hora de la sustitución de un elemento defectuoso, se puede convertir en un inconveniente a la hora de protegernos contra robos por parte de personal externo o de nuestra propia empresa.

Código dañino. Llamamos código dañino a los programas no autorizados que realizan funciones que el usuario no conoce y probablemente no desea, bien porque han sido modificados para alterar su fucionalidad o porque han sido diseñados ex-profeso para permanecer ocultos y destruir o robar datos. Los mas frecuentes ejemplos de código dañino son los virus y los troyanos.

La detección del código dañino una vez introducido en nuestro sistema puede ser una tarea muy complicada, así que lo mejor es extremar las precauciones en cuanto al *software* que es introducido en nuestros equipos, permitiendo exclusivamente la instalación de *software* homologado por la dirección técnica de la empresa y

realizando esta siempre de forma controlada por personal especializado y nunca por el usuario en cuestión.

Es totalmente indispensable para ello deshabilitar o eliminar las disqueteras y lectores de CD-ROMs de las estaciones de trabajo, prohibir el uso de unidades de almacenamiento externo y modems en los equipos y, si tenemos conexión a Internet, deshabilitar los servicios de FTP a los usuarios comunes. Otro punto indispensable es un sistema de antivirus siempre actualizado (de forma automática a ser posible) que funcione en cooperación con nuestro servidor de correo electrónico y que nos permita bloquear la entrada de determinados contenidos (ejecutables, scripts, etc.).

Ataques a través de Internet. Siempre que conectemos nuestra red con el mundo exterior estamos entrando en un terreno hostil. La mejor defensa para evitar ataques externos es un *firewall*. Un *firewall* es un dispositivo que evita que personas desautorizadas entren en nuestra red. Puede tratarse de un ordenador autónomo con filtro de paquetes o de un dispositivo *hardware* que realiza tales funciones. Los *firewalls* funcionan como punto único de entrada, evaluando las diversas peticiones y comprobando cuándo están autorizadas y cuándo no, permitiendo tambien realizar bloqueos contra determinados protocolos y contenidos. En definitiva, un *firewall* controla quién puede entrar, qué puede entrar y dónde y cómo pueden entrar en nuestra red.

Habitualmente el *firewall* separa nuestra red interna de los equipos que necesariamente deben de estar conectados directamente al mundo exterior. La zona donde se encuentran estos últimos se denomina habitualmente zona desmilitarizada o DMZ.

Copias de seguridad. Un correcto programa de copias de seguridad es indispensable para asegurar la disponibilidad de los datos en nuestro sistema. Una vez establecido un programa adecuado de copias de seguridad, el principal problema es la necesidad de la intervención humana: la rutina nos hace olvidar y, precisamente después de una noche en la que nos olvidamos de hacer las copias de seguridad es seguramente cuando precisamos de ellas. Para solventar este inconveniente la mejor opción es un *autoloader* o robot de *backups*. Existe una amplia gama de *autoloaders* en el mercado de diferentes capacidades en cuanto a número de cintas admitibles. Un *autoloader*, por ejemplo, de siete cintas nos permitiría hacer una o dos copias diarias de todos nuestros datos (según el volumen de información de que dispongamos) de forma automática durante todos los días de la semana. Según nuestra política de *backups* podríamos reemplazar dichas cintas al final de la semana por otras nuevas y conservar las grabadas para cualquier eventualidad o sobreescribirlas. No olvidemos, en cualquier caso, que aunque elijamos sobreescribirlas, las cintas de *backup* están sometidas a un fuerte envejecimiento y es necesario reemplazarlas por unas nuevas después de determinado número de escrituras. Es del todo imprescindible que nuestro *software* de *backup* sea capaz de realizar una verificación de los datos una vez grabados en cinta. Las copias de seguridad deben de guardarse en un lugar seguro y deseablemente en un lugar diferente (pero no demasiado apartado) de donde se encuentran nuestros servidores.

Imágenes de los servidores críticos. Un complemento a las copias de seguridad que se ha introducido fuertemente en los últimos tiempos es la creación completa de imágenes de los equipos servidores en CD-ROMs, de forma que éstos pueden ser rápidamente restaurados en caso de un desastre total. Veritas Backup-Exec tiene un sistema denominado Intelligent Disaster Recovery que nos permite crear un CD-ROM autoarrancable que nos permite copiar la información vital de nuestro sistema para, posteriormente, poder realizar una recuperación de los datos restantes desde la última copia en cinta de que dispongamos y así, en un corto espacio de tiempo, tener nuestros servidores totalmente recuperados. Adaptec ofrece un programa similar denomindo Take Two que nos permite crear un disquete de arranque capaz de leer y restaurar desde un conjunto de CD-ROMs una imagen completa de nuestro sistema. Existen otros productos similares comercializados por diversos fabricantes (PQDI, Norton, etc.). Todo lo dicho en cuanto a verificación, reutilización y almacenaje de las cintas de *backup* es válido para las imágenes de servidores en CD-ROM.

En el caso que nos ocupa, y debido a la gran diversidad de ubicaciones, no siempre fue posible escoger un emplazamiento adecuado con unas condiciones mínimas de seguridad para los servidores. No se estableció ningún programa de renovación y control de las contraseñas de los servidores y los equipos críticos. Por requerimientos del cliente no se deshabilitaron las disqueteras ni los CD-ROMs de los equipos de trabajo pero todos ellos disponían de servicios antivirus permanentemente actualizados de forma automática. Se limitó el uso de FTP a determinados usuarios y el servidor de correo electrónico poseía un antivirus integrado de la casa Symantec que controlaba y filtraba los documentos entregados antes de servirlos al buzón del usuario. El *firewall* se instaló en un ordenador dedicado a tal fin y se eligió un producto de la multinacional Trend Antivirus que, aparte de las funciones propias de un cortafuegos, realizaba también un analisis antivirus de los paquetes que entraban en la red. Para las copias de seguridad se escogío un robot fabricado por IBM con capacidad para siete cintas mas una limpiadora. El programa de copias realizaba dos volcados diarios. Al final de la semana se reemplazaban las siete cintas por otras vírgenes y estas eran almacenadas durante todo un mes al cabo del cual eran reutilizadas. Se programó una limpieza semanal de los cabezales del robot. Como *software* de *backup* se usó Veritas Back-up Exec de la casa Seagate. Este mismo *software* proporciona una solución de recuperación ante desastres mediante CD-ROMs que fue convenientemente realizada. Las cintas semanales y los CD-ROMs con las imágenes de los servidores se almacenan en un despacho próximo pero separado del cuarto de servidores.

3. Bibliografía

Libros:

- Microsoft Windows 2000 Server Administrator’s Companion. 2000. Charlie Russell and Sharon Crawford. Microsoft Press

- Redes de Alta Velocidad. Enero de 1997. Jesús García Tomás, Santiago Ferrando y Mario Piattini. RAMA-Editorial
- Maximun Security. Special Edition. 2000. Anónimo. Prentice All.
- High Performance Cluster Computing Vol. 1 & 2. 1999. R. Buyya. Prentice All.
- The RAIDbook 6th Edition: A Handbook of Storage System Technology. 1997. P. Massiglia. RAID Advisory Board.

Páginas HTML:
- Building a Highly and Scalable Web Farm. December 2000. Paul Johns and Aaron Ching. Microsoft Developer Network.

Documentos PDF:
- IBM Netfinity RAID Technology, Reliabilty throught RAID technology. 1999. 15 páginas. International Bussiness Machine Corporation
- IBM Netfinity. High-Availability Cluster Solutions. Using the IBM ServeRaid-3H and IBM ServeRaid-3HB Ultra2 SCSI Controllers. Second Edition. Junio de 1999. 54 páginas. International Bussiness Machine Corporation.
- Evaluating Uninterrumpible Power Supplies. 1997. Technical Report, International Power Technologies.

Revistas:
- Windows 2000 Magazine. Nº 50. Febrero de 2001. Las soluciones de Cluster de Microsoft. Páginas 56 a 64. Greg Todd. NewTec Ediciones S.L.
- Windows 2000 Magazine. Nº 50. Febrero 2001. Los componentes de un sistema de alta disponibilidad. Páginas 65 a 68. David Chernicoff. NewTec Ediciones S.L.