Seguridad en el Hardware. Almacenamiento y Recuperación de los Datos.

Caso Práctico

Ha llegado la hora de abordar una serie de problemas que Juan no se había encontrado hasta el momento. Dichos problemas, están estrechamente relacionados con la seguridad del hardware y almacenamiento de la información.

En la empresa de Juan, existen una serie de dispositivos hardware que son susceptibles de fallo, como discos duros, fuentes de alimentación, lápices de memoria, etc. Por ejemplo, hace poco tiempo, una sobrecarga eléctrica, hizo que se quemase la fuente de alimentación de un ordenador. En este caso, lo peor no ha sido el costo de la reparación, sino que cuando el ordenador dejó de funcionar los datos con los que estaba trabajando no habían sido guardados y se perdieron.

Como responsables de seguridad en la empresa, Juan e Ignacio deben poner las medidas adecuadas para que un fallo en estos dispositivos no ocasione la pérdida de datos irreversible.

Además, Juan sabe que su empresa tiene una serie de servicios, como una aplicación de comercio electrónico alojada en un servidor de la propia empresa, que deben estar disponibles 24 horas al día. Cada minuto que no esté disponible el servicio, puede traducirse en pérdidas económicas, sin contar con la mala imagen que la empresa está dando cuando ofrece un servicio que no está disponible.

Para garantizar dicha disponibilidad es importante tener en cuenta varios aspectos de seguridad, entre ellos, que la integridad física de los equipos se mantenga previniendo los posibles fallos mediante mecanismos activos.

Además, el equipo del departamento de administración, ha hecho una estimación económica de las pérdidas en caso de pérdida de datos críticos. Dicha cifra es tan elevada que podría poner en peligro la continuidad de la empresa. Teniendo en cuenta la importancia de salvaguardar la información, Juan e Ignacio también deberán poner en práctica una serie de elementos pasivos que permitan recuperar la información en caso de desastre.

Como sabes, cuando se habla se seguridad, lo primero que se tiende a pensar es en medidas de seguridad lógica y activa, como por ejemplo, un antivirus. Este tipo de medidas, servirán para prevenir gran parte de los problemas relacionados con el software. Además, es necesario incorporar medidas tanto activas como pasivas que protejan físicamente el hardware ya que, de nada servirá proteger el software si el hardware que lo almacena falla o es destruido.

El objetivo de esas medidas será darnos la posibilidad de restaurar el sistema al estado previo a producirse el problema (incendio, por ejemplo).

Introducción a la Seguridad en el Hardware.

Caso Práctico

En la empresa, Juan cuenta con diferentes dispositivos de almacenamiento como discos duros, memorias USB soportes CD y DVD, etc. Mantener en condiciones óptimas desde el punto de vista físico estos dispositivos es tan importante como salvaguardar los datos de amenazas lógicas, ya que, de estropearse el soporte físico donde se almacenan los datos, es probable que se pierda la información. De hecho, Juan sabe por experiencia en gran parte de las ocasiones, es menos probable que la información se pueda recuperar después de un fallo físico que cuando se trata de un error de tipo lógico.

Por esta razón, el departamento de seguridad ha decidido realizar una pequeña formación a los responsables de los demás departamentos de la empresa. El objetivo de dicha formación es que en cada departamento se tome conciencia de la importancia de mantener el hardware en condiciones correctas de funcionamiento para así, por extensión, mantener los datos seguros.

El ponente inicia la sesión lanzando una actividad de "tormenta de ideas". Nos pregunta: ¿Alguna vez te has planteado, qué acciones podrías poner en práctica para prevenir fallos en el hardware?

Nos dejó cinco minutos para el debate.

A continuación, nos propuso que hiciésemos una relación de tipos de catástrofes que se nos ocurriesen.

Es increíble la imaginación que tiene la gente...

Finalmente, el ponente nos sugirió que eligiésemos dispositivos que a un coste relativamente bajo podrían proteger los equipos de la empresa ante catástrofes del tipo que habíamos elegido.

La actividad acabó con una apuesta en común del trabajo realizado en cada grupo. De esta forma, nuestra lista fue mucho mas completa que al principio.

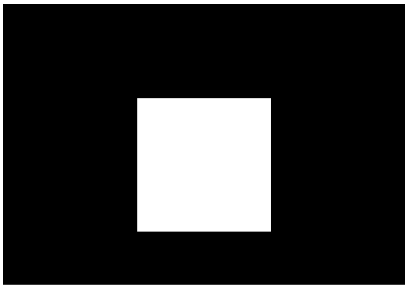
"Creo que el trabajo en grupo funciona muy bien" –pensó Juan.

Cuando hablamos de seguridad en el hardware, en la mayor parte de los casos nos referimos a seguridad física. El objetivo principal de la seguridad en el hardware, consiste en mantener el buen funcionamiento de los dispositivos que forman el sistema informático, como ordenadores y periféricos, routers, cableado, etc.

Como dijimos en la primera unidad, la seguridad absoluta en cualquier ámbito es imposible, por eso trataremos de conseguir la mayor fiabilidad que sea posible. Para ello y teniendo en cuenta que estamos ante un enfoque de seguridad en el hardware, podemos seguir una serie de pautas genéricas que verás en este apartado.

Debes conocer

En el siguiente enlace dispones de una presentación sobre los contenidos fundamentales que se tratarán a lo largo de todo el tema. Es interesante que veas esta presentación para hacerte una idea de que vas a aprender en la presente unidad:



Monitorización del Hardware.

Antes de definir el concepto de monitorización del hardware, es preciso que sepas que cuando hablamos de monitorización, es frecuente asociarlo a la detección y análisis de intrusiones en el sistema, especialmente mediante elementos software y que tienen como finalidad monitorizar otros elementos software. En este caso no nos vamos a referir a este tipo de monitorización, sino a la monitorización en el hardware.

Una vez aclarado esto, podemos definir la monitorización del hardware como una serie de procedimientos por software o hardware cuya finalidad es obtener determinados parámetros físicos del hardware y de esta forma poder controlar su correcto funcionamiento y comprobar que dichos parámetros se encuentras dentro de los rangos oportunos.

Para realizar una monitorización por hardware necesitarás algún tipo de medidor como un polímetro (el cuál se muestra en la figura superior) mediante el cual podrás medir diferentes magnitudes como el voltaje, la resistencia o la intensidad de la corriente que circula a través de un circuito.

Si bien hay veces en que se hace necesario utilizar elementos hardware para monitorizar, es habitual utilizar software para comprobar algunos parámetros de la CPU como voltaje o temperatura. Un ejemplo de este software que monitoriza parámetros físicos del hardware es el programa Everest.

Debes conocer

En el siguiente enlace podrás ver una pequeña muestra de los diferentes parámetros físicos que se pueden monitorizar con el programa AIDA64 Extreme. Su versión Trial nos permite usarla durante un periodo de 30 días, tras el cuál, deberemos pagar por su uso. Puedes encontrar esta versión en este enlace.

AIDA64 Extreme

http://www.youtube.com/embed/cGJJCP57ssM

Reflexiona

Cuando se produce un fallo en el software o en otro elemento de tipo lógico, la disponibilidad del sistema puede verse comprometida durante un largo periodo de tiempo, pero, ¿te has parado a pensar cómo puede afectará al sistema un ataque de tipo físico? En este caso, si no se toman las medidas necesarias, en muchos casos, el sistema quedará inoperativo para siempre.

Autoevaluación

Un polímetro…

- ○ Es un elemento hardware para monitorizar el hardware.
- ○ Es un elemento hardware para monitorizar el software.
- ○ Es un elemento software para monitorizar el hardware.
- ○ Es un elemento software para monitorizar el software.

Correcto. Muy bien, has captado la idea…

Incorrecta, porque muestra magnitudes físicas propias del hardware.

No es correcto, el polímetro es un dispositivo hardware, no un programa informático.

No es la opción correcta, el polímetro es un dispositivo hardware, no un programa informático. Además, muestra magnitudes físicas propias del hardware.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

Sistemas de Alimentación Ininterrumpida.

Caso Práctico

Juan se encuentra trabajando en la política de seguridad de la empresa cuando se produce un apagón. Después de dos horas de trabajo Juan no había guardado el documento. Por suerte, el procesador de textos realizó una copia automática, pero no ha recuperado el 100% de su trabajo.

Por si esto fuera poco, un cliente muy importante de la empresa había escrito solicitando información urgente de un producto en el que estaba interesado. La venta de ese producto para ese cliente en concreto, podría suponer un volumen muy importante para la empresa.

Pues bien, parece ser que hoy no es un día de suerte… Juan acababa de leer el correo y no le había dado tiempo de enviarle al cliente esa información.

Juan intenta hacer memoria para recordar el intervalo de tiempo que hace que salvaguardó su trabajo por última vez. También lamenta que de haber tenido un sistema de alimentación ininterrumpida habría tenido tiempo suficiente para poder enviar el correo.

En primer lugar, es una buena costumbre guardar nuestro trabajo tras intervalos de tiempo no demasiado largos. Además de esto, existen dispositivos hardware que pueden evitar este y otros problemas derivados del suministro eléctrico. Veremos que, en el caso del correo electrónico, el hecho de contar con un sistema de alimentación ininterrumpida, le hubiese proporcionado a Juan un margen de tiempo suficiente para poder enviar el correo.

¿Nunca has pensado que las fluctuaciones de alimentación pueden dañar los equipos o sus datos? Los sistemas de alimentación ininterrumpida (UPS, acrónimo en inglés de Uninterrupted Power System, significa sistema de alimentación ininterrumpida) proporcionan protección de alimentación y aseguran los equipos informáticos y sus datos críticos contra daños causados por una alimentación inconsistente y fluctuante.

A lo largo de este epígrafe conocerás lo que son los sistemas de alimentación ininterrumpida, los tipos que existen y su finalidad. Dichos dispositivos son un elemento fundamental dentro de la seguridad física.

¿Qué es un SAI?

Como hemos dicho, un sistema de alimentación ininterrumpida (de aquí en adelante SAI) es un dispositivo que te permite proteger a los equipos y en consecuencia a sus datos, de posibles fluctuaciones en el suministro eléctrico. Además, disponen de una batería que te permitirá mantener el equipo en marcha durante el tiempo suficiente para guardar los datos y cerrar de forma adecuada las aplicaciones activas en ese momento. Incluso podrías seguir trabajando durante un tiempo, siempre limitado por la batería.

Tomando una serie de factores a considerar, los SAI pueden proteger casi cualquier tipo de equipo de informática de prácticamente todas las perturbaciones eléctricas.

Entre los factores que debes considerar para elegir el tipo de SAI correcto, se encuentran:

- La capacidad en voltio-amperios en función acuerdo al número y tipo de equipos a proteger, si se necesita alguna opción especial como monitorización.
- La capacidad de actualización.
- El soporte técnico (disponibilidad de centros de servicio), así como la confiabilidad del proveedor.

No debemos confundir los SAI con otro tipo de dispositivos como pueden ser las regletas protectoras. Si bien una regleta protectora puede disponer de una serie de filtros que pueden ayudar a prevenir ciertas perturbaciones en la corriente eléctrica, a diferencia de los SAI, éstas no cuentan con una batería. Se puede decir que las regletas protectoras son una alternativa barata (y menos efectiva lógicamente) que los SAI.

Autoevaluación

Teniendo en cuenta las dos clasificaciones que has visto de seguridad informática en la primera unidad (Física/Lógica, Activa/Pasiva) en el caso de un SAI, ¿a qué tipos de seguridad corresponde?

- [ ] Física.
- [ ] Lógica.
- [ ] Activa.
- [ ] Pasiva.

Mostrar retroalimentación

Solución

1. Correcto
2. Incorrecto
3. Correcto
4. Incorrecto

Tipos de SAI.

Como puedes suponer, dependiendo de la marca y modelo se podría hacer una extensa clasificación con pequeños detalles que diferencian unos dispositivos de otros. En este caso, vamos a agrupar dichas características en tres grupos que reúnen los elementos más significativos que los diferencian. Teniendo esto en cuenta, tenemos los tipos on-line (en inglés significa "En línea"), interactivo y Stand By (en inglés significa "espera").

- **SAI On-Line**: Son los SAI en los que el dispositivo suministra energía eléctrica al equipo protegido de manera continua. Esta alternativa constituye el más alto nivel de protección. La mayor parte de estos SAI suministran de 5 a 10 minutos de respaldo de batería, lo cual es más que suficiente para el 98% de los apagones cortos. Esta alternativa, es la mejor selección que podrías realizar para aplicaciones críticas o de alta importancia. Como contrapartida, está el alto costo de estos equipos, por lo que sería conveniente que solamente los utilizases en este tipo de aplicaciones realmente críticas.
- **SAI Interactivo**: Estos SAI combinan la protección de los **SAI Off-Line** y los Stand-by con los reguladores de voltaje. Proporcionan una excelente protección en ubicaciones donde el voltaje de la línea varía frecuentemente. Al incluir la función "regulación de voltaje", se obtiene una vida útil en las baterías de 3 a 5 años. Constituyen la mejor protección contra la gran mayoría de anomalías presentadas por las líneas eléctricas alrededor del mundo.
- **SAI Stand By**: También llamado Off-Line, consiste en la alternativa de menor coste para aplicaciones no críticas. Estos SAI alimentan al equipo protegido directamente de la línea eléctrica hasta que ocurre un fallo en el servicio. En ese momento entra en funcionamiento la batería del SAI. Constituyen la tecnología más antigua en SAI. En general no incluyen comunicación con el ordenador y son las que ofrecen menores tiempos de vida útil en sus baterías ya que por carecer de regulador de voltaje emplean muchas más veces sus baterías ante variaciones menores en el servicio eléctrico. Esta característica produce un aumento de los ciclos de carga y descarga de las baterías acortando su vida útil.

Ejercicio resuelto

¿Qué tipo de SAI utilizarías para un CPD? Razona tu respuesta.

Mostrar retroalimentación

Debido a sus características el SAI más adecuando sería el SAI On-Line. Como has visto, este tipo de dispositivos son los que mayor protección ofrecen, ya que suministran continuamente energía eléctrica al equipo protegido, evitando así cualquier irregularidad que se produzca en el suministro de la red eléctrica.

Almacenamiento Redundante.

Caso Práctico

Andrea, la directora de la empresa, se pone en contacto con Ignacio y Juan para tomar una decisión respecto al almacenamiento de cierta información muy importante para la empresa.

El hecho de que a la directora le preocupe especialmente la manera de almacenar dicha información, es porque el año pasado llegaron unos discos defectuosos y se perdió parte de esa información tan vaposa para la empresa.

-El año pasado se estropeó uno de los discos que teníamos en el servidor. Como consecuencia, el servidor estuvo fuera de servicio 5 horas –les explicó Andrea.

-Además, coincidió que en dichas horas era donde se encontraban los mayores picos de facturación. Las pérdidas ascendieron a varios miles de euros -se lamenta Andrea.

Juan e Ignacio se mantienen expectantes.

-Es fundamental tomar medidas para que este año no nos vuelva a pasar lo mismo –sentenció la directora.

-No te preocupes Andrea, con un costo menor al que pueden suponer las pérdidas, te daremos una solución. –Respondía Ignacio con convencimiento.

-Sí, Sí. –confirma Juan.

-Bien, como buenos profesionales de la seguridad que sois, confío que me presentaréis una solución para evitar que vuelva a suceder algo así, o al menos, minimizar las posibipdades de que se repita.

Reflexiona

¿Alguna vez has pensado en la importancia que tiene almacenar la información en soportes seguros? En muchas ocasiones guardamos datos de importancia en memorias USB, discos duros y demás dispositivos que son susceptibles de estropearse. Un fallo de este tipo, supondría la pérdida de la información a no ser que contemos con la información replicada en otro dispositivo de forma que nos permita recuperarla.

En los epígrafes posteriores conocerás algunas opciones de almacenamiento, profundizando especialmente en sistemas redundantes.

Citas para pensar

Francis Bacon, filósofo: "*La información es poder*".

Sistemas de Tolerancia a Fallos y Seguridad Física Redundante.

Como ya sabrás, cuando hablamos de elementos redundantes, nos referimos a la replicación de dichos elementos. En seguridad física, en algunas ocasiones, se replican elementos del sistema informático para que, en caso de que el elemento principal falle, entre en funcionamiento otro elemento de respaldo. En el siguiente epígrafe, verás los sistemas **RAID**, que utilizan información redundante con el mismo objetivo.

Algunos ejemplos de elementos físicos redundantes son, como ya hemos dicho, los discos duros (RAID), fuentes de alimentación, tarjetas de red o incluso podría estar duplicado por completo un CPD dando lugar a otro **CPD** de respaldo.

Teniendo esto en cuenta, podemos distinguir entre redundancia estática o dinámica, dependiendo de si los elementos duplicados están en funcionamiento continuamente o entran en funcionamiento al detectar el fallo respectivamente.

El inconveniente de los sistemas con componentes físicos redundantes es que conllevan un coste económico muy elevado.

Estos sistemas con componentes redundantes son también llamados **sistemas de tolerancia a fallos**.

Otra alternativa segura es el almacenamiento remoto. Lo verás en apartados posteriores.

Autoevaluación

¿A qué nos referimos cuando hablamos de un sistema tolerante a fallos?

- ○ Confidencialidad
- ○ Integridad.
- ○ Disponibilidad.
- ○ No repudio.

Muy bien, has captado la idea…

Incorrecta, porque el mensaje no ha sido alterado, por tanto, no afecta a su integridad.

No es correcta. El mensaje llega a su destinatario, por lo tanto, no afecta a su disponibilidad.

No es la opción correcta. El hecho de interceptar el mensaje no afecta para nada al repudio del mismo

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

Sistemas RAID.

Habrás comprendido en la introducción que un sistema RAID consiste en distribuir la información almacenada entre un conjunto de discos duros, de forma que, en algunos casos la información está replicada, aunque veremos que esto no siempre es así.

El hecho de tener información replicada y distribuida en diferentes discos supone una importante ventaja de cara a la seguridad, especialmente si tienes en cuenta la integridad de los datos y la tolerancia a fallos. Además de ser un sistema más seguro que el almacenamiento en un solo disco, también hay que tener en cuenta la ventaja del aumento de la velocidad.

Por otra parte, en configuraciones RAID con redundancia, hay que tener en cuenta que, lógicamente, la capacidad será siempre menor que si utilizásemos el mismo número de discos para almacenar información de forma no redundante.

Otra característica importante a tener en cuenta es que, un RAID, a pesar de estar formado por diferentes discos físicos, desde el punto de vista lógico, es como si se tratase de un solo disco. Es decir, cuando trabajes con un RAID, no debes preocuparte del disco exacto en que se encuentra la información con la que vas a trabajar. Todo el proceso de acceso al disco conveniente será transparente al usuario o usuaria.

En cuanto a la manera de implementar un RAID, algunos PC (Personal Computer) incluyen en su placa base controladoras RAID. En el caso de que queramos utilizar el disco en modo RAID, deberemos conectar el número de discos físicos adecuados a la configuración deseada y configurarlos en la BIOS.

Más adelante veremos los mecanismos que proporciona Windows para implementar un RAID. En este aspecto, debemos conocer lo que Windows denomina como volúmenes dinámicos. Los discos dinámicos, a diferencia de los discos básicos, tienen la posibilidad de crear volúmenes repartidos entre varios discos físicos y de crear volúmenes tolerantes a errores (RAID 1 o RAID 5).

Además de esto, también tenemos en el mercado actualmente discos externos con configuraciones RAID. Estos discos vienen preparados para ajustarse a diferentes configuraciones de manera que el usuario o usuaria solamente tiene que elegir la que más le convenga.

Para saber más

En el siguiente enlace puedes ver una comparativa realizada por José Antonio Castillo sobre las características principales de los principales sistemas RAID existentes, junto con las ventajas e inconvenientes proporcionados por cada uno de los sistemas.

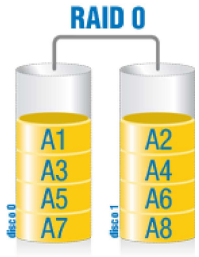
Comparativa de diferentes tipos de RAID

Configuraciones o Niveles RAID Básicos.

Como ya sabes, un RAID es un conjunto de discos que almacenan la información conjuntamente de forma redundante. Pero para llevar esto a la práctica nos encontramos con multitud de posibilidades dependiendo del número de discos y de la manera en la que se distribuye la información redundante entre los mismos.

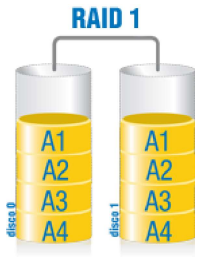
Existen multitud de configuraciones, pero en este apartado nos vamos a centrar en algunas de las más comunes, que son las siguientes:

- RAID 0: el nivel 0, es una excepción en lo que a información redundante se refiere. En este caso, verás que la información se distribuye equitativamente entre dos o más discos, pero sin información replicada. Su principal ventaja es el incremento de rendimiento. La razón de que el rendimiento sea mayor, es que se realizan operaciones en paralelo entre los dos discos. Por ejemplo, si tenemos que guardar un fichero que ocupa 10 Megas, se guardarán 5 Megas en un disco y 5 Megas en otro, lo que se traduce en la mitad de tiempo de escritura. El problema de este método es que si uno de los dos discos falla, se pierde toda la información.



- RAID 1: también se conoce con el nombre de espejo, debido a que consiste en duplicar toda la información. Por tanto, implica redundancia y tolerancia a fallos proporcionando un sistema con alto nivel de fiabilidad. Si se pierden los datos de un disco podrán ser recuperados del otro disco.
  Por otra parte, el rendimiento de las operaciones de lectura también se ve incrementado al igual que ocurría con el RAID 0, ya que son capaces de realizar búsquedas en paralelo siempre que la tarjeta sea moderna (anteriormente solo eran capaces de leer de un solo disco). Si hablamos de operaciones de escritura, el RAID se comporta igual que si de un solo disco se tratase.

  En cuanto a la capacidad de los discos empleados, no es necesario que ambos sean iguales, pero la capacidad total de almacenamiento que tendrás será la equivalente al menor de los mismos. Esta se podría considerar una desventaja, ya que se pierde bastante capacidad de almacenamiento en comparación con otras configuraciones. Su elección dependerá de la importancia que le des a la seguridad, sobre la capacidad de almacenamiento requerida en el sistema.



Autoevaluación

Señala las afirmaciones correctas respecto a RAID

- [ ] Con un RAID 0, podremos recuperar la información a no ser que fallen los dos discos a la vez.
- [ ] Con un RAID 1 tenemos mayor seguridad debido a la redundancia.
- [ ] Con un RAID 0 no conseguimos mayor seguridad en los datos.
- [ ] Con un RAID 1, aumentamos la velocidad de escritura en disco.

Mostrar retroalimentación

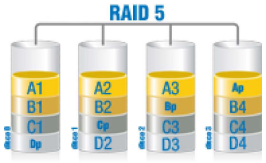
Solución

1. Incorrecto
2. Correcto
3. Correcto
4. Incorrecto

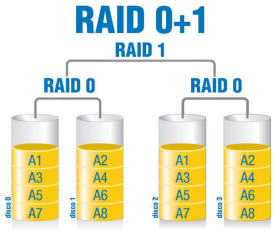
Configuraciones o Niveles RAID Avanzados.

Siguiendo con la clasificación anterior, verás otras dos configuraciones de las más comunes, como son RAID 5 y RAID 0 +1:

- RAID 5: En este caso, la información de distribuye por bloques. Cada disco contendrá un bloque redundante, de manera que si nos referimos a una línea como un conjunto que tienen un orden "n" en cada disco, en cada línea habrá un bloque redundante que va rotando de disco a disco haciendo un recorrido cíclico). En la siguiente imagen puedes comprobar este tipo de distribución: en la primera línea el bloque de paridad está en el disco 4, en la segunda línea en el disco 3, en la tercera en el disco 2 y así sucesivamente.
  Este tipo de configuración requiere al menos tres discos para ser implementado. Como hemos dicho, proporciona tolerancia a fallos y en comparación con un RAID 1, tiene la ventaja de que aprovecha mejor la capacidad de almacenamiento. Su principal inconveniente, es que en el caso de fallar más de un disco, la información no se puede recuperar ya que el bloque de paridad necesita el resto de los discos para reconstruir la información.



- RAID 0+1: Esta configuración, también llamada RAID 01, se denomina de esta forma por ser una combinación entre un RAID 0 y un RAID 1. Como podrás comprobar en la siguiente imagen, en primer lugar se crea un conjunto RAID 0 y posteriormente, se crea un espejo (RAID 1) de ese conjunto.
  El problema de esta configuración, es que al añadir un disco en uno de los RAID 0, estamos obligados a añadir otro en el conjunto replicado para mantener la configuración. Otro problema es que, en el caso de fallar en dos discos simultáneamente, no es posible de recuperar la información (a no ser que ambos discos sean del mismo conjunto RAID 0).



Para saber más

El siguiente enlace te llevará a una entrada de la Wikipedia sobre los RAID donde podrás ampliar la información, especialmente en cuento a otras configuraciones de RAID menos frecuentes.

RAID en Wikipedia.

RAID en Windows.

A continuación verás que, a partir de Windows 2000 en adelante, contamos con la posibilidad de crear volúmenes dinámicos con algunas excepciones, como equipos basados en Windows XP Home Edition (Inglés. Significa, edición doméstica). Debido a esto, debemos tener cuidado cuando creamos volúmenes dinámicos en un equipo con varios sistemas operativos, por si alguno no es compatible con los mismos.

Los discos dinámicos, a diferencia de los discos básicos, tienen la posibilidad de crear volúmenes repartidos entre varios discos y de crear volúmenes tolerantes a errores (RAID 1 ó RAID 5). Todos los volúmenes de los discos dinámicos se consideran volúmenes dinámicos.

En Windows (el ejemplo de la imagen está tomado de Windows 10 Pro) encontrarás cinco tipos de **discos dinámicos**:

- **Simples**: es un volumen que se corresponde con un solo disco físico.
- **Distribuidos**: el volumen se corresponde con varios discos físicos, pero, a diferencia de un RAID 0, la información se guarda indistintamente en un disco o en otro. Por este motivo, un volumen distribuido no ofrece mayor velocidad.
- **Seccionado**s: este tipo de volumen se corresponde con un nivel RAID 0.
- **Reflejados**: este tipo de volumen se corresponde con un nivel RAID 1.
- **RAID 5**: este tipo de volumen se corresponde con un nivel RAID 5.

Veamos cómo poner esto en práctica. Vamos a configurar un volumen reflejado en Windows 10 Pro. Para administrar los discos vamos a "**Inicio > Panel de Control > Herramientas Administrativas > Administración de Equipos > Administración de Discos**". En la siguiente imagen vemos la ventana de administración. En este caso, con cuatro discos adicionales al del sistema, que están sin asignar.

Como hemos visto, el volumen reflejado se corresponde con un RAID 1, con lo cual, la copia del disco se tendrá que hacer en otro disco de igual o mayor tamaño. Lo ideal es que ambos discos sean del mismo tamaño. Además, Microsoft recomienda que sean de las mismas características **pero tengan controladoras diferentes**. Esto se debe al hecho de que las controladoras diferentes hacen que se minimice la posibilidad de fallos simultáneos.

Para agregar el disco reflejado, hacemos clic sobre el disco que queremos reflejar y seleccionamos la opción "Nuevo volumen reflejado". Posteriormente, aparecerá una ventana con el resto de discos para que seleccionemos el que queremos utilizar. Se nos pedirá que indiquemos qué letra de unidad queremos asignar, y se nos facilitará el proceso de formateado en el sistema de archivos que proceda (NTFS por defecto).

Como sabes, el RAID 1, espejo o volumen reflejado, implica que los datos serán guardados en ambos discos. De esta forma, si uno de los dos discos falla, se podrá recuperar la información a partir del otro.

Es importante que tengas en cuenta, antes de realizar una conversión de este tipo, que, aunque un disco duro básico puede ser convertido a dinámico como en este caso, la conversión de dinámico a básico, no es factible sin pérdida de datos. Es decir, que para llevarla a cabo es necesario eliminar todos los volúmenes dinámicos (con la consiguiente pérdida de datos).

Autoevaluación

Relaciona cada configuración con el tipo de volumen, escribiendo el número asociado al volumen que le corresponda en el hueco correspondiente.

Ejercicio de relacionar.

Configuración	Relación	Volumen
Varios discos físicos sin operaciones en paralelo.	☐	1. Reflejado.
RAID 0.	☐	2. Simple.
Un solo disco.	☐	3. Distribuido.
RAID 1.	☐	4. Seccionado.

Enviar

Como has visto a lo largo del epígrafe, en Windows un volumen simple se corresponde con un solo disco; el distribuido y el seccionado con varios discos, trabajando este último como un RAID 0 y por el último el volumen reflejado equivale a una configuración en espejo.

Clusters de Servidores.

Caso Práctico

Existe un módulo de software en la empresa que requiere una serie de características que no requería cuando se empezó a trabajar con el mismo, de manera que se ha quedado escaso en cuanto a procesamiento de peticiones.

Un servidor con las características que requiere, para que no se volviese a quedar obsoleto en poco tiempo, se sale de presupuesto en este momento para la empresa. Por otra parte, la migración del servicio a una máquina más potente no puede esperar más tiempo.

A Juan se le ocurre una idea:

-Nunca he hecho nada parecido, pero… podríamos tratar de montar un cluster con los equipos que están "muertos de risa" en el almacén. De esa forma seguramente tendríamos una solución al problema procesando en paralelo las peticiones –sugirió Juan.

Ignacio, el jefe de Juan, se queda impresionado por la idea.

-Claro, -responde Ignacio- además, sería una solución escalable, que teniendo en cuenta lo que varían los requerimientos con el tiempo, me parece algo importante.

Juan se siente gratificado por la acogida de su idea, cree que esa convicción que tiene en su vida cotidiana sobre el reciclaje le ha servido en su vida profesional.

Juan e Ignacio deciden ponerse manos a la obra.

A lo largo de este epígrafe conocerás los beneficios del empleo de clusters así como su clasificación y componentes.

Los clusters ofrecen las siguientes **características**:

- Alto rendimiento.
- Alta disponibilidad.
- Alta eficiencia.
- Escalabilidad.

Clasificación de los Clusters.

Es importante que comprendas que el término cluster tiene diferentes connotaciones para diferentes grupos de personas. Los tipos de clusters, dependiendo del uso que se les da y los servicios que ofrecen, determinan el significado del término para el grupo que lo utiliza.
Los clusters pueden clasificarse según sus características: puedes tener clusters de alto rendimiento, clusters de alta disponibilidad o clusters de alta eficiencia. Vamos a ver con más detalle cada uno de ellos:

- **Cluster de alto rendimiento:** Son clusters en los cuales se ejecutan tareas que requieren de **gran capacidad computacional**, **grandes cantidades de memoria**, o ambos a la vez. El llevar a cabo estas tareas puede consumir gran parte de los recursos del cluster por largos periodos de tiempo.
- **Cluster de alta disponibilidad:** Son clusters cuyo objetivo es el de **proporcionar disponibilidad y confiabilidad.** Estos clusters tratan de ofrecernos la máxima disponibilidad de sus servicios. La confiabilidad se consigue mediante software que detecta fallos y permite recuperarse frente a los mismos. En hardware, se evita tener un único punto de fallos, de forma análoga a cuando hablábamos de componentes redundantes. De alguna manera, un cluster viene a ser un sistema de componentes redundantes, aunque el objetivo de dichos componentes no sea exclusivamente de respaldo.
- **Cluster de alta eficiencia:** Son clusters cuyo objetivo es el de ejecutar la mayor cantidad de tareas en el menor tiempo posible. Existe independencia de datos entre las tareas individuales.

Los clusters también podemos clasificarles como **clusters comerciales** que combinan alta disponibilidad y alta eficiencia y **clusters científicos** cuya principal característica es el alto rendimiento. A pesar de las discrepancias a nivel de requerimientos de las aplicaciones, muchas de las características de las arquitecturas de hardware y software que están por debajo de las aplicaciones en todos estos clusters, son las mismas. Por tanto, un cluster de determinado tipo, puede también presentar características de los otros.

Autoevaluación

Relaciona cada situación con la característica que describe dicha situación, escribiendo el número asociado a la característica que le corresponda en el hueco correspondiente.

Ejercicio de relacionar

Situación	Realación	Característica.
El sistema necesita realizar una gran cantidad de tareas en el menor tiempo posible.	☐	1. Alto rendimiento.
Existen varios servicios importantes online, por lo que es imprescindible que el sistema esté operativo en todo momento.	☐	2. Alta disponibilidad.
En un momento dado, cambian los requerimientos del sistema y se necesita ampliar tanto su capacidad de almacenamiento como de computación.	☐	3. Alta eficiencia.
Existe un módulo software que necesita resolver complejas operaciones en el menor tiempo posible.	☐	4. Escalabilidad.

Enviar

El hecho de realizar un gran número de tareas en el menor tiempo posible hace referencia a la eficiencia del sistema. Por otra parte, la capacidad de mantener el sistema operativo en todo momento, está relacionada con la disponibilidad. En cuanto a la flexibilidad, de cara a modificar los requerimientos del sistema, está asociada a la escalabilidad. Por último, el rendimiento es la medida de la velocidad con que se realiza una tarea o proceso.

Componentes de un Cluster.

Hasta ahora, como habrás comprobado, hemos hablado de los cluster como unidades lógicas independientes, pero conviene que conozcas los diferentes elementos por los que están constituidos. Dichos elementos son:

- Nodos: se le llama nodo a cada una de las máquinas que componen el cluster. A la hora de formar un cluster, por razones de eficiencia, conviene que los nodos sean lo más homogéneos posibles en cuanto a características, aunque no tienen por qué ser iguales.
- Sistema de almacenamiento: en cuanto a la manera de almacenar la información, podríamos utilizar cada uno de los discos de los nodos que componen el cluster de la misma forma que si se utilizasen de forma individual. También es posible utilizar un sistema de almacenamiento más sofisticado como el que proporciona un dispositivo NAS o las redes SAN, de las que hablaremos en el siguiente epígrafe.
- Sistemas operativos: en principio podríamos utilizar cualquier sistema operativo que tenga unas características básicas, como la posibilidad de utilizar varios procesos concurrentemente, es decir, multiproceso y que permita proveer a diferentes usuarios simultáneamente, lo que se conoce como multiusuario.
- Conexiones de Red: necesitaremos conectar los nodos del cluster de alguna manera. La más básica es mediante una conexión Ethernet, que es el tipo más utilizado actualmente, debido a que es relativamente económica. Otras opciones, son redes especiales de alta velocidad como, por ejemplo, Fast Ethernet o Gigabit Ethernet.
- Middleware (Inglés. Es un anglicismo): se conoce como middleware el software existente entre el sistema operativo y las aplicaciones que va a gestionar el cluster de manera que los usuarios y usuarias lo percibamos como una única máquina proporcionando una interfaz única de acceso al sistema. Además, dicho software realiza una serie de funciones como:
  - Gestionar el balanceo de carga.
  - El mantenimiento y actualización de servidores.
  - Detección nuevos servidores que se añadan al cluster, etc.

Autoevaluación

El sistema operativo del cluster, debe ser, como mínimo…

- [ ] De 64 bits.
- [ ] Multiproceso.
- [ ] Multiusuario.
- [ ] Posterior a Windows XP.

Mostrar retroalimentación

Solución

1. Incorrecto
2. Correcto
3. Correcto
4. Incorrecto

Almacenamiento Externo.

Caso Práctico

A día de hoy, la empresa cuenta con un gran volumen de datos, entre ellos, datos personales de su clientela. Para la empresa es muy importante mantener la confidencialidad los datos personales, o de lo contrario, podría ser sancionada por la Agencia de Protección de Datos. A medida que pasa el tiempo, la cantidad de datos almacenados en los dispositivos de la empresa, va aumentando considerablemente.

Los equipos de la empresa, a pesar de haber mejorado mucho en cuanto a seguridad en los últimos tiempos, siguen sin convencer a Ignacio. Esto sin contar con que la capacidad de almacenamiento puede verse mermada en el caso de que la empresa siga creciendo de la forma que lo está haciendo actualmente. Es entonces cuando Ignacio piensa en utilizar almacenamiento remoto, un concepto que su compañero Juan desconocía hasta el momento.

La directora de la empresa se reúne con Ignacio para hablar de este tema.

-Mira Ignacio, como ya sabes, cada vez tenemos más volumen de datos y más software en los equipos. Sé que el almacenamiento se está quedando corto, tendremos que comprar más equipos, pero no tenemos demasiado presupuesto.

Ignacio aprovecha para comentarle su nueva idea.

-Sí, la verdad es que los equipos están al límite. De todos modos yo te propongo que almacenemos los datos en un servidor externo. Algunas empresas ofrecen servicios de este tipo a un coste relativamente bajo. De esa forma nos ahorraríamos tener que comprar más equipos y desde el punto de vista de la seguridad también tiene sus ventajas.

-Vale Ignacio. Tú dirás, que eres el que entiende de esto.

-De acuerdo. Si te parece, para mañana te preparo un presupuesto detallado de alguna empresa de las que te he hablado y lo contrastamos con el presupuesto de los equipos para que no nos quede duda de que compensa económicamente.

-Vale, perfecto. Muchas gracias.

Hoy en día, cada vez es mayor el número de **aplicaciones "on-line"**. Estas aplicaciones, guardan los datos y ejecutan las operaciones en servidores remotos. Este conjunto de servidores utilizados remotamente, es lo que está siendo bautizado como "la nube", de ahí el concepto de computación en **la nube** o cloud computing.

Algunas de las aplicaciones de la llamada Web 2.0 como, por ejemplo, Google Docs, siguen esta filosofía de funcionamiento. Con Google Docs, podemos crear, editar y almacenar diferentes tipo de documentos sin tener instalado ningún software adicional al navegador web en nuestro ordenador. Esta es una de las múltiples ventajas de procesar la información a través de un servidor remoto. A lo largo de este epígrafe veremos otras ventajas tiene y profundizaremos en el concepto.

Reflexiona

¿Alguna vez has pensado que utilizas **computación en la nube** en muchos servicios que usas? La empresa Google dispone de un servicio llamado Google Play Music. Dicho servicio está relacionado con el concepto de computación a la nube. En este caso, el usuario o usuaria almacena su música en la nube para poder reproducirla desde cualquier lugar y dispositivo con una conexión a Internet. Existen otros servicios similares en cuanto a la forma de procesar tus datos en la nube que llevan bastante tiempo funcionando. Algunos ejemplos son Google Docs o Google Fotos.

NAS.

Como sabes, hoy en día, las necesidades de almacenamiento de datos están aumentando notablemente tanto en el ámbito doméstico como en un entorno empresarial. En este apartado verás lo que son los dispositivos **NAS** que proporcionan una serie de características adicionales a los sistemas de almacenamiento convencionales.

Los NAS o Network Attached Storage, son servidores especializados en almacenamiento. Dicho de otro modo, son máquinas dedicadas a almacenar información a la que podemos acceder de forma remota a través de la red.

Desde el punto de vista de la seguridad podríamos destacar el hecho de ser un almacenamiento externo a los equipos, con lo cual, evitamos el peligro de la pérdida de datos por fallos locales al equipo. Esta característica, se ve apoyada por sistemas de almacenamiento tolerantes a fallos (si es que está configurado de esta forma), RAID 1 y RAID 5 principalmente. Estas características entre otras, hacen que un NAS sea un dispositivo propicio para realizar copias de seguridad de los datos.

NAS es muy útil para proporcionar el almacenamiento centralizado a ordenadores clientes en entornos con grandes cantidades de datos. El ámbito de utilización de NAS es bastante amplio, pero cada vez es más utilizado en entornos donde se necesita almacenar grandes cantidades de información multimedia.

En cuanto a su coste económico, el precio de las aplicaciones NAS se ha reducido en los últimos años, existiendo dispositivos para el consumidor doméstico, quizá sea este tu caso, con costo menor de lo normal, con discos externos USB o FireWire.

Reflexiona

¿Alguna vez has dejado un equipo encendido días enteros solamente para poder acceder a los datos desde otros equipos?

Ejercicio resuelto

Enumera alguna ventaja que pueda proporcionar la utilización de NAS a nivel de seguridad.

Mostrar retroalimentación

Algunas ventajas podrían ser:

- Almacenamiento en un soporte externo y alejado físicamente de los equipos.
- Puede proporcionar tolerancia a fallos (Mediante RAID).
- Son dispositivos preparados para realizar copias de seguridad a través de la red.

SAN.

En primer lugar, debes saber que las siglas **SAN**, podrían traducirse como red de área de almacenamiento. Por tanto, una SAN, consiste en una red dedicada exclusivamente al **tráfico de almacenamiento**. Estas redes están optimizadas para mover grandes cantidades de datos y utilizan tecnologías como Fibre Channel o **SCSI**.

La tecnología **Fibre Channel** consiste en un canal de fibra altamente veloz. El problema es que es una tecnología muy costosa. En la imagen puedes ver cables fibre channel.

Por otra parte, está **iSCSI** es una nueva tecnología que envía comandos SCSI sobre una red TCP/IP. Este método no es tan rápido como una red de fibra óptica, pero ahorra costes ya que utiliza un hardware de red menos costoso.

Las SAN se componen de tres **capas**:

- **Capa Host.** Esta capa consiste principalmente en servidores y software (sistemas operativos).
- **Capa Red.** Esta capa la conforman los componentes de la propia red: cables de fibra óptica (en el caso de red "Fibre Channel"), switches, etc.
- **Capa Almacenamiento.** Esta capa la componen elementos empleados para almacenar datos como discos, cintas, etc.

Además, las SAN tienen una serie de **ventajas** con respecto a la utilización de redes convencionales. Vamos a señalar algunas:

- **Menor tiempo de respuesta / Mayor velocidad.** De tal forma que se comparten datos en la red sin afectar al rendimiento, porque el tráfico de SAN está totalmente separado del tráfico de usuario. En definitiva, son dispositivos muy veloces y como subsistema del sistema principal que repercutirá en su velocidad de cómputo final.
- **Mayor conectividad.** Permite a un conjunto de servidores compartir el mismo medio de almacenamiento.
- **Posibilita una mayor distancia entre dispositivos.** En el caso de las SAN de fibra óptica, teniendo en cuenta las características de este medio de conexión, pueden tener dispositivos con una separación de hasta 10Km sin repetidores.
- **Disponibilidad.** Al tener mayor conectividad, permiten que los servidores y dispositivos de almacenamiento se conecten más de una vez a la SAN. De esta forma, se pueden tener rutas redundantes que, a su vez, incrementaran la tolerancia a fallos.

Una parte esencial de la seguridad de las SAN es la **ubicación física** de todos y cada uno de los componentes de la red. Cuando hablamos de ubicación física, nos referimos a la decisión de dónde pondremos los componentes de la red tanto software como hardware. Al implementar seguridad física, sólo los usuarios y usuarias autorizadas deben tener la capacidad de realizar cambios tanto físicos como lógicos en la topología. Además de la ubicación de los componentes, también debemos tener en cuenta las cuestiones físicas del **medio ambiente** como puede ser la refrigeración.

Además de todo lo mencionado, debemos tratar de que las redes que gestionan estos dispositivos sean seguras, de la misma forma que lo hacemos con otro tipo de redes, como utilizando **contraseñas** de acceso seguras y modificándolas regularmente.

Autoevaluación

Señala las afirmaciones correctas respecto a SAN:

- [ ] Son las siglas de Standard Attachment Network.
- [ ] Ofrece una mayor conectividad a cambio de un aumento en el tiempo de respuesta.
- [ ] iSCSI es una alternativa al Fibre Channel menos costosa.
- [ ] La conexión con fibra óptica proporciona la posibilidad de tener dispositivos bastante alejados físicamente.

Mostrar retroalimentación

Solución

1. Incorrecto
2. Incorrecto
3. Correcto
4. Correcto

Copias de Seguridad.

Caso Práctico

La empresa de Juan tiene diferentes departamentos, entre ellos un departamento comercial. Dicho departamento es el encargado de gestionar los datos de su clientela. Dichos datos están amparados por la LOPDGDD y es necesario tener especial cuidado a la hora de gestionarlos. La empresa tiene muy presente dicha ley ya que recoge una serie de obligaciones que todas las empresas deben cumplir.

Entre estas obligaciones está la de realizar copias de seguridad de los datos. Esta es precisamente la tarea que se disponen a llevar a cabo Juan y su jefe. Deben crear copias de seguridad de todo el fichero de datos personales de los clientes y clientas de la empresa.

-Bueno, voy a empezar a copiar los datos de los clientes a esta memoria USB. -Dice Juan con convencimiento-

-Espera Juan, hay una serie de cosas a tener en cuenta para hacer las copias de seguridad. En primer lugar debes buscar un soporte de almacenamiento que sea lo más seguro posible.

-Es verdad –reconoció Juan- una unidad USB no es demasiado segura, la podemos perder fácilmente.

-En relación al proceso, podemos utilizar algún programa que automatice la tarea –indicó Ignacio.

-Claro, por eso, hacen las copias siempre a la misma hora –observó Juan.

-Efectivamente, automatizando el proceso, todo será más fácil y evitaremos descuidos.

A continuación, Juan e Ignacio se pusieron manos a la obra eligiendo un software adecuado y configurándolo para que realice las copias automáticamente.

En este punto, comprenderás la importancia de las copias de seguridad y verás algunos mecanismos para llevarlas a cabo en diferentes ámbitos.

Reflexiona

Los fallos en los lápices de memoria USB son algo frecuente. ¿Alguna vez se te ha estropeado un lápiz donde guardabas información valiosa? En tal caso, ¿Has logrado recuperarla? En muchos casos, cuando el problema afecta físicamente a la propia memoria, se hace imposible recuperar los datos. Si nunca te has visto en dicha situación piensa en las consecuencias que podría acarrear. ¿Cómo lo podrías solucionar?

Políticas de Copias de Seguridad.

Debes ser consciente, de que la información es el único elemento en un equipo que puede llegar a ser imposible de sustituir. Teniendo en cuenta que a la hora de realizar copias de seguridad hay muchos parámetros que pueden variar, es importante hacer una buena **planificación** como paso previo. Estos parámetros o directrices, están recogidos en la política de copias de seguridad. Por ejemplo, la periodicidad con la que se van a hacer o el soporte en el que se van a almacenar. Cuando tomamos decisiones para llevar a cabo las copias de seguridad es importante que exista un equilibrio entre el coste de realizar una copia y las consecuencias que ocasionaría perder esos datos.

A continuación vamos a ver con más detalle algunos de los principales parámetros a definir junto con algunas recomendaciones:

- **Periodicidad de las copias**: debemos definir cada cuanto tiempo se van a realizar las copias. Este parámetro dependerá, en gran parte, de la frecuencia con la que actualicemos los datos que queremos guardar y de su importancia. Por ejemplo, no vamos a guardar todos los días unos datos que sabemos que modifican muy pocas veces al año. En cambio, los datos importantes que se modifican con frecuencia seguramente sí conviene salvarlos diariamente.
- **Lugar y soporte de almacenamiento**: otro elemento a tener en cuenta es el soporte de almacenamiento. Este podrá ser de diferentes tipos, discos ópticos, memorias flash, discos duros externos, servidores remotos, etc. En este aspecto, habrá que tratar de que el soporte sea lo más fiable posible. Por ejemplo, las memorias flash o los lápices de memoria son dispositivos que suelen fallar bastante, no siendo lo más aconsejable para una copia de seguridad.
  En cuanto la ubicación de las copias, en principio se recomienda que los datos no se guarden en una partición del mismo disco, ya que si falla el disco también perderemos la copia de seguridad. Este criterio es ampliable hasta el punto que las grandes empresas ni siquiera guardan las copias de seguridad en el mismo edificio, para evitar que una catástrofe como un incendio pueda terminar con todo.

- **Etiquetado y comprobación de las copias**: el etiquetado de las copias de seguridad es un aspecto al que se le resta importancia frecuentemente. De poco sirve que realicemos correctamente las copias de seguridad si cuando llega el momento de restaurarlas no somos capaces de determinar donde se encuentra la información que perdimos, cuando se realizó la copia o quien es el responsable de la misma. Por esta razón, es muy recomendable etiquetar las copias con al menos la siguiente información: un **código** o identificador que diferencie cada copia, **el tipo** de copia (total, incremental o diferencial), **la fecha**, su **contenido** y el **responsable** de la misma.
  Además de etiquetar la copia, es conveniente que cada cierto tiempo se compruebe que la copia se realizó correctamente.

- **Otros aspectos**: aparte de lo que ya hemos dicho en los puntos anteriores, es importante que las copias de seguridad se realicen de **forma automática**. Así evitaremos descuidos y errores. Además, la franja horaria donde se realiza la copia, también llamada **ventana de backup**, conviene que esté en un horario en el que la actividad sea la menor posible. Por ejemplo, por la noche considerando un equipo con el que se trabaje de día normalmente.

Autoevaluación

Señala las prácticas recomendables a la hora de hacer una copias de seguridad:

- ○ Realizar copias diariamente de cualquier tipo de dato para asegurarnos de que no se pierde nada.
- ○ Guardar los datos en una ubicación física diferente a la de los datos originales.
- ○ Realizar copias manualmente, ya que si utilizamos software para automatizar la copia ralentizará mucho el equipo.
- ○ Las tres opciones son incorrectas o más de una es correcta.

Incorrecta. Es conveniente guardar las copias con la frecuencia que sea necesaria, especialmente para datos importantes. Pero no conviene guardarla todos los días ya que las copias son costosas, tanto económicamente hablando como computacionalmente.

Exacto, de lo contrario, es más fácil que la copia sea destruida por la misma causa que acabó con los datos originales.

Falso. Conviene que automaticemos las copias para evitar descuidos. El problema del consumo de recursos se minimizará si programamos las copias en horas en las que el equipo esté inactivo.

No es correcta, ya que solamente es correcta la opción que habla de la ubicación física de los datos.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

Clasificación.

Ahora, que tendrás más claro lo que son las copias de seguridad y la utilidad que tienen, vamos a clasificarlas. Dicha clasificación la haremos **en función de la información que se guarda** cada vez que se hace una copia de seguridad. De tal modo que podemos efectuar:

- **Copias totales:** en cualquier tipo de copia, el primer paso es una copia total. A partir de esa primera copia es cuando se diferencia cada tipo. Cuando realizamos una copia total, quiere decir que vamos a copiar toda la información que queremos almacenar en la copia de seguridad, independientemente de que se haya modificado o no anteriormente.
- **Copias diferenciales:** una vez hecha la primera copia total, las siguientes copias van a contener todos los ficheros que hayan sido modificados tomando como referencia la copia total. En la siguiente ilustración puedes comprobar que el segundo día se realiza una copia de la franja de ficheros modificados. En el tercer día, se copia una nueva franja de ficheros que se han modificado, pero además, se vuelven a copiar los ficheros que fueron modificados en el segundo día.

- **Copias incrementales:** en este caso, se copian solamente los ficheros modificados tomando como referencia la anterior copia. Como puedes ver en la siguiente ilustración, hasta el segundo día, el procedimiento es el mismo que en la copia diferencial. Es en el tercer día cuando, a diferencia de la copia diferencial, solamente copia los ficheros modificados respecto al segundo día.

Para saber más

En este enlace podrás ver como se aplica el procedimiento de copias de seguridad por parte de Microsoft a una base de datos SQL Server.

Copias de Seguridad y Restauración de Base de Datos en entorno Microsoft

Copia de Seguridad del Registro.

Aunque normalmente, son las aplicaciones las que editan este registro de forma automática, es posible que en alguna ocasión hayas tenido que modificar el registro de Windows. En el registro se guarda información sobre el hardware, aplicaciones que tenemos instaladas en nuestro equipo, cuentas de usuario, etc. Debes tener en cuenta que estos datos suelen ser bastante delicados. De hecho, si modificamos algunos elementos indebidamente, podríamos hacer que el equipo deje de funcionar. Por esta razón, siempre es conveniente realizar una copia de seguridad del registro antes de realizar alguna modificación.

Veamos como hacerlo, es un proceso bastante sencillo:

1. En primer lugar debemos iniciar una sesión con una cuenta de administrador.
2. Desde "Ejecutar" tecleamos **regedit**.

   Otra opción para acceder al registro es escribir desde línea de comandos la instrucción **regedit**.

3. Una vez abierto el editor, seleccionamos el elemento del que queremos hacer la copia, en este caso como queremos realizar una copia del registro completo, seleccionaremos el equipo (Mi PC / Equipo, dependiendo de la versión de Windows).

4. Seleccionamos la opción Archivo > Exportar.
5. Una vez cuando realizamos el paso anterior, aparece un diálogo para guardar el fichero. Hacemos lo mismo que haríamos para guardar cualquier otro fichero, asignándole un nombre y su ubicación. En ese mismo diálogo, se nos permitirá (dependiendo de la versión de Windows, exportar solo lo seleccionado o exportar todo el registro).

Este proceso es válido tanto desde Windows XP hasta Windows 10.

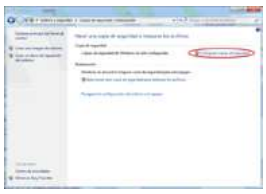
Copia de Seguridad de Datos en Windows.

A la hora de realizar copias de seguridad tendrás varias opciones. Por un lado, es posible que dependiendo del sistema operativo que utilices, que éste incluya soporte para las copias de seguridad. Otra opción será, la de instalar un software específico para dicho cometido.

En este caso, vamos a ver como realizar un backup con las herramientas que proporciona **Windows 7**. No obstante, anteriores versiones de Windows también ofrecen herramientas similares. Asímismo, **Windows 10** ofrece una herramienta prácticamente idéntica a esta aquí descrita.

Lo primero que vamos a hacer, es acceder a la herramienta de copias de seguridad. Para ello, vamos a "Panel de control > Sistema y seguridad > Hacer una copia de seguridad del equipo".

Posteriormente, seleccionamos "Configurar copias de seguridad" en el panel siguiente:



En la siguiente ventana, debemos seleccionar una ubicación para almacenar la copia de seguridad. Las copias de seguridad se pueden almacenar en un CD/DVD, un lápiz de memoria, una unidad flash o en un disco de red, aunque debemos fijarnos que tenga como mínimo 1GB de capacidad.

En el caso de que decidamos guardar una copia de seguridad en un disco de red, deberemos configurar algunos parámetros más. En nuestro caso vamos a seleccionar un disco externo.

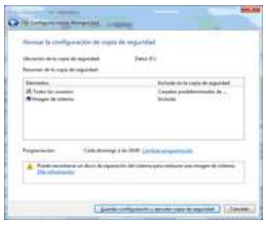
Una vez que hemos seleccionado la unidad donde guardar la copia de seguridad, el sistema operativo nos permite dejar que sea él quien determina las carpetas y ficheros a guardar o ser nosotros quien decidamos estos datos. Si pulsamos sobre "Dejar a Windows que elija", el proceso se creará sólo. Si por el contrario, pulsamos sobre "Déjame Elegir", se abrirá otra ventana en la que tendremos que seleccionar las carpetas o ficheros que queremos incluir en nuestra copia de seguridad.

También permite, además, la opción de crear una copia de seguridad de los ficheros **asociados a una cuenta** de usuario en concreto.

Seleccionadas las carpetas que queremos incluir en nuestra copia de seguridad, el siguiente paso del asistente nos preguntará si deseamos crear un programa de copias de **seguridad automáticas** que se ejecutará con la frecuencia temporal que nosotros indiquemos.

Si queremos omitir este paso, sólo tendremos que desmarcar la casilla "Ejecutar copia de seguridad de forma programada", aunque, como hemos dicho anteriormente, es aconsejable hacerlas programadas para evitar descuidos y errores que puedan ocasionar pérdidas de datos importantes en un futuro.

En la siguiente captura vemos la última ventana del asistente con un resumen de la configuración.



Una vez guardada nuestra copia de seguridad, podremos restaurarla en el momento que nos haga falta desde el mismo panel de Copias de Seguridad.

Copia de Seguridad de Datos en Linux.

Una vez que has visto como hacer una copia de seguridad en Windows, vamos a ver un ejemplo del proceso en un sistema operativo Linux. En este caso veremos el ejemplo en un Ubuntu 18.04.

En primer lugar debemos instalar un software llamado **"duplicity"**. Para ello, abrimos el terminal desde “Sistema > Terminal” y tecleamos la siguiente instrucción:

```
sudo apt install duplicity
```

Una vez instalado el programa lo ejecutamos vamos a ejecutar desde el terminal, tal y como hicimos para su instalación. Principalmente vamos a tener dos opciones:

duplicity [full | incremental] [opciones] dir_origen url_destino

duplicity [restore] [opciones] url_origen dir_destino

Si se ejecuta el comando:

duplicity --help

obtendremos una información completa de las diferentes opciones. Así, se puede realizar realizar un encriptado de la copia, una compresión de la misma, etc.

duplicity /home/usuario/Documentos file:///backup/usuario/Documentos

nos va a realizar un copia de seguridad de los archivos que se encuentran en la carpeta Documentos dentro de /home/usuario en la carpeta Documentos que se encuentra dentro de /backup/usuario

Si quisieramos restaurar una copia, haríamos lo siguiente:

duplicity file:///backup/pepito/Descargas /home/pepito/Descargas/Restaurado

Al hilo de esto, el cron nos permitiría configurar temporalidad para llevar a cabo esta tarea (automatización). Es interesante conocer los atributos del cron. El cron tiene 5 caracteres, el primero se refiere a los minutos (0-59), el segundo a las horas (0-23), el tercero especifica el día del mes (1-31), el cuarto el mes (1-12) y el quinto es para referirse al día de la semana (0-6, siendo 0 el Domingo). Si colocamos un asterisco en alguna de las 5 posiciones, quiere decir que se **ejecutará la copia en todos los elementos de ese rango**. Por ejemplo un asterisco en la tercera posición significa que la copia se ejecuta todos los días del mes.

Autoevaluación

Teniendo en cuenta lo que sabes sobre los parámetros del Cron, una configuración con los parámetros “0 1 * * *”, significa que la copia de seguridad se ejecutará…

- ○ A las 00:01h todos los días del año.
- ○ A la 1:00h todos los días del año.
- ○ Todos los domingos del mes de Enero.
- ○ Todos los días 1 de cada mes a las 01:00h.

Incorrecto, el primer parámetro indica los minutos y el segundo las horas y no al revés como indicaría este caso.

Muy bien, has captado la idea. El primer número especifica los minutos, por tanto, es una hora en punto, el segundo las horas, lo que quiere decir que es a la 1 y por último, los asteriscos indican que será todos los días de cada mes.

No es correcto, para especificar los Domingos habría que poner un 0 en el último parámetro.

No es la opción correcta, para especificar que se realice el día uno de cada mes se debería poner un 1 en el tercer parámetro.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto

4. Incorrecto

Recuperación de Datos.

Caso Práctico

Julián es un empleado que trabaja en el departamento de Recursos Humanos de la empresa. Un día, haciendo una "limpieza" de ficheros que ya no necesitaba, borró por equivocación una carpeta que contenía una serie de documentos que había estado redactando en el último mes.

Aunque Julián no es ningún experto en informática, sabe que es posible restaurar ficheros que han sido mandados a la papelera de reciclaje, pero en este caso, los ha borrado con la combinación de teclas "shift + supr", con lo cual se pone en lo peor.

Aún así, su compañero Isaac, que está enterado del problema, trata de tranquilizarle:

-Tranquilo Julián, no está todo perdido. Yo tengo un amigo que perdió todas las fotos de su boda por un error similar y se puso en contacto con una empresa. Finalmente, después de pagar una cantidad bastante razonable, no me preguntes cómo, pero consiguieron recuperar las fotos.

-¿Es que existen empresas dedicadas a la recuperación de datos?

-Sí claro. Por eso, no des los datos por perdidos hasta haber agotado todas las posibles soluciones.

-Eso me deja más tranquilo, no obstante hablaré antes con Ignacio y Juan, a ver que me cuentan.

Un poco más aliviado, Julián decide llamar a Juan e Ignacio y comentarles lo que le ha pasado para ver si existe alguna posibilidad de recuperar los ficheros borrados.

En la primera unidad has visto lo que existen mecanismos de prevención, de detección y de recuperación. Como su propio nombre indica, la recuperación de datos, es un claro ejemplo de un mecanismo de recuperación.

Llamamos **recuperación de datos** a una serie de procedimientos que llevamos a cabo para recuperar información que ha sido borrada previamente por un ataque, un accidente o un error.

Software de Recuperación de Datos.

En la mayor parte de los casos, cuando borramos un dato en el disco duro, dicho borrado no es un borrado **físico**, sino que el disco **marca** como disponible la parte del mismo donde estaban almacenados esos datos. Por tanto, existen programas que pueden aprovechar este hecho para recuperar la información antes de que esa parte del disco sea sobrescrita. En los casos en los que los datos de pierden por un problema en el medio físico de almacenamiento, resulta mucho más difícil llegar a recuperar los datos, llegando a ser imposible en ocasiones.

Un programa clásico es la recuperación de datos es **Recuva**. Se trata de un programa gratuito. Su manejo es muy simple y permite hacer recuperaciones selectivas. No obstante, existen multitud de programas para la recuperación de datos y ninguno es infalible. La elección de un programa u otro dependerá de las necesidades concretas de cada usuario o usuaria.

Además de existir diversos programas que podemos utilizar para tratar de recuperar datos borrados, existen numerosas empresas dedicadas exclusivamente a este cometido, que cuentan con sofisticadas tecnologías.

Debes conocer

En el siguiente vídeo-tutorial puedes ver una demostración de los sencillos pasos que debes seguir para configurar una búsqueda con el asistente de Recuva.

Tutorial Recuva.

http://www.youtube.com/embed/imdxegUUw5o

Creación de Imágenes del Sistema.

Hasta ahora has visto algunas posibilidades en cuanto a copias de seguridad de los datos. En este epígrafe verás que también existe la posibilidad de crear **copias del sistema al completo**. De esta forma realizaremos una copia del estado actual del sistema que nos será muy útil en caso de tener que volver a instalarlo por algún problema.

Para realizar una imagen del sistema existen diferentes programas. Algunos de los más conocidos son **Clonezilla** o **Acronis True Image**.

Ejercicio resuelto

Explica brevemente los pasos que debes seguir para crear una imagen de una partición con el software Acronis True Image.

Mostrar retroalimentación

En este caso hemos utilizado una versión de prueba del Acronis True Image Home 2011, que se puede descargar del siguiente enlace:

Descarga de Acronis.

Al ejecutar la aplicación nos encontramos con una ventana como la siguiente:

Seleccionamos la opción "Ir a pantalla principal" para ver el resto de las opciones.

En este caso seleccionamos "Copia de seguridad de discos y particiones". Esta opción nos llevará a un pequeño asistente donde tenemos que seleccionar las particiones de las que queremos crear la imagen y la ubicación donde la queremos almacenar.

Debes tener en cuenta que la imagen de una o varias particiones puede llegar a ocupar bastante espacio, por lo que debes asegurarte de que la ubicación de destino cuenta con el suficiente espacio libre.

Una vez realizado el proceso tendremos una imagen con **extensión .tib**.

A la hora de utilizar la imagen tenemos la posibilidad de restaurar la imagen completa, con lo cual, necesitaríamos crear un disco de arranque de Acronis para restaurar la imagen desde el mismo. Por otra parte, es posible que no necesitemos restaurar todo el sistema, sino recuperar algún elemento en concreto de la copia de seguridad. En este caso, debemos hacer clic con el botón derecho encima de la imagen y seleccionar "Archivo comprimido > Montar".

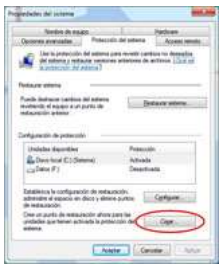
Entonces se lanzará un asistente que nos preguntará por la **letra** que queremos asignar a la **unidad virtual** que se va a formar a partir de la imagen. Una vez seleccionada, podemos ver en el equipo la unidad virtual como si fuese cualquiera de las unidades reales, de forma que podremos explorarla y recuperar los ficheros que necesitemos.

Restauración del Sistema.

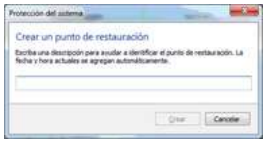
Como vas a ver a continuación, en los sistemas operativos de Microsoft, tenemos la opción de incluir **puntos de restauración del sistema**. De esta forma, podremos volver a un punto anterior al momento en que se produce un fallo sin tener que volver a reinstalar todo el sistema operativo desde cero. Dependiendo de la versión del sistema operativo, puede existir la opción de guardar los puntos de restauración automáticamente. Para esto, debemos tener activada la protección del sistema. Debes tener en cuenta que restaurar sistema puede llegar a ocupar un parte importante del disco duro (en torno a un 15%).

A continuación vamos a ver como crear un punto de restauración de forma manual. Este método se puede aplicar a Windows 7, Windows 8 / 8.1 y Windows 10.

En primer lugar, vamos a "Equipo > Propiedades > Propiedades del Sistema" o "Equipo > Propiedades > Configuración Avanzada del Sistema" (dependiendo de la versión de Windows) y veremos una ventana como la siguiente.

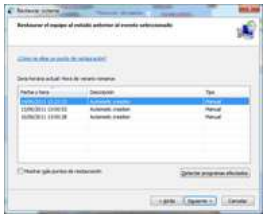


En la pestaña "Protección del Sistema" tenemos un botón "Crear" para crear un punto de restauración. Después de hacer clic, podemos ver otra ventana en la que nos pide que le pongamos un nombre al punto de restauración.

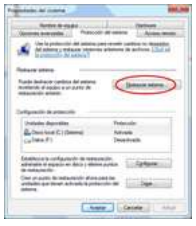


Con estos sencillos pasos ya tendríamos creado un punto de restauración. Vamos a ver ahora como podríamos restaurar el sistema a uno de los puntos guardados previamente.

En primer lugar vamos a la misma ventana que cuando creamos el punto de restauración, peor en este caso nos fijamos en un botón que pone "Restaurar sistema".



Una vez que hacemos clic en dicho botón, veremos una ventana en la que se muestran los puntos de restauración guardados hasta el momento.



Por último, elegiremos uno de los puntos y haremos clic en siguiente para terminar con los pasos que determina el asistente.

Para saber más

Enlace a un artículo de la compañía Microsoft en el muestra, de manera guiada, cómo usar la restauración del sistema de manera correcta en Windows:

Guía - Cómo usar Restaurar Sistema correctamente.

Anexo.- Licencias de Recursos.

Licencias de recursos utilizados en la Unidad de Trabajo.

Recurso (1)	Datos del recurso (1)	Recurso (2)	Datc
	Autoría: ejbsf Licencia: CC BY-NC-ND Procedencia: http://www.flickr.com/photos/ejbsf/3492566759		Autoría: alejandrocolombo Licencia: CC BY-NC-SA Procedencia: http://www.flickr.co
	Autoría: edans Licencia: CC BY Procedencia: ttp://www.flickr.com/photos/edans/221269446/sizes/s/in/photostream/		Autoría: william hook Licencia: CC BY-SA Procedencia: http://www.flickr.co
	Autoría: nearsoft Licencia: CC BY-NC-SA Procedencia:http://www.flickr.com/photos/nearsoft/3704855174		Autoría: -Jos Licencia: cc by-nc-sa Procedencia: http://www.flickr.co
	Autoría: zdw Licencia: CC BY-SA Procedencia: http://www.flickr.com/photos/zdw/181740158		Autoría: JaviMZN Licencia: CC BY http://upload.wikimedia.org/wikip Raid0.png
	Autoría: JaviMZN Licencia: CC BY Procedencia: http://upload.wikimedia.org/wikipedia/commons/thumb/e/e2/Raid1.png/461px-Raid1.png		Autoría: JaviMZN Licencia: CC BY Procedencia: http://upload.wikimedia.org/wikip Raid5.png
Esquema del nivel RAID 0 + 1	Autoría: JaviMZN Licencia: CC BY Procedencia: Montaje sobre http://upload.wikimedia.org/wikipedia/commons/thumb/c/c4/Raid0mas1.png/692px-Raid0mas1.png		Autoría: Diego Méndez Licencia: Copyright (cita) Procedencia: Captura de pantall
	Autoría: mpolla Licencia: CC BY-NC-SA Procedencia: http://www.flickr.com/photos/mpolla/329018110/		Autoría: skimaniac Licencia: CC BY-NC Procedencia: http://www.flickr.co
	Autoría: penguincakes Licencia: CC BY-NC-SA Procedencia: http://www.flickr.com/photos/penguincakes/2826994009		Autoría: Rocío Lara Licencia: CC BY-NC-SA Procedencia: http://www.flickr.co
	Autoría: driusan Licencia: CC BY-NC Procedencia: http://www.flickr.com/photos/driusan/2472706272/		Autoría: olivierh Licencia: cc by-nc-nd Procedencia: http://www.flickr.co
	Autoría: herrolm Licencia: cc by-nc Procedencia: http://www.flickr.com/photos/herrolm/2820552527		Autoría: tonyhall Licencia: CC BY-NC-SA Procedencia: http://www.flickr.co
	Autoría: Diego Méndez Licencia: Copyright (cita) Procedencia: Captura de pantalla en Windows XP (ejecutar)		Autoría: Diego Méndez Licencia: Copyright (cita) Procedencia: Captura de pantall
	Autoría: Diego Méndez Licencia: Copyright (cita) Procedencia: Captura de pantalla en Windows XP (Editor del registro)		Autoría: Diego Méndez Licencia: Copyright (cita) Procedencia: Captura de pantall
	Autoría: Diego Méndez Licencia: Copyright (cita)		Autoría: Diego Méndez Licencia: Copyright (cita)

	Procedencia: Captura de pantalla en Windows 7		Procedencia: Captura de pantall
	Autoría: Diego Méndez Licencia: Copyright (cita) Procedencia: Captura de pantalla en Windows 7		Autoría: Diego Méndez Licencia: SO Ubuntu, propiedad Procedencia: Captura de pantall
	Autoría: Diego Méndez Licencia: Copyright (cita) Procedencia: Captura de Recuva, propiedad de Piriform		Autoría: Diego Méndez Licencia: Copyright (cita) Procedencia: Captura de pantall
	Autoría: Diego Méndez Licencia: Copyright (cita) Procedencia: Captura de pantalla de Acronis, propiedad de Acronis		Autoría: Diego Méndez Licencia: Copyright (cita) Procedencia: Captura de pantall
	Autoría: Diego Méndez Licencia: Copyright (cita) Procedencia: Captura de pantalla en Windows 7		Autoría: Diego Méndez Licencia: Copyright (cita) Procedencia: Captura de pantall
	Autoría: Diego Méndez Licencia: Copyright (cita) Procedencia: Captura de pantalla en Windows 7		Autoría: Diego Méndez Licencia: Copyright (cita) Procedencia: Captura de pantall

Cloud Computing.

Como sabes, mantener la información en unas condiciones favorables desde el punto de vista de la seguridad, requiere un consumo de recursos importante. Empezando por el propio medio de almacenamiento y siguiendo por un conjunto de mecanismos de **seguridad activa** que sean capaces de prevenir fallos, así como, **mecanismos pasivos** de recuperación en caso de que se produzcan errores.

En algunas ocasiones, este despliegue de recursos no está al alcance de la organización utilizando sus propios medios. En otras ocasiones, aun estando dentro de sus posibilidades, no compensa con respecto a otro tipo de soluciones.

Entre las alternativas posibles a este planteamiento se encuentra lo que se conoce como "**Cloud Computing**" o computación en la nube. Esta solución consiste básicamente en almacenar no solamente datos, sino las propias aplicaciones en servidores remotos, de manera que se contrata el servicio a una empresa que se compromete a mantener nuestros datos y aplicaciones en unas condiciones adecuadas. De esta forma, la organización puede delegar el conjunto de responsabilidades y de gastos de los que hablábamos al principio de este epígrafe a cambio de pagar una cuota a la empresa que ofrece el servicio.

En muchos casos, dependiendo de la empresa, es posible que entre las condiciones de contratación exista algún tipo de seguro con indemnizaciones en caso de pérdida de datos o caída de algún servicio.

Debes conocer

El siguiente vídeo, ilustra de forma gráfica el concepto de cloud computing.

Cloud computing