Práctica 2: Copias de Seguridad

Actividad 1

Realiza una investigación sobre los principales soportes para copias de seguridad utilizados en un entorno empresarial. Realiza una comparativa de las ventajas e inconvenientes de uso de cada uno de ellos.

1. EaseUs Todo

Realiza respaldo de archivos, de discos y del sistema completo.

Realiza copias incrementales y diferenciales.

Tiene opción de clonación de disco, bit a bit.

Puedes crear discos de recuperación de arranque.

Permite el uso de compresión y encriptado.

Permite planificar copias de seguridad automatizadas.

Posee un sistema de control del rendimiento.

Puede correr un entorno de rescate Linux.

Se adapta a usuarios avanzados e inexpertos.

Es fácil de usar por su interfaz clara e intuitiva.

Existe una opción gratuita.

2. Comodo Backup

Respalda archivos, directorios, particiones y unidades.

Almacena copias de seguridad en tu disco local o las envía a servidores externos vía FTP, o a la nube de Comodo.

Comprime y encripta archivos.

Hace copias de seguridad completas, diferenciales e incrementales.

Programa backups a intervalos regulares que se puede usar en segundo plano.

Cuenta con edición gratuita que viene con 10GB de almacenamiento online, gratis, durante 90 días.

Tiene un funcionamiento sencillo.

Es muy flexible.

3. Aomei Backupper Standard

Permite la sincronización de archivos.

Realiza imágenes de disco o del sistema.

Permite clonar discos.

Automatiza los respaldos a intervalos regulares.

Puede crear discos de rescate para emergencias.

Posee un planificador muy flexible.

Es fácil de utilizar.

Es perfecto para usuarios inexpertos.

4. Areca Backup

Es más complejo de utilizar.

Puede filtrar los respaldos por extensión, carpeta, tamaño, fecha, estado y expresión regular.

Posee compresión Zip y soporte Zip64, AES y encriptación AES256.

Realiza copias de seguridad de unidades locales o de red.

Usa protocolos de transferencia de datos FTP, FTPS o SFTP.

Tiene una interfaz poco amigable.

Puede realizar copias de seguridad de parte de archivos modificadas.

Puede recuperar archivos de una fecha específica.

Es un programa dirigido al usuario experto.

5. Cobian Backup

Programa multi tarea.

Se ejecuta en segundo plano

Crea copias de seguridad de un equipo, una red local o de/desde un servidor FTP

Consume muy pocos recursos (tanto de hardware como de red)

Permite encriptar la información

No es sencillo de usar

Actividad 2

Realiza una investigación sobre las principales herramientas utilizadas para copias de seguridad en entornos GNU/Linux y ámbito empresarial. Realiza una comparativa de las principales ventajas que presentan cada una ellas.

Dentro del ámbito doméstico se pueden utilizar las herramientas Dejà Dup y Sbackup. ¿En qué sentido podrían ser utilizadas dentro de un entorno empresarial?

Simple Backup

Se trata de una opción muy sencilla pero no por ello exenta de opciones. En este caso nos permite definir qué directorios incluimos en las copias de seguridad y dentro de los mismos que tipo de archivos. Por ejemplo, podemos omitir los archivos de música o copiar sólo los de imagen. Tiene la opción de crear expresiones regulares para definir estos aspectos, lo que flexibiliza mucho la selección de los archivos.
Podemos programar las copias de forma diaria, semanal o mensual. A la vez también las podemos realizar de forma manual. El gran pero que le podemos poner a esta opción es que no realiza copias diferenciales, lo que traducido quiere decir que sólo copiará los archivos que hayan cambiado desde la última copia de seguridad completa.

Mint copia de seguridad

Se trata de una opción que viene en los paquetes de Linux Mint 9, pero que no he conseguido encontrar en otras distribuciones. Su gran punto a favor es que nos puede hacer una copia de seguridad del software que tenemos instalado en nuestra distribución de Mint. En este sentido basta con seleccionar que programas o paquetes queremos tener una copia de seguridad e indicarle la carpeta de destino de la copia. Muy interesante cuando vamos a instalar algún paquete que está todavía en beta y si no funciona como necesitamos volver atrás será muy fácil.
Respecto a la copia de archivos, es un sistema para realizar la copia de forma esporádica, puesto que no permite ni programar la copia ni copias diferenciales, lo cual limita mucho su ámbito de acción. En este caso está bien para el ámbito doméstico pero queda corta para un usuario más exigente.

Sbackup

En este caso no es una solución específica de copias de seguridad, sino de sincronizacion de carpetas. Sin embargo nos puede ser muy útil cuando realizamos copias de seguridad de manera esporádica, puesto que podemos sincronizar nuestro archivo original con nuestra copia de seguridad, de manera que sólo se copiarán los archivos nuevos que no estén en la copia ya generada en un primer momento. Funciona de forma ágil y en el modo usuario experto nos permite configurar toda una serie de opciones por defecto que nos evitarán responder a las preguntas que nos formula si encuentra un archivo duplicado o modificado y más nuevo en la copia que en el original. Es una gran opción para realiza copias de seguridad en discos duros externos de forma puntual.

Déjà Dup

Fedora tiene por defecto uno de los más completos gestores de copia de seguridad, Déjà Dup, no en vano es la distribución más enfocada al mercado profesional y en este caso se nota. No le faltan

opciones a la hora de configurarlo, para que nos ejecute la copia en un servidor remoto y subirla utilizando distintos protocolos. También nos permite la opción de encriptar la información de manera que el flujo de datos vaya encriptado.

Tampoco faltan opciones para configurar los archivos que copiamos, aunque quizás no nos permite excluir determinados tipos de archivos. Su punto débil puede estar en la falta de una copia diferencial que nos permita crear un esquema de seguridad programado más completo y seguro.

En definitiva, no existe el sistema perfecto o por lo menos yo no lo he encontrado. Para mi gusto, los más completos son los que incorporan OpenSuse y Fedora, siendo Déjà Dup mi favorito, que también se encuentra disponible para otras distribuciones. Además debemos tener en cuenta que tan importante es realizar la copia de seguridad como la facilidad para restaurar la copia. Las opciones analizadas pueden ser suficientes para el usuario doméstico y quizás algo más escasas para entornos profesionales que exigen esquemas de seguridad más completos.

Actividad 3

Una empresa dispone de 1 servidor NAS para albergar documentos, 1 servidor de base de datos y 1 servidor de aplicaciones, todos ellos con entorno operativo GNU/Linux. Proporciona servicio a unos 100 puestos de trabajo cliente con sistema operativo Microsoft Windows 10, en los cuales los usuarios no deberían guardar ningún tipo de documento que pueda ser susceptible de pérdida; si un documento se pierde de un puesto de trabajo se considerará que es responsabilidad del usuario aunque no obstante el Departamento de Informática debe proporcionar las herramientas adecuadas para que los usuarios puedan realizar sus propias copias personales y albergarlas en el espacio que tienen disponible en el servidor NAS, donde podrán ser incluidas en la copia de seguridad corporativa.

Se considera que los datos albergados en la base de datos son críticos, por lo que el tiempo de recuperación de los mismos frente a una eventual pérdida o corrupción de datos debe ser mínimo. Por otro lado, algunos de estos datos están catalogados como de nivel medio/alto según el Documento de Seguridad conforme a la LOPD.

Los documentos albergados en el servidor NAS pueden ser considerados como no tan críticos, por lo que la pérdida o corrupción de los mismos es posible asumirla con una pérdida de las modificaciones realizadas de hasta 12 horas.

El servidor de aplicaciones no debería albergar datos más allá de los temporales para el correcto desempeño de sus funciones.

Los diferentes puestos de trabajo deben estar operativos en un tiempo de máximo de 3 horas frente a cualquier posible incidencia. No son importantes los datos contenidos en ellos de los que el propio usuario no se haya hecho responsable realizando una copia de seguridad que deberá haber albergado en otro soporte.
Se pide diseñar una estrategia de copia de seguridad que permita una rápida recuperación de los datos en caso de desastre (pérdida o corrupción de los datos) y minimice tanto el tiempo como la ocupación de los datos respaldados. Se deberá intentar hacer uso de las estrategias de copias de seguridad completas, incrementales y diferenciales.

Pon un ejemplo del procedimiento de restauración para la estrategia de copia de seguridad que has planteado.

Podemos optar por varias opciones a la hora de crear copias de seguridad: o lo hacemos de forma básica para tranquilizar la conciencia, o evaluamos los riesgos de verdad para evitar que cualquier tipo de imprevisto se convierta en un gasto inesperado a final de mes. Esto implica desarrollar una estrategia de copias de seguridad, que deberá seguirse con rigor para que la empresa pueda trabajar en condiciones de seguridad.

Existen diferentes fórmulas, tanto con dispositivos físicos como programas en la nube, para realizar copias de seguridad. Cualquiera que sea el sistema que utilicemos, debes cuidar de hacer copias de respaldo teniendo en cuenta algunos esenciales en tu estrategia de seguridad informática.

¿Qué ficheros debo incluir en mis copias de seguridad?

Este es un punto importante. A veces las empresas sólo guardan en las copias de seguridad los trabajos diarios de sus clientes. Pero, ¿tenemos copia de seguridad de nuestro sistema operativo? ¿hemos realizado copias de seguridad de nuestros programas?

Y en cuanto a los archivos que están en un servidor externo, sujeto a otras medidas de seguridad, como nuestra página web, ¿tenemos una copia nosotros en caso de que fallara la empresa con la que trabajamos?

Cada cuánto se van a hacer las copias de seguridad?

Otro detalle relevante que debes fijar en tu estrategia. ¿Cada cuánto tiempo deseas tener copias de seguridad? ¿Cada día? ¿Cada semana? La respuesta a esta pregunta depende en gran parte de la naturaleza de los ficheros.

No es necesario hacer una copia de seguridad de los archivos que no cambian demasiado, pero sí es muy importante que la última versión guardada de los ficheros muy cambiantes (trabajo diario) sea lo más actual posible, ya que si no perderemos parte de nuestro esfuerzo.

¿Las copias serán automáticas, o manuales?

En este aspecto hay que preguntarse por los riesgos de seguridad de la empresa. Cuando se estropea un ordenador, ¿sucede de improviso o con previo aviso? ¿verdad que siempre sucede en el momento más inoportuno?

Si nuestras copias son manuales, estamos sujetos a una tasa de incidencias mucho más elevada: errores humanos (al empleado se le olvidó hoy hacer el backup) o por falta de previsión en el tiempo (hice la copia de seguridad ayer, pero los trabajos del miércoles al domingo se han borrado todos).

En caso de fallo de seguridad, ¿cuánto tiempo se tarda en recuperar los archivos perdidos?

En las grandes organizaciones, esta pregunta se vuelve muy compleja. Sobre todo, en los casos en los que se ha borrado una gran parte de los ficheros necesarios para el trabajo.

La empresa no puede estar días y días esperando a encontrar un archivo, que no sabemos si estaba en el disco duro A o en el Z, ni en qué carpeta. Al igual que en cualquier almacén, un fichero mal etiquetado o sin nombre es un fichero casi perdido.

Ficheros informáticos

¿Has asegurado tus copias de seguridad?

Hay empresas que no tienen en cuenta que están en ocasiones guardando archivos personales de particulares o empresas y por lo tanto son de carácter privado y tienen una responsabilidad en caso de violación de la privacidad. Tu negocio es el responsable en caso de que se produjera cualquier fallo de seguridad y éste fichero cayera en malas manos.

Por tanto, no sólo has de crear copias de respaldo, sino asegurarte de que ninguna persona ajena a ti, que es con quien esa persona física o jurídica ha firmado el contrato, pueda acceder o robar esos ficheros. Se impone crear ficheros encriptados si trabajamos con backup en la nube y también disponer de un sistema de protección online actualizado.

Si fallaran las copias de respaldo, ¿tengo otras?

Resulta que hay empresas, una gran parte de ellas, que sólo trabajan con discos duros externos .Pero, ay, un día el disco duro en el que guardábamos absolutamente todo, desde inventarios hasta las facturas, se cae al suelo, se rompe y ya no se puede acceder; o lo dejamos al sol sin darnos cuenta a la hora de comer y se queman sus componentes internos. O el mismo virus que ha atacado a nuestro ordenador se ha colocado también en la unidad del disco duro y ha dañado los ficheros.

¿Qué pasa con todas las copias de seguridad que hemos hecho? ¡A la basura! A menos que tengas un plan B, un sistema de copias de seguridad en la nube que te permita recuperar tus ficheros perdidos en poco tiempo.

Teniendo estos puntos en cuenta, podremos hacer una estrategia de copias de seguridad que vaya mucho más allá de las prácticas básicas que se utilizan habitualmente. Espero que este artículo te haya sido útil. ¿Has tenido problemas porque se te han borrado los archivos o ficheros de tu ordenador? ¿Estás preocupado por lo que pueda pasar en tu empresa si un día se produce un imprevisto?