

Decálogo de buenas prácticas a la hora de realizar un backup



¿Qué ocurriría si en el día de mañana los discos duros de tus **servidores** u ordenadores se estropearan y perdiera toda la información? Esto te provocaría un gran dolor de cabeza y muchos problemas al perder toda la información almacenada en esos discos. Para evitar esta situación, la mejor opción es realizar copias de seguridad de los datos para que en caso de catástrofe se pueda volver a recuperar esa información.

¿Por qué es necesario un backup?

Los discos donde guardan la información los equipos informáticos suelen ser bastante seguros pero en ocasiones sufren caídas, ralladuras o cortes de luz que ponen en peligro toda la información almacenada.

A veces se puede recuperar la información, pero puede llegar a ser un proceso lento y excesivamente costoso, por lo que muchos usuarios desisten de recuperarla. En estas ocasiones en las que los discos fallan, el simple hecho de tener copiados los archivos en otro sistema externo proporcionará muchísima más seguridad a la hora de conservar los datos, además de ofrecer más tranquilidad al saber que ante cualquier problema que ocurra, podremos restaurar nuestra información de forma rápida y sencilla.

A la hora de realizar un **backup** podemos hacer uso de varios medios distintos, como una memoria USB o un DVD, o bien contratar el servicio externo de una empresa, como el servicio de Backup que ofrecemos en **Hostalia**.

Prácticas a tener en cuenta a la hora de realizar el backup

Identificar los datos críticos para nuestro negocio

En un equipo informático se almacenan inmensas cantidades de información pero no toda es importante. A la hora de planificar una copia de seguridad es importante que tengamos muy claro que información es la más importante, para no gastar tiempo, esfuerzo y espacio en copiar datos que no son relevantes.

Determinar la frecuencia adecuada para nuestros backups

Este es un punto muy importante a la hora de crear una buena política de copias de seguridad. Hay que determinar la periodicidad de los backup, y para decidirlo lo mejor es tener en cuenta cada cuánto tiempo cambia nuestra información. Por ejemplo, si nuestros archivos cambian una vez en semana no tiene sentido hacer copias de seguridad diarias, ya que estaremos almacenando los mismos datos una y otra vez.

Copia continua

Aun teniendo en cuenta lo anterior, lo ideal es que el backup esté permanentemente actualizado, es decir, que en caso de pérdida de la información podamos recuperar todo, incluso lo que haya sucedido sólo unos segundos antes del incidente.

Recuperación de los datos perdidos de forma rápida

Tan importante es asegurarnos de tener replicada la información como restaurarla en un espacio corto de tiempo, por ello las copias deben estar en un sitio cercano a nuestro equipo. Y para no depender de esto, siempre podemos usar un backup online para disponer de la información donde quiera que estemos, asegurándonos que el servicio nos permite restaurar la información rápidamente.

Verificar los backups para garantizar que se pueden restaurar

No hay nada peor que estar haciendo copias de seguridad durante un largo periodo de tiempo y cuando las necesitemos nos demos cuenta de que los datos almacenados no son los correctos. Es aconsejable que cada cierto tiempo nos cercioremos de que los datos que se almacenan en el backup son los correctos, y que se puede acceder a ellos sin ningún tipo de problema.

Recuperación granular desde un backup

Cuando hablamos de una recuperación granular nos estamos refiriendo a poder restaurar un archivo en concreto, no toda la estructura, ya que en la mayoría de las ocasiones sólo necesitaremos restaurar ciertos ficheros.

Externalizar una copia cifrada fuera de la organización

Si la información es de extrema importancia o confidencial, deberías tener un segundo backup en un depósito seguro, en un lugar alejado, a salvo de los robos y el fuego. De esta manera, las posibilidades de perder información se verán reducidos al mínimo. Por ejemplo, el [Centro de Datos de Hostalia](#) cuenta con las máximas medidas de protección y sistemas de alimentación independientes para que los servidores funcionen siempre.

No concentrar la información crítica del negocio en una única persona

Dejar todos nuestros datos en una única persona conlleva que en caso de que a esa persona le suceda algo o abandone la empresa no podamos acceder a los datos. Es importante replicar esta tarea en varios usuarios, para que en caso de que uno falle otro la pueda recuperar en su lugar.

Destrucción de los backups

En ocasiones es importante destruir los datos almacenarlos para que no caigan en manos de terceras personas. Si realizamos copias en dispositivos externos como CD o DVD, a la hora de destruir esos dispositivos es fundamental asegurarnos de que el proceso cumple con la [ley de protección de datos](#), que nos asegure que ningún tipo de información caiga en manos no deseadas.

Las copias de seguridad aportan valor a las empresas

Aunque se piense que el backup sólo sirve para gastar dinero de la empresa, lo cierto es que es uno de los valores más valiosos que puede tener en caso de ocurrir cualquier problema. Por un lado para que no perdamos información de nuestros clientes (como puede ser de facturación), y también para que los clientes tengan siempre disponible los datos y archivos que hayan colocado en nuestra web.

Servicio backup Hostalia

Hostalia utiliza un sistema de backup + snapshot a nivel de bloque en almacenamiento externo clusterizado + snapshot en otro CPD, de esta forma la información estará totalmente segura.

El uso de virtualización para la web y Bases de Datos nos permite hacer un redimensionamiento "en caliente" de los recursos, distribuyendo la carga entre los diferentes nodos, para que ninguno de ellos esté sobrecargado y ralentizado. Además, nos facilita las operaciones de backup a nivel de fichero, lo que nos permitirá recuperar tus datos ante una pérdida accidental.