

## Respaldos de información (*backups*)

Uno de los activos intangibles más importantes para cualquier organización es la información. Es claro que sin esta, toda empresa o institución dejaría de funcionar, pues se trata de un elemento indubitablemente necesario para su operación diaria. Para garantizar que las instituciones puedan disponer de información en el momento que es requerida cuando se presenta una eventualidad, es necesario llevar a cabo un proceso preventivo denominado “respaldo” o “*backup*”.

En general, un respaldo es una copia de la información que una organización genera, utiliza y actualiza a lo largo del tiempo; también este término se emplea para referirse a las copias de seguridad que se llevan a cabo en los sistemas de información, bases de datos, *software* de aplicación, sistemas operativos, utilerías, entre otros. El objetivo de un respaldo es garantizar la recuperación de la información, en caso de que haya sido eliminada, dañada o alterada al presentarse alguna contingencia.

Normalmente, los respaldos se llevan a cabo en unidades de almacenamiento secundario, como discos duros externos, memorias *flash*, discos compactos, cartuchos e incluso en la nube (Internet) o en otros equipos de cómputo, locales o remotos.

Es una buena práctica establecer políticas institucionales relacionadas con la creación de respaldos, pues el tiempo que hay entre la posible pérdida de información y su recuperación puede ser determinante para la supervivencia de una organización. Existen casos documentados de empresas que han desaparecido debido a que, después de un ataque informático, un sismo, una inundación, un incendio o vandalismo, sus equipos de cómputo quedan inservibles y, al

no contar con respaldos o tener respaldos obsoletos, les resulta virtualmente imposible recuperar o actualizar la información generada a lo largo de meses e incluso años.

Es muy importante puntualizar que si bien el área de sistemas es la encargada de realizar respaldos de los sistemas de información y bases de datos de uso común, es el usuario el directamente responsable de llevar a cabo los *backups* de su equipo de cómputo, en particular sobre aquellos documentos o archivos de uso diario y que sufren actualizaciones constantes a lo largo del día. Evidentemente, la información a respaldar será la de interés e importancia para el usuario (archivos de datos, imágenes, fotografías, presentaciones, hojas de cálculo, documentos PDF, etc.); asimismo, para garantizar que esta información se respalde adecuadamente, lo más conveniente será organizarla en carpetas clasificadas por proyectos, tipos de datos, fechas o cualquier otra forma que le resulte al usuario práctica y fácil de identificar. Existe una regla denominada 3-2-1, aplicada sobre todo para aquellos archivos de importancia crítica:

- 1- Mantener una de las copias “fuera de sitio” (*offsite*), es decir, en un lugar físico distinto al lugar de trabajo (casa, taller, bodega, caja fuerte, etc.). Si por desgracia la contingencia es mayor, por ejemplo, un sismo

o un incendio y se daña o se destruye por completo el equipo de cómputo, al menos existirá en algún otro lugar la información respaldada, y podrá ser recuperada.

La frecuencia con la que se realice un respaldo estará determinada fundamentalmente por la frecuencia en los cambios de la información. Por ejemplo, ¿con qué periodicidad se debe respaldar la base de datos de una nómina si esta se actualiza dos veces al mes, en contraste con la base de datos de un sistema de reservaciones de vuelos, cuya actualización es continua? La respuesta es evidente. Aunque el anterior es un ejemplo orientado al área de sistemas, un usuario común debe aplicar el mismo criterio con sus archivos. No hay que suponer que jamás se presentará alguna contingencia. Hacer un respaldo de información es como adquirir un seguro de automóvil; es mejor tenerlo para jamás usarlo, que no tenerlo y requerirlo en el momento menos esperado. |

### DÓNDE ENCONTRAR MÁS INFORMACIÓN:

- [http://www.gfi.cz/whitepapers/The\\_Business\\_Implications\\_of\\_not\\_having\\_a\\_Backup\\_Strategy.pdf](http://www.gfi.cz/whitepapers/The_Business_Implications_of_not_having_a_Backup_Strategy.pdf).
- <http://www.syscorp.net/PDF-Collateral/SeagatePP-Importance%20of%20Backup.pdf>.
- [http://www.brocade.com/downloads/documents/white\\_papers/DataProtection\\_WP\\_00.pdf](http://www.brocade.com/downloads/documents/white_papers/DataProtection_WP_00.pdf).