



Decálogo de buenas prácticas

# Backups



- Un *backup*, o copia de seguridad, se puede definir como el almacenamiento y archivado de la información de modo que se pueda recuperar ante una eventual pérdida de la misma. Las copias de seguridad se encuentran condicionadas a su vez por los periodos de retención, tiempo en el cual se realizará una custodia o conservación, en ocasiones impuestos por normativas y estándares.

## ¿Qué puede pasar?

No utilizar una política de copias de seguridad puede tener múltiples consecuencias de las que no seamos necesariamente conscientes:



**Pérdida de información:** Tanto como usuarios como empresas han de ser conscientes de que el activo mas valioso que poseen es la información con la que trabajan. La perdida de datos de clientes, facturas, proveedores, o información sensible de cualquier tipo, puede ocasionar problemas tanto a nivel legal como a nivel económico dentro de la empresas que no mantienen una política activa de copias de seguridad.



**Sanciones administrativas:** En caso de incumplimiento de los debidos controles de seguridad, que pudieran derivar en la perdida de información relacionada con datos de terceras personas, podría suponer sanciones administrativas por incumplimiento de la Ley Orgánica de Protección de Datos, sanciones que, dependiendo del carácter y sensibilidad de la información perdida, pueden variar entre 900€ y 600.000€.

## ¿Cómo me protejo?

- Implementar una política de *backups* que gestione tanto copias de seguridad incrementales como completas según las necesidades de la empresa o usuario.
- Cifrar los datos que se van a almacenar en las copias de seguridad para aumentar la seguridad de la información a respaldar.
- Evitar tener las copias de seguridad en el mismo lugar donde se realiza la operativa diaria de la información.
- Conocer las consideraciones legales que apliquen a cada negocio con respecto a los periodos de retención de la información.