ESCURA

Telf. +34 902 702 037
escura@escura.com
www.escura.com

Protección de Datos – Circular informativa sobre medidas de seguridad.

Capítulo dos: copias de seguridad.

Las copias de seguridad son tal vez la medida de seguridad más importante para proteger la información.

A la hora de implantar un sistema de copias de seguridad o modificar el sistema que tenemos implantado en nuestra empresa u organización, debemos tener en cuenta varias cuestiones:

1.- Analizar **qué información estamos copiando actualmente**, si es que estamos realizando copias de seguridad y si es realmente esa información la que debemos guardar en nuestra copia de seguridad por poder necesitarla en un futuro o si tal vez, es necesario guardar otra información crítica de la que no estamos haciendo copia. Podemos por tanto descartar toda aquella información que no guarde relación con el negocio o actividad.

2.- Establecer un protocolo escrito o **política de copias de seguridad** que permita definir, entre otras cosas, cuántas versiones se almacenarán, cada cuánto tiempo se realizarán las copias, su período de conservación o el soporte y ubicación de las mismas.

3.- Realizar **pruebas de restauración periódicas** que garanticen que no habrá problemas en caso de tener que recuperar la información. Es decir, hay que comprobar que efectivamente la copia de seguridad funciona, que en la misma se está copiando la información necesaria y que resulta posible utilizar la misma para restaurar la información de nuestros sistemas. Con ello podríamos llegar a comprobar que todo funciona correctamente, pero que el tiempo que necesitemos para la restauración de la copia resulta excesivo, ya que podría darse el caso que no podamos trabajar hasta que finalice la restauración de la copia. Aspectos como éste son importantes, ya que un sistema de restauración excesivamente lento, podría suponer perjuicios económicos para la empresa o entidad.

El tiempo de restauración de la copia de seguridad es por lo tanto un elemento fundamental de una buena política de copias de seguridad. Es necesario prever que sucedería si la persona encargada de realizar dicha función (normalmente el informático de la empresa) no está disponible o está ausente el día que sea necesario realizar la restauración.

Las circulares de **Bufete Escura** tienen carácter meramente informativo, resumen disposiciones que por carácter limitativo propio de todo resumen pueden requerir de una mayor información. La presente circular no constituye asesoramiento legal.

©La presente información es propiedad de **Bufete Escura** quedando prohibida su reproducción sin permiso expreso.

4.- Debemos determinar la **periodicidad de la copia de seguridad** para garantizar la seguridad de nuestros sistemas de información. Como mínimo se recomienda hacer una copia diaria, siendo incluso necesario utilizar sistemas de copia de seguridad en tiempo real, en función de los datos que tratemos y las consecuencias de su pérdida.

5.- Igualmente, debemos determinar dónde vamos a guardar la copia de seguridad o su **lugar de almacenamiento**, cobrando cada día más fuerza los sistemas de copia de seguridad en la nube, basados en salvaguardar nuestras copias de seguridad en servidores de terceros. Este sistema cuenta con múltiples ventajas, principalmente la de tener una copia de seguridad fuera de la empresa y por lo tanto a salvo de riesgos físicos como incendios o inundaciones.

6.- Otro factor a tener en cuenta, es el **cifrado de la copias de seguridad**. Es decir, que éstas se conserven cifradas mientras están almacenadas, de forma tal que ante un acceso no autorizado a la copia, la información no sea accesible para un tercero que no disponga de la clave de cifrado.

7.- También es importante destacar la importancia de realizar una correcta gestión del **deshecho de las copias de seguridad**. Si por cualquier motivo queremos desechar un soporte que contenga copias de seguridad (por ejemplo por obsolescencia del soporte, avería, etc), será necesario borrar la información del soporte mediante su formateado y proceder a la destrucción física del mismo.

El Reglamento General de Protección de Datos (UE) 679/2016 y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, han establecido el **principio de responsabilidad proactiva**, es decir que las empresas tienen libertad para determinar qué medidas de seguridad adoptan para proteger sus datos, pero al mismo tiempo, deben ser responsables, ya que estas medidas deberán ser suficientes para garantizar la protección de los datos de carácter personal.

Anteriormente, la antigua Ley Orgánica 15 /1999 y el RD 1720/2007 establecían que se debían realizar copias de seguridad como mínimo una vez a la semana y que si tratábamos datos de nivel de seguridad medio o alto, una copia de seguridad se debía guardar en un lugar separado del resto de la información de la empresa. Dichos requisitos han quedado desfasados, una copia de seguridad semanal es a todas luces una medida insuficiente en la actualidad, en cambio muchas empresas no realizan todavía una copia de seguridad fuera de sus instalaciones, en un lugar separado de sus sistemas de información.

En conclusión, las copias de seguridad, como medida de seguridad para la protección de los sistemas de información de las empresas, es tal vez la medida de seguridad más importante y que por lo tanto, requiere de una especial atención por parte de las mismas.

Las circulares de **Bufete Escura** tienen carácter meramente informativo, resumen disposiciones que por carácter limitativo propio de todo resumen pueden requerir de una mayor información. La presente circular no constituye asesoramiento legal.

©La presente información es propiedad de **Bufete Escura** quedando prohibida su reproducción sin permiso expreso.