Sugerencia 04/2018

COPIAS DE SEGURIDAD

Las copias de seguridad (*respaldos*) de los datos de carácter personal son fundamentales para garantizar la integridad, disponibilidad y resiliencia que el RGPD establece para los mismos. Os emplazamos a incorporar esta práctica en los Colegios para garantizar el cumplimiento del del marco legal.

¿Qué es una copia de seguridad?

Es una copia de datos originales fuera del espacio físico/virtual/infraestructura que los contiene con el fin de disponer de la recuperación de dichos datos ante:

- Pérdida de datos por accidente informático (virus, corrupción del sistema de ficheros, borrado fortuito, etc.).
- Transferencia de datos a otra ubicación.
- Cualquier imprevisto que conlleve riesgo en los datos almacenados (robo, pérdida, destrucción del soporte, etc.).

El objetivo es que, respaldando estos datos, podamos resolver cualquier eventualidad de forma rápida y eficaz.

Tipos de copia de seguridad

Existen varios tipos de copias de seguridad, dependiendo del alcance.

- Completa
- Incremental
- Diferencial

En cada caso es preciso valorar cuál se adapta más a nuestras necesidades pero es conveniente tener al menos una copia completa y adicionalmente otras incrementales o diferenciales, la redundancia, en este caso, es siempre aconsejable. También es importante valorar adecuadamente la frecuencia de ejecución de las copias.

¿Cómo se realiza una copia de seguridad?

Bien sea por procedimientos manuales o automatizados, es básico escoger el soporte que alojará la copia que, en la medida de lo posible, deberá estar situado en dependencias distintas a las que contienen los datos originales. Atendiendo al soporte y centrándonos únicamente en los datos de carácter digital, podemos distinguir los siguientes escenarios posibles:

- Sobre un elemento de almacenamiento externo local: cinta digital, NAS, disco duro externo, pen drive, fotocopia.
- Servidor propio en otra localización.
- Servicio de terceros de almacenamiento en nube.

Estos soportes deberán contar con medidas asociadas que garanticen su seguridad (cifrado en caso de datos digitales, acceso restringido en otros casos) y establecer un control en cuanto a quién la realiza y tiene acceso a las mismas.

Es necesario realizar las copias de forma cíclica y recurrente para tener siempre actualizados los datos. Igualmente es preciso garantizar que la copia de seguridad es correcta y que podemos recuperar los datos originales sin problema.

Una manera de simplificar y centralizar aquellos datos sensibles que queremos preservar posteriormente en respaldos es por medio de un *NAS*, una unidad digital especializada que aloja y disponibiliza en red aquellos datos que precisamos y puede implementar mecanismos de backup adicional como el *mirrorizado* por medio de sistemas *RAID*.

No consideramos aconsejable emplear servicios corporativos de tipo "*cloud computing*" como *Google Drive*, *Dropbox* y similares para realizar sobre ellos copias de seguridad, dadas las complicaciones legales derivadas en cuanto a cesión a terceros, la necesidad de implementar medidas de protección adicionales y especialmente el poco respeto que estas corporaciones demuestran tener por la protección de los derechos de sus usuarios en lo referente al tratamiento de sus datos personales.

LA SEGURIDAD DE LOS DATOS EN EL RGDP

La necesidad de establecer una política de gestión de copias de seguridad viene derivada de los siguientes artículos del Reglamento General de Protección de Datos:

ART. 5

1. Los datos personales serán:

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

ART. 32

Seguridad del tratamiento.

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) La seudonimización y el cifrado de datos personales.

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Los responsables y encargados establecerán las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado atendiendo a los riesgos detectados en el análisis previo.

En este sentido es preciso tener en cuenta que el **Delegado de Protección de Datos** será quien analice y diseñe la protección de datos del Colegio estando entre sus competencias:

- Redactar el procedimiento de realización de copias de seguridad.
- Autorizar la contratación de un tercero, en caso de querer externalizar el servicio.
- Diseñar pruebas de recuperación con datos reales.

Esperamos haber clarificado mínimamente este particular. Como siempre quedamos a vuestra disposición para cualquier duda o cuestión.

Links:

- https://protecciondatos-lopd.com/empresas/copias-seguridad/
- https://searchdatacenter.techtarget.com/es/cronica/Copia-de-seguridad-completa-incremental-o-diferencial-como-elegir-el-tipo-adecuado
- https://marcosmarti.org/crear-servidor-nas-casero/
- https://dpd.aec.es/blog/page/2/
- https://www.welivesecurity.com/la-es/2017/07/10/google-drive-informacion-corporativa/