DECÁLOGO DE RECOMENDACIONES

EN EL ÁMBITO DEL RGPD Y LA CIBERSEGURIDAD

01

Antes de iniciar cualquier tratamiento de datos, verifica si es necesario realizar una **EVALUACIÓN DE IMPACTO.** Debes evaluar si puede afectar a derechos y libertades de los interesados.

02

Realiza un **ANÁLISIS DE LOS RIESGOS** sobre el tratamiento de datos que vayas a poner en marcha para determinar qué medidas de seguridad debes aplicar.

03

Establece **POLÍTICAS INTERNAS DE SEGURIDAD** sobre el tratamiento de datos que vayas a poner en marcha para determinar qué medidas de seguridad debes aplicar.

04

Mantén **LIMPIOS Y ACTUALIZADOS** tus dispositivos. Revisa periódicamente ordenadores de sobremesa, portátiles, teléfonos corporativos, tablets, ...

05

CONTROLA LOS ACCESOS de los usuarios a tu sistema de información. Utiliza escritorios remotos cuando sea posible, controla los usuarios autorizados y limita el uso de WIFI públicas.

06

CONFIGURA EL ACCESO A INTERNET Impide el acceso a páginas con contenidos peligrosos.

07

INSTALA SOFTWARE DE SEGURIDAD en tus sistemas que proteja tus ordenadores de virus y malware.

08

Establece sistemas efectivos de comunicación, estudio y resolución de **INCIDENCIAS y BRECHAS DE SEGURIDAD.** Estos sistemas te permitirán minimizar el impacto y evitarán que se puedan volver a dar situaciones de vulnerabilidad.

09

Utiliza sistemas de **SEUDONIMIZACIÓN Y CIFRADO** de datos para mitigar los riesgos y proteger la información de amenazas y accesos no autorizados.

10

FORMA Y CONCIENCIA A LOS USUARIOS de la importancia de trabajar respetando las políticas de seguridad para garantizar la confidencialidad de la información.

Edición julio 2018

Ametic