



DECÁLOGO DE PROTECCIÓN DE DATOS PARA EMPLEADOS PÚBLICOS

1. Consulta con la DELEGADA DE PROTECCIÓN DE DATOS siempre antes de la implantación de un procedimiento o proyecto en el que se traten datos personales y siempre que tengas cualquier duda sobre el tratamiento de datos personales.
2. Si tienes que acceder a datos de carácter personal..., piénsalo, sólo debes acceder si es necesario para los fines de tu trabajo.
No informes sobre datos personales de terceros, salvo que sea necesario para desarrollar tu trabajo y tengas una justificación.
3. Si necesitas un acceso urgente y tienes cualquier contratiempo, contacta con el CAU o tu Servicio de Informática.
4. Si tienes que compartir información con datos personales por correo electrónico o por cualquier otro medio, consulta con el Servicio de Informática sobre el modo de hacerlo para garantizar la máxima confidencialidad.
5. No realices por tu propia cuenta copias, en memorias USB u otro tipo de dispositivos, de documentos con datos personales.
No envíes documentación administrativa a tu correo personal ni la subas a tu nube.
6. No dejes los expedientes o documentos a la vista sin supervisión. Retira inmediatamente los documentos que envíes a la fotocopidora/impresora, sobre todo si está en espacios comunes sin supervisión.
7. Cuando salgas del despacho, asegúrate de bloquear o cerrar la sesión abierta en tu ordenador. No facilites a nadie tu clave de acceso y contraseña.
8. No tires documentos con datos personales a la papelera; utiliza los contenedores especiales precintados de color azul dispuestos para tal fin en las dependencias de la Consejería.
9. Cuando termines tu jornada de trabajo, deja cerrados con llave los armarios o archivadores que contengan información con datos personales.
10. Si así se te ha indicado, cierra con llave la puerta de tu despacho.

Para cualquier duda puedes consultar con la Delegada de Protección de Datos:
dpd.sanidad@jcy.l.es