

FIRMA
FIRMADO por : VALDECABRES ORTIZ, MARIA ISABEL. A fecha: 24/02/2023 12:50 PM
FIRMADO por : MORENO GARCIA-CANO, JAIME ALBERTO. DIRECTOR GENERAL DE TRANSPORTE TERRESTRE. A fecha: 27/02/2023 09:25 AM
Total folios: 10 (7 de 10) - Código Seguro de Verificación: MIFOM7ZSF7BEAD905B95982650
Verificable en <https://sede.mtma.gob.es>



- Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día, y serán custodiados cuando, con motivo de su tramitación, se encuentren fuera de los dispositivos o salas de archivo.
- No se desecharán documentos (papel) o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción, de forma que la información no sea recuperable.
- No se comunicarán datos personales o cualquier información personal a terceros, se prestará atención especial en no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.
- El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral o de prestación de servicios.
- Deberá contar con un procedimiento de gestión de las Violaciones de seguridad de datos de carácter personal.

Medidas de seguridad técnicas, relativas a la identificación. EL ENCARGADO implantará como mínimo las siguientes medidas técnicas para garantizar la identificación y autenticación de los usuarios con acceso a los datos:

- No se permitirá el uso para fines particulares de aquellos ordenadores y dispositivos destinados al tratamiento de los datos personales.
- Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador o dispositivo.
- Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
- Se garantizará la existencia de contraseñas (o mecanismos equivalentes) para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras, y se renovarán periódicamente (al menos de forma anual).
- Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).