

## **Buenas prácticas para el uso de datos personales en el ámbito del MEFPD**

### **- NO UTILICES LOS DATOS PARA FINALIDADES NO AUTORIZADAS**

- Los datos personales que la persona interesada proporciona al Ministerio deben ser tratados para la finalidad para la que fueron solicitados o recabados.
- Se debe guardar la debida confidencialidad. Solo deben tener conocimiento de los datos quienes los necesitan para el desempeño de sus funciones.

### **- PRINCIPIO DE MINIMIZACIÓN**

- De acuerdo con el principio de minimización, los datos recogidos serán los mínimos necesarios para el procedimiento, trámite o servicio.
- Solo serán objeto de tratamiento, los datos personales necesarios para cada uno de los fines específicos del procedimiento, trámite o servicio. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.
- Los datos personales que se recaben deberán ser adecuados, pertinentes y limitados a lo necesario para los fines que son tratados.

### **- INFORMACIÓN A LAS PERSONAS TITULARES DE LOS DATOS**

- Se debe informar a las personas titulares del tratamiento qué se va a realizar con sus datos personales, “Deber de Informar”.
- Además, se les debe facilitar el acceso a la solicitud para el ejercicio de sus derechos.

### **- HERRAMIENTAS**

- Cuando manejes datos personales en tu trabajo utiliza siempre las herramientas institucionales proporcionadas por el Ministerio, tales como el correo corporativo, carpetas de red, nube institucional, etc.
- Si utilizamos otras herramientas estamos comprometiendo los datos personales de las personas interesadas sin su autorización.

### **- POLÍTICA DE MESAS LIMPIAS**

- No dejes datos a la vista: mesas limpias, archivadores cerrados, cuando dejes tu puesto de trabajo, apaga o bloquea tu ordenador, cerrando las aplicaciones en uso.
- No saques datos fuera del Ministerio y en caso de que sea imprescindible el contenido deberá estar cifrado. En caso de dudas consulta con la Unidad de Informática .
- Evita el uso de papel siempre que sea posible.

### **- INCIDENCIAS DE SEGURIDAD EN EL TRATAMIENTO DE DATOS**

- Si tienes conocimiento de procedimientos o conductas que pueden poner en riesgo la privacidad y la confidencialidad de los datos personales, debes ponerlo en conocimiento de la Delegación de Protección de Datos para activar los mecanismos necesarios que mitiguen las posibles consecuencias sobre los derechos de las personas afectadas.
- Cualquier incidente de seguridad que se produzca se debe informar, lo antes posible, a la persona responsable del tratamiento y a Delegación de Protección de Datos

- **USO DE CONTRASEÑAS SEGURAS.**
- **APLICA LA SEGURIDAD EN DISPOSITIVOS MÓVILES.**
- **Y EN CASO DE DUDAS...**
  - Contacta con nuestro equipo [dpd@educacion.gob.es](mailto:dpd@educacion.gob.es)
  - Visita nuestra sección <https://intranet.educacion.gob.es/mis-servicios-electronicos/protecciondatos-caracter-personal.html>
  - La Subdirección de Atención al Ciudadano, Documentación y Publicaciones ejerce las competencias relativas al delegado de protección de datos (DPD) previstas en el Reglamento (UE) 2016/679 y la coordinación y supervisión de la política de protección de datos de carácter personal del Departamento.