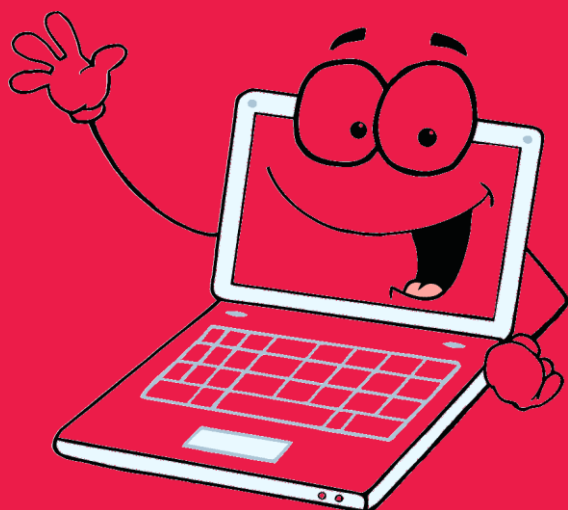


# Guía de Uso Responsable de Dispositivos Digitales



**IES MAESTRO JUAN DE ÁVILA**

C/Ronda de Calatrava 1 13003 CIUDAD REAL

Tfno. 926221207

<http://www.maestrojuandeavila.es/>



Esta guía está diseñada para promover el uso adecuado y responsable de los equipos y recursos informáticos del centro, garantizando su preservación y aprovechamiento por parte de toda la comunidad educativa. Su uso es clave para el aprendizaje y la formación de toda la comunidad educativa. Sin embargo, para garantizar un uso efectivo, ético y sostenible, es fundamental establecer líneas claras y adaptadas a cada grupo: profesorado, alumnado y familias.

## 1. Principios generales.

- Todo usuario debe ser consciente de que los equipos son bienes compartidos y deben cuidarse como si fueran propios.
- Usar los recursos informáticos respetando las normas del centro y los derechos de los demás.
- Hacer uso de los recursos informáticos únicamente para fines educativos y laborales, evitando actividades no autorizadas.
- Respetar la privacidad y proteger los datos personales al utilizar los recursos.

## 2. Alumnado.

### 2.1. Normas de uso.

- Tratar los ordenadores, las pantallas digitales y otros recursos como si fueran propios, evitando daños o mal uso.
- Comprobar siempre el estado del dispositivo al cogerlo e informar de cualquier defecto o problema inmediatamente.
- En el caso de utilizar los equipos almacenados en los carros, siempre colocar cada ordenador en su sitio correspondiente y después conectar el cargador (si se hace al contrario se puede romper la clavija del cargador).
- Apagar el equipo correctamente después de su uso.
- No modificar los ajustes del sistema sin autorización.
- No instalar programas sin la debida autorización.
- No acceder a sitios web, juegos o aplicaciones que no estén autorizados por el profesorado.
- Para almacenar la información, usar memorias USB o bien el almacenamiento corporativo personal para usos académicos cedido por la plataforma EducamosCLM.

### 2.2. Ciberseguridad.

- Usar contraseñas seguras con combinaciones de letras (mayúsculas y minúsculas), números y símbolos. No usar la misma contraseña en distintos sitios web. No compartir las contraseñas con nadie.

- Mantener en privado los datos de acceso a plataformas educativas o sitios web que necesiten registro. Al finalizar el uso del dispositivo, siempre cerrar la sesión de los sitios web en los que se esté trabajando.
- Navegar por sitios seguros, utilizando únicamente sitios web recomendados por los profesores. Verificar que los sitios tengan una conexión segura (<https://>)
- Descargar solo documentos y aplicaciones necesarias, siempre de fuentes oficiales. Consultar con un profesor si tienes dudas de un archivo.
- No abrir correos electrónicos de remitentes desconocidos y sobre todo hay que tener mucho cuidado con enlaces o archivos adjuntos inesperados. También con los SMS sospechosos en los smartphones.
- No tomar ni compartir fotos, videos o datos de tus compañeros o profesores sin permiso.
- No copiar trabajos y respetar los derechos de autor, fomentando la creación de contenido propio.

### 2.3. Consecuencias de un mal uso.

- Pérdida temporal del acceso a los recursos informáticos.
- Reparación o reposición de equipos en caso de daños causados por negligencia.
- Sanciones según el Reglamento de Régimen Interno del centro.

## 3. Profesorado.

### 3.1. Recomendaciones en el aula.

- Al inicio de cada clase, elaborar un listado con los alumnos de clase y los equipos que utilizan.
- Comprobar al inicio y al finalizar la clase el estado físico de los dispositivos y que estos quedan ordenados en los carros y en las aulas de informática.
- Asegurarse de que el alumnado utilice los recursos de manera adecuada durante la clase.
- En las aulas de informática, al finalizar el día asegurarse de bajar los automáticos de control de carga de los ordenadores.
- En los carros, al dejarlos asegurarse de que quedan correctamente conectados al cable de carga.
- Integrar actividades digitales que promuevan aprendizaje crítico y creativo.
- Informar sobre desperfectos o incidencias que puedan ocurrir en clase.

### 3.2. Buenas prácticas.

- Utilizar los equipos únicamente para fines educativos y administrativos, evitando su uso para actividad

- Proteger la privacidad de los datos del alumnado, cumpliendo con las normativas vigentes de protección de datos. En comunicaciones con familias y alumnos usar solo los canales proporcionados por la plataforma EducamosCLM.
- Cuidar los equipos prestados, manteniéndolos limpios, evitando exponerlos a temperaturas extremas o humedad y **transportándolos con funda protectora** para evitar golpes.
- Enseñar con el ejemplo prácticas como el uso correcto del correo electrónico, la navegación segura y la creación de contraseñas seguras.
- Participar en actividades de formación relacionadas con la transformación digital educativa para optimizar el uso de herramientas digitales en el aula.

### 3.3 Ciberseguridad.

- Usar contraseñas seguras con combinaciones de letras (mayúsculas y minúsculas), números y símbolos. No usar las mismas contraseñas en distintas plataformas y cambiarlas periódicamente.
- Mantener actualizados el sistema operativo y el antivirus, para protegerse frente a vulnerabilidades.
- No abrir correos electrónicos ni enlaces de remitentes desconocidos. Hay que tener mucho cuidado con intentos de phishing que imiten a la dirección del centro o entidades educativas.
- Navegar únicamente por sitios confiables y relacionados con actividades educativas.
- Bloquear el ordenador cuando se deje, incluso por períodos cortos. No dejar sin supervisión en lugares accesibles por terceros.
- Evitar utilizar programas no autorizados que puedan comprometer la seguridad del sistema.
- Realizar copias de seguridad regularmente de la información guardada en el sistema.
- Informar sobre cualquier sospecha de brecha de seguridad, malware o acceso no autorizado.