



LIBRE

Estrategia de
Digitalización Educativa
de la Región de Murcia

Recomendaciones para centros educativos

PRIVACIDAD Y SEGURIDAD DE DATOS PERSONALES



Contenido

1. Introducción	1
2. Principios clave de protección de datos.....	2
3. Uso de aplicaciones educativas y almacenamiento en la nube.....	9
4. Buenas prácticas en el uso de medios electrónicos.....	14
5. Conclusión.....	19
6. Anexos.....	20

1. INTRODUCCIÓN

Los centros educativos gestionan diariamente una gran cantidad de información personal de alumnado, familias, docentes y personal no docente. Esta información, en muchos casos sensible como datos de salud, imágenes, información familiar o académica, requiere una especial atención en su tratamiento para garantizar los derechos fundamentales de las personas, especialmente, de los menores.

Con la progresiva digitalización de los procesos educativos, uso de plataformas digitales, apps educativas, almacenamiento en la nube y dispositivos electrónicos, aumenta también la exposición a riesgos relacionados con la seguridad de la información y el cumplimiento de la normativa sobre protección de datos.

Por este motivo, la Administración educativa de la Región de Murcia promueve estas recomendaciones para apoyar a la comunidad educativa en la aplicación efectiva de las obligaciones establecidas por:

-  El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, por el que se deroga la Directiva 95/46/CE (Reglamento General de protección de Datos (RGPD)).
-  Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
-  Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
-  Decreto 79/2025, de 5 de junio, por el que se establece la política de seguridad de la información en la Administración Regional.
-  Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
-  Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
-  El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
-  Orden de 30 de enero de 2017, de la Consejería de Hacienda y Administración Pública por la que se aprueba el manual de uso de medios electrónicos para el personal de la Administración Pública Regional.
-  Las orientaciones de la Agencia Española de Protección de Datos (AEPD).



2. PRINCIPIOS CLAVE DE PROTECCIÓN DE DATOS

A. LO QUE DEBEN HACER LOS CENTROS.

Los centros educativos tienen la obligación legal y ética de garantizar el cumplimiento de los principios establecidos en el Reglamento General de Protección de Datos (RGPD), la LOPDGDD y las instrucciones de la Administración regional. En concreto, deben:

1. Garantizar una base legal para el tratamiento de datos

El tratamiento de datos personales por parte de los centros no requiere consentimiento si está amparado en una base jurídica como el ejercicio de la función educativa u otras obligaciones legales (por ejemplo, la matrícula, la gestión de becas o la evaluación). Para fines no directamente relacionados con la educación (como difusión en redes sociales), sí es necesario consentimiento informado de los titulares o de sus representantes legales si se trata de menores de 14 años, y de los propios alumnos si tienen 14 años o más. En este sentido, la Consejería de Educación y Formación Profesional ofrece un modelo a los centros

Región de Murcia
Consejería de Educación y Cultura
Dirección General de Centros Educativos e Infraestructuras

CONSENTIMIENTO INFORMADO TRATAMIENTO DE IMAGEN/VOZ DEL ALUMNADO EN CENTROS DOCENTES PÚBLICOS NO UNIVERSITARIOS DE LA COMUNIDAD AUTÓNOMA DE LA REGIÓN DE MURCIA. CENTRO:

La rápida evolución tecnológica, así como la proliferación de plataformas de difusión de la actividad de los centros implica el tratamiento de datos de carácter personal de alumnos con finalidades distintas a la actividad educativa, por lo que es necesario contar con el consentimiento de padres y/o tutores de alumnos menores de 14 años o de los propios alumnos, si estos tienen 14 o más años, para el tratamiento de estos datos.

La finalidad de este documento es:

- Informar a los padres/tutores de los alumnos menores de 14 años y a los alumnos mayores de 14 años del centro, del tratamiento que este realizará de la imagen/voz de los alumnos.
- Recabar el consentimiento de padres, tutores o alumnos como base jurídica que permita al centro el tratamiento de la imagen/voz de los alumnos.

Con carácter previo a la firma del presente documento usted deberá leer la información relativa a la protección de datos de carácter personal sobre el tratamiento de imagen/voz de los alumnos en centros docentes públicos no universitarios, que se detalla al dorso del presente documento.

Si el Alumno es menor de 14 años: ☐ con DNI ☐ con DNI y DGP

Si el Alumno es de 14 o más años: Este alumno/a ☐ con DNI ☐ con DNI y DGP

En su caso, el alumno/a ☐ CONSENTIR ☐ NO CONSENTIR

Al Centro, ☐ el tratamiento de la imagen/voz de su hijo/a, o de su hijo/a menor de 14 años o más, especialmente mediante fotografías o vídeos, con la finalidad de difundir las actividades del centro, en los siguientes medios:

(Solo se entenderá que consiente la difusión de imagen/voz por los medios expresamente marcados o continuados):

☐ Página Web del centro ☐ Instagram ☐ YouTube ☐ Intranet institucional CARM

☐ Montajes multimedia (CD o DVD con fotos, películas, etc.) ☐ Facebook ☐ Twitter

En _____ a _____ de 20__

Fdo. _____ Fdo. _____ Fdo. _____

Padre/madre/tutor/a del alumno/a (Nombre, apellidos y firma) Padre/madre/tutor/a del alumno/a (Nombre, apellidos y firma) Alumno/a de 14 años o más años (Nombre, apellidos y firma)

Región de Murcia
Consejería de Educación y Cultura
Dirección General de Centros Educativos e Infraestructuras

INFORMACIÓN ADICIONAL SOBRE PROTECCIÓN DE DATOS EN TRATAMIENTO DE IMAGEN/VOZ DEL ALUMNADO EN CENTROS DOCENTES PÚBLICOS NO UNIVERSITARIOS DE LA COMUNIDAD AUTÓNOMA DE LA REGIÓN DE MURCIA

RGPD-REGULAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016
LEY ORGÁNICA 3/2018, de 5 de diciembre, de PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

Epígrafe	Información adicional
Responsable del tratamiento	Dirección General de Centros Educativos e Infraestructuras Consejería de Educación y Cultura de la CARM Dr. Postal: Avda. Fama, 15. 30006 Murcia. Edificio Administrativo Educación, 7ª planta. Teléfono 968 279 628
Finalidad del tratamiento	Designación de Protección de Datos: Correo electrónico: proteccion@educacion.murcia.es Quedan los datos relativos a imagen/voz de los alumnos, con la finalidad de difundir y promover las actividades culturales, recreativas, deportivas y sociales en los que participe el centro a través de los medios de difusión que se detallan en el documento que figura en el anexo de este informe por el que se otorga o deniega el consentimiento para este tratamiento. La imagen/voz almacenada será conservada durante el tiempo necesario en el que sean tratados.
Legitimación del tratamiento	Artículo 6.1 a) del RGPD Consentimiento de los padres o tutores para aquellos alumnos menores de 14 años, o de los propios alumnos, cuando tengan 14 o más años. El consentimiento se otorgará y otorgará en su caso otorgará para cada uno de los medios de difusión citados, siendo posible que se autorice el tratamiento de la imagen/voz en uno o varios medios de difusión y en otros no. Si se toma una imagen/voz a través de fotografía, vídeo o cualquier otro medio de captación, de alumnos que no han consentido el tratamiento, se procederá a destruir sus rasgos identificativos, especialmente cuando en una fotografía concurren con otros compañeros que sí cuentan con la autorización para el tratamiento de su imagen/voz.
Destinatarios de cesiones transferencias internacionales	No se cederán datos a terceros. La difusión de datos de imagen/voz en redes sociales supondrá una comunicación de datos a terceros, atendiendo a la naturaleza y funcionamiento de estos servicios. No están previstas transferencias internacionales de datos.
Derechos de las personas interesadas	El titular o sus padres o tutores legales puede ejercitar, si lo desea, los derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad de los datos, dirigiendo una solicitud al responsable del tratamiento por vía electrónica, a través de la sede electrónica de la CARM, o presencialmente a través de la red de oficinas de asistencia en materia de registro. Puede ejercer sus derechos aquí . Tiene derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la legalidad del tratamiento basado en el consentimiento previo a su retirada. Pueden ejercer estos derechos ante el responsable del tratamiento o ante el Delegado de protección de datos. Además, en caso de discrepancia con el tratamiento de los datos personales, podrán interponer una reclamación ante la Agencia Española de Protección de Datos mediante escrito (C/ Jorge Juan, 6, 28001 Madrid) o telemáticamente en su Sede electrónica.

2. Informar de forma clara y transparente

Existe el deber de informar a las personas interesadas (alumnado, familias, personal no docente) sobre:

- La finalidad del tratamiento.
- La legitimación legal.
- Los destinatarios de los datos.
- Los derechos que pueden ejercer y cómo hacerlo.
- La identidad del responsable del tratamiento y del Delegado de Protección de Datos para los Centros Docentes

Esta información debe facilitarse de manera accesible, clara y adaptada al público destinatario con un lenguaje sencillo.

3. Aplicar medidas de seguridad adecuadas

Los datos deben ser tratados de forma que se garantice una seguridad adecuada, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

En la práctica esto supone, entre otras medidas, usar contraseñas seguras y autenticación en dos pasos en las plataformas educativas.

Un ejemplo sería la manera de acceder de los docentes al expediente digital del alumnado; estos deben hacerlo, únicamente, a través de conexiones seguras y mediante cuentas institucionales (Educarm, portal de aplicaciones de la Consejería de Educación y Formación Profesional, entorno colaborativo @murciaeduca.es). En el caso de que existan físicamente expedientes en papel, habría que protegerlos mediante archivadores cerrados y un acceso restringido



4. Buscar asesoramiento en el Delegado de Protección de Datos para los Centros Docentes

En la Región de Murcia, los centros educativos públicos no designan un DPD-CD individual para cada centro. En su lugar, la Consejería de Educación y Formación Profesional actúa como responsable del tratamiento de datos personales y ha designado un DPD único a nivel regional (dpd.centros@murciaeduca.es) que supervisa el cumplimiento de la normativa en todos los centros públicos de la región.

Este DPD-CD es el encargado de asesorar a los centros sobre sus obligaciones en materia de protección de datos, supervisar el cumplimiento de la normativa aplicable y actuar como punto de contacto entre los centros y la Agencia Española de Protección de Datos (AEPD).

Para los centros concertados y privados, la obligación de designar un DPD-CD viene establecida en el artículo 34 de la Ley Orgánica 3/2018 (LOPDGDD)".

5. Regular las relaciones con terceros



Cuando un centro contrata a una empresa o entidad externa, las empresas que prestan estos servicios actúan como encargadas del tratamiento de datos personales por cuenta del centro o de la Administración educativa. Por tanto, se debe formalizar un contrato de encargo del tratamiento con la empresa que preste el servicio. Este contrato debe recoger: finalidad, duración, medidas de seguridad, prohibición de usar los datos para otros fines y obligación de devolución o destrucción al finalizar el servicio.

6. Formar e informar al personal del centro

Todo el personal que maneja datos personales, docente y no docente, debe recibir formación básica en protección de datos. Se debe reforzar el conocimiento del deber de secreto (artículos 52, 53 y 54 del Real Decreto Legislativo 5/2015, de 30 de octubre TREBEP ) , el uso adecuado de plataformas digitales y la prevención de riesgos relacionados con el uso de dispositivos electrónicos, así como conocer la Orden de 30/01/2017, por la que se aprueba el manual de uso de medios electrónicos para el personal de la Administración Pública Regional.

7. Aplicar políticas claras sobre uso de las tecnologías digitales

Para las apps educativas, plataformas y servicios digitales que no traten datos personales o sensibles, será el propio centro el que, atendiendo a sus condiciones específicas, podrá seleccionar la que mejor se adapte a sus fines pedagógicos. No obstante, cuando hay necesidad de contratar alguna aplicación que requiera la comunicación de datos de carácter personal, de docentes y/o alumnado, a una tercera empresa, con objeto de cumplir con la normativa de protección de datos, previo a su uso deben seguir el procedimiento establecido por la Consejería de Educación. Dicho procedimiento será supervisado y autorizado por el Delegado de Protección de Datos para los Centros Docentes.

8. Establecer mecanismos para la supresión de los datos

Los datos deben conservarse solo el tiempo necesario para la finalidad para la que fueron recogidos. Tras ese periodo deben ser eliminados o bloqueados, permitiendo el acceso solo en caso de responsabilidad legal o reclamaciones, antes de su destrucción definitiva.

Existen unas instrucciones  específicas relativas a la gestión documental y organización de archivos de centros docentes públicos no universitarios de la Comunidad Autónoma de la Región de Murcia, con especial consideración a la eliminación de documentos.



¿Por qué se necesita un protocolo de PROTECCIÓN DE DATOS?



Orden
08/09/2025 de
estrategia
digital LIBRE 

En el artículo 11 de la Orden de estrategia digital LIBRE, se establece la necesidad de implantar un protocolo para fomentar el uso responsable y ético en cuanto a la privacidad y la protección de datos en la comunidad educativa.

Al tiempo que se protege la privacidad y seguridad de los datos personales, se garantiza la implementación efectiva, equitativa y sostenible en la estrategia digital del centro. Para cumplir con estas premisas, la guía recoge un protocolo para la protección de datos y la seguridad a modo de ejemplo en el anexo II.

IMPORTANT!

Para ampliar información, consultar la guía para centros educativos de la AEPD



B. LO QUE DEBEN EVITAR LOS CENTROS

Además de lo que deben hacer, los centros educativos deben evitar conductas que puedan poner en riesgo la privacidad, la legalidad del tratamiento o la seguridad de la información, tales como:

1. Recoger datos innecesarios o excesivos

Se recabarán únicamente los datos estrictamente necesarios para cumplir con las funciones educativas y administrativas, evitando recoger información excesiva o no pertinente. Por ejemplo, para autorizar una salida escolar se podrá solicitar nombre, alergias o contacto familiar, pero no se pedirán datos innecesarios como el DNI del alumnado o la situación laboral de los padres o tutores. Tampoco se tienen por qué solicitar datos bancarios antes de que un alumno o alumna haya sido admitido/a o recabar datos sobre creencias religiosas sin que estén directamente relacionados con la actividad educativa.

2. Publicar información personal sin autorización

No se deben publicar nombres, imágenes, voz o cualquier otro dato de carácter personal del alumnado en la web del centro o redes sociales sin base legal o consentimiento informado. Tal y como se ha comentado anteriormente en la página 2, habría que utilizar un documento específico de consentimiento.



3. Utilizar apps o servicios no evaluados ni autorizados

Con carácter general, cualquier app o herramienta, ya sea para el profesorado, el personal de administración o el propio alumnado, debe cumplir unos mínimos de transparencia y seguridad. Por eso, se deberán evitar aquellas aplicaciones o servicios que :

-  No especifiquen quién es el responsable del tratamiento: quién decide para qué y por qué se recogen los datos.
-  No indiquen dónde se almacenan los datos: país, proveedor de infraestructura, etc.
-  No aseguren unas medidas de seguridad y una política de retención adecuadas, por ejemplo, cifrado de la información, procedimientos de borrado, conservación solo mientras sea necesario, etc.



Esta recomendación cobra especial importancia cuando hablamos de apps que van a procesar datos de estudiantes como son calificaciones, información personal, comunicaciones profesor-alumno/a, etc. Esas tres condiciones dejan de ser “buenas prácticas” para pasar a ser requisitos imprescindibles. Si una herramienta no cumple cualquiera de esos puntos, no debe emplearse con el alumnado porque hay un riesgo elevado de incumplir la normativa de protección de datos, especialmente, por tratarse de menores de edad.

4. Almacenar datos personales en dispositivos personales no autorizados

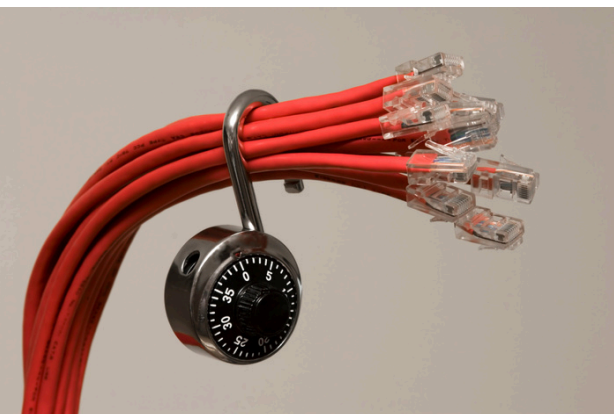
No se debe guardar información sensible como listas de clase, notas o informes en cuentas personales o dispositivos privados que no estén protegidos adecuadamente y autorizados por el centro.

5. Permitir el uso inadecuado de dispositivos o redes

No se deben dejar ordenadores desbloqueados, compartir contraseñas, no proteger el acceso al correo institucional o no reportar incidencias al CAU mediante el procedimiento establecido en el centro, entre otros.



6. Utilizar medios de comunicación no seguros



Hay que evitar el uso de medios de comunicación no seguros tales como WhatsApp o redes sociales para compartir información personal entre docentes y familias o entre docentes y alumnado.

7. No actualizar la documentación ni revisar procedimientos

Se debe fomentar una cultura institucional de respeto a la protección de datos, incluyendo formación al personal, revisión periódica de los procedimientos y adaptación continua a la normativa vigente.

El centro debe ser capaz de demostrar, en todo momento, que cumple con la normativa de protección de datos, documentando procedimientos, autorizaciones, incidencias y decisiones tomadas.



3. USO DE APLICACIONES EDUCATIVAS Y ALMACENAMIENTO EN LA NUBE

El uso de herramientas digitales como apps educativas, plataformas de comunicación, gestores de notas o servicios en la nube, se ha generalizado en los centros educativos. Sin embargo, su incorporación en el entorno escolar implica el tratamiento de datos personales de alumnado, familias y docentes, por lo que su utilización debe estar sujeta a un control riguroso por parte del centro educativo.

La Agencia Española de Protección de Datos (AEPD) advierte de los riesgos de utilizar aplicaciones no autorizadas o insuficientemente transparentes que pueden conllevar tratamientos no deseados, elaboración de perfiles del alumnado o transferencias internacionales no controladas.

A. EVALUACIÓN PREVIA DE APLICACIONES QUE REQUIERA LA SUBIDA DE DATOS PERSONALES A LA NUBE: UNA OBLIGACIÓN LEGAL Y PREVENTIVA

Cuando las aplicaciones o servicios en la nube, que traten datos personales o sensibles del alumnado, docentes y personal no docente de los centros, no hayan sido contratadas desde la Administración, previo a su uso deben seguir el procedimiento establecido por la Consejería de Educación y estar autorizadas por el Delegado de Protección de Datos para los Centros Docentes. En general, se deberían tener en cuenta los siguientes criterios:

Criterio	Aspecto a comprobar
Finalidad	¿Qué hace la aplicación: ¿gestiona calificaciones? ¿permite crear perfiles? ¿comunica con terceros?
Datos recogidos	¿Qué tipo de datos personales trata? (nombres, imágenes, vídeos, etc.)
Base legal del tratamiento	¿Se ampara en interés público o requiere consentimiento? ¿Se pide consentimiento a las familias?
Responsable del tratamiento	¿Es el centro o una empresa externa quien controla los datos?
Ubicación de los servidores	¿Se almacenan en la UE o en terceros países? ¿Se cumple con las garantías del RGPD?
Política de privacidad	¿Está disponible, clara, accesible y completa? ¿Indica quién accede a los datos? ¿Durante cuánto tiempo? ¿Para qué?
Medidas de seguridad	¿Cifra la información? ¿Permite la gestión de accesos? ¿Hay trazabilidad de las acciones de los usuarios?
Control docente	¿Permite al profesorado controlar lo que el alumnado publica o comparte?

Estas comprobaciones deberán documentarse mediante una ficha de evaluación interna, por ejemplo, y formar parte de la política de seguridad del centro.

B. PROCEDIMIENTO DE AUTORIZACIÓN Y USO

El uso de cualquier app o servicio en la nube que implique tratamiento de datos personales o sensibles y que no haya sido contratada desde la Administración, debería seguir el siguiente procedimiento:

1. Solicitud de evaluación por parte del docente o grupo que propone la app y posterior valoración del equipo directivo.
2. Solicitud de autorización al Delegado de Protección de Datos para los Centros Docentes al que se le remitirá a través de un [Clip a Soporte de Murciaeduca](#) en la categoría “ Encargo de tratamientos de datos personales”. En el campo título del ticket debe incluir el **nombre de la aplicación** que se pretende contratar y en el campo descripción, una **justificación de la necesidad** de contratación. Los documentos a remitir son:
 - ADENDA  Descargue el documento y exija a la empresa seleccionada que incluya en su oferta el documento debidamente cumplimentado, firmado en formato PDF y sin eliminar ni modificar ningún apartado.
 - Documento de cumplimiento de política de privacidad de la empresa propietaria de la aplicación (anexado a la ADENDA).
 - Documento de cumplimiento del Esquema Nacional de Seguridad (ENS) de la empresa propietaria de la aplicación (anexado a la ADENDA).
3. Autorización formal por escrito, en acta de reunión o resolución interna.
4. Información a las familias, siempre y cuando se traten datos de carácter personal.
5. Registro en el inventario de herramientas digitales del centro.



C. INFORMACIÓN CLARA Y ANTICIPADA A LAS FAMILIAS

Cuando las herramientas digitales utilizadas por el centro tratan datos personales del alumnado, incluso mínimamente, las familias deben ser informadas de forma completa, clara y accesible. Esta información debe incluir:

-  Nombre y funcionalidad de la aplicación.
-  Qué tipo de datos personales se van a tratar.
-  Si se almacenan en la nube y dónde.
-  Si existe un perfil público del menor o posibilidad de interacción con terceros.
-  Qué derechos tienen las familias y cómo pueden ejercerlos (acceso, oposición, retirada del consentimiento, etc.).

Esta información puede integrarse en la documentación inicial de curso como anexo a la matrícula o difundirse a través de circulares o plataformas oficiales.



INFORMATION

D. CASOS DE USO FRECUENTES Y RIESGOS ASOCIADOS

En la siguiente tabla se muestran casos frecuentes que encontramos en las aulas. Ten en cuenta que incluso cuando la app es "gratuita", el tratamiento de datos puede ser su forma de financiación, a través de publicidad, análisis de comportamiento o venta de perfiles.

Categoría	Ejemplos frecuentes	Riesgos si no se controla su uso
Cuadernos digitales del docente	Additio, Idoceo	Almacenan calificaciones, asistencia, informes. ¿Dónde se guardan? ¿Quién accede?
Plataformas en la nube	Google Drive, Dropbox, OneDrive	Almacenamiento de trabajos, fotos, documentos. Riesgo si se usan cuentas no corporativas.
Gamificación educativa	Kahoot, Quizizz, Classcraft	Puede requerir registros de alumnos y alumnas y generar perfiles de aprendizaje.
Mensajería instantánea	WhatsApp, Telegram, Signal	No permite trazabilidad institucional. Uso incontrolado.
Redes sociales	Instagram, Facebook, TikTok	Publicación de imágenes y datos personales sin consentimiento en RRSS.
Páginas web	Alojar la web en un dominio distinto a https://web.murciaeduca.es .	No controlar la ubicación de imágenes y datos de los servidores.

IMPORTANT!

Si la página web del centro no es la ofrecida por la Consejería de Educación (Wordpress) y se trata de una web contratada por el centro, es imprescindible que esté autorizada por el procedimiento indicado en la página anterior.

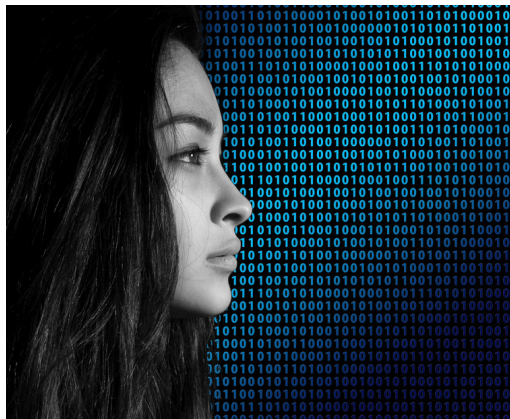
E. CLAVES PARA EL USO DE APPS EN LA NUBE

- Usar únicamente aplicaciones previamente autorizadas por el centro y validadas por el DPD para los centros docentes de la Consejería de Educación.
- Incluir en el Plan Digital de Centro, punto 6.2, un catálogo de herramientas digitales seguras.
- Informar a las familias y recoger consentimiento explícito cuando sea necesario.
- Configurar todas las apps y plataformas con opciones máximas de privacidad.
- Evitar que los menores creen cuentas personales sin supervisión.
- Desactivar funciones innecesarias (geolocalización, seguimiento, perfiles públicos).
- Establecer protocolos de uso y desactivación de cuentas una vez finalizado el curso, salvo que se tenga la intención de seguir usándolas.



F. ELIMINACIÓN DE DATOS Y VIDA ÚTIL DE LAS CUENTAS

El centro debe establecer criterios para la eliminación o anonimización de los datos personales tratados mediante aplicaciones digitales. Esto incluye:



1. Eliminar los grupos de clase de alumnado al finalizar el curso si no se va a utilizar de nuevo.
2. Comprobar que la app ofrece opciones de eliminación efectiva y no conserva datos ocultos.
3. Suprimir vídeos, grabaciones, fotos y materiales que ya no sean necesarios.
4. Exigir al proveedor que devuelva o destruya los datos si se cancela el uso.

G. RESPONSABILIDAD DEL CENTRO EDUCATIVO

El centro es responsable del tratamiento incluso cuando los docentes utilicen apps por iniciativa propia. Por tanto, no es válido alegar desconocimiento o que el profesorado ha actuado por su cuenta. Además:

- El uso inadecuado de una aplicación puede derivar en reclamaciones por parte de familias.
- Una mala gestión puede generar una brecha de seguridad denunciante ante la AEPD.
- El tratamiento no autorizado puede acarrear sanciones económicas o responsabilidad disciplinaria si se ha actuado con negligencia.



IMPORTANT!

Para ampliar información, consultar la Guía para el uso de apps en la nube en el ámbito docente de la AEPD.



4. BUENAS PRÁCTICAS EN EL USO DE MEDIOS ELECTRÓNICOS

La digitalización de los procesos educativos ha incrementado la dependencia de los sistemas de información y de los dispositivos electrónicos (ordenadores, redes, plataformas digitales, aplicaciones móviles, etc.). El uso adecuado de estos medios no solo garantiza una mayor eficiencia organizativa, sino que es fundamental para preservar la confidencialidad, integridad y disponibilidad de los datos personales tratados en los centros.

El Manual de uso de medios electrónicos para el personal de la Administración Pública Regional  establece un marco normativo y operativo para todo el personal público de la Región de Murcia, incluyendo expresamente al personal docente de enseñanzas no universitarias.



A. PRINCIPIOS FUNDAMENTALES QUE DEBEN GUIAR EL USO DE LOS MEDIOS ELECTRÓNICOS

Los centros educativos deben adoptar una cultura institucional basada en los siguientes principios:

Principio	Descripción
Finalidad profesional	Los medios electrónicos deben utilizarse únicamente para el desarrollo de la función docente, administrativa o de gestión del centro.
Buena fe y diligencia	El uso debe regirse por la honestidad, el sentido común y la responsabilidad personal en la gestión de la información.
Seguridad de la información	Todo usuario debe contribuir activamente a proteger la información frente a accesos no autorizados, pérdidas o alteraciones.
Trazabilidad y control	Los accesos y acciones sobre los sistemas deben ser registrados y verificables. El uso indebido puede ser objeto de revisión o auditoría.
Respeto a la legalidad	Especial atención al cumplimiento del RGPD, la LOPDGDD y la normativa autonómica sobre protección de datos y administración electrónica.

B. COMPORTAMIENTOS ESPERADOS DEL PERSONAL DE LOS CENTROS



El personal docente, administrativo o de servicios debe conocer y aplicar, de forma proactiva, las siguientes buenas prácticas:

1. Uso de cuentas y contraseñas

No compartir nunca las credenciales de acceso a plataformas o sistemas.
Cambiar las contraseñas periódicamente y utilizar combinaciones robustas.
Cerrar sesión en ordenadores compartidos y nunca dejar dispositivos desbloqueados.
Activar sistemas de doble autenticación cuando estén disponibles.

2. Uso de dispositivos informáticos

Usar únicamente equipos autorizados por el centro o la Administración educativa.
Evitar instalar software no autorizado o descargado desde fuentes inseguras.
No manipular el hardware ni cambiar configuraciones sin autorización.
Mantener el equipo actualizado y con antivirus activo.
Apagar o suspender el equipo al finalizar la jornada; bloquearlo en ausencias temporales.

3. Almacenamiento y tratamiento de la información

No guardar información personal o sensible en dispositivos externos no cifrados o sin control institucional.
Utilizar las carpetas de red o entornos corporativos para guardar documentos de gestión escolar.
Evitar almacenar información en el escritorio o en carpetas locales no respaldadas.
Utilizar sistemas de almacenamiento autorizados (como nubes corporativas o intranet regional).

4. Uso del correo electrónico

Usar siempre el correo institucional (@murciaeduca.es o @carm.es) para comunicaciones con familias o alumnado.
No reenviar cadenas, enlaces sospechosos ni contenidos que puedan comprometer la seguridad.
Revisar cuidadosamente los documentos adjuntos antes de enviarlos para evitar filtraciones.

5. Comunicación y uso de plataformas

Priorizar el uso de plataformas oficiales (Mirador, Plumier XXI, plataformas Moodle de la Consejería de Educación y Formación Profesional).
Evitar el uso de mensajería instantánea (WhatsApp, Telegram, etc.) para gestionar datos personales o enviar documentación educativa. En caso de utilizarlas se debe recurrir a las que están contratadas por la Consejería de Educación.

C. CONDUCTAS QUE DEBEN EVITARSE

A continuación se resumen algunas acciones expresamente prohibidas por la normativa vigente:



Conducta incorrecta	Riesgo asociado
Instalar software no autorizado o sin licencia	Posible entrada de malware, vulneración de derechos de autor
Acceder a datos sin autorización específica	Infracción del principio de minimización de datos
Usar dispositivos personales no autorizados para gestionar datos escolares	Fuga de información, falta de control y trazabilidad
Conectar dispositivos externos sin revisión previa	Introducción de virus o acceso no autorizado
Dejar el equipo desbloqueado o sin vigilancia	Acceso indebido a información confidencial
Compartir contraseñas o credenciales	Riesgo de suplantación de identidad y pérdida de control
Utilizar el correo personal para remitir información del alumnado o del centro	Pérdida de trazabilidad y posible vulneración del RGPD
Almacenar datos sensibles en carpetas no protegidas o nubes no autorizadas	Exposición a accesos no autorizados
No comunicar incidentes detectados o sospechas de seguridad	Obstaculiza la respuesta rápida y eficaz ante ciberataques

F. RESPONSABILIDADES Y CONSECUENCIAS

Los centros educativos tienen la obligación de comunicar brechas de seguridad a la AEPD si se producen filtraciones relevantes de datos personales.

Por otro lado, el uso indebido de los medios electrónicos puede conllevar:

- Consecuencias disciplinarias para el empleado público (según régimen disciplinario).
- Responsabilidad civil o penal si el incidente causa daños a terceros o infringe la normativa de protección de datos.



Para conocer si el centro aplica buenas prácticas con respecto al uso de la tecnología sería recomendable utilizar una lista de control.

A modo de ejemplo se ofrece la siguiente propuesta



5. CONCLUSIÓN

La protección de los datos personales en los centros educativos es un compromiso fundamental para garantizar la privacidad y seguridad de los estudiantes, docentes y personal no docente. Implementar medidas claras y efectivas de seguridad, en conformidad con las normativas legales vigentes, no solo es una obligación, sino también un pilar para fomentar un entorno educativo de confianza y respeto.

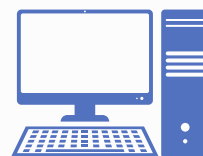
Es esencial que todos los miembros de la comunidad educativa conozcan y comprendan la importancia de proteger la información personal y adopten buenas prácticas en el manejo de los datos. En este sentido, los órganos de coordinación docente, tales como el Claustro de profesores, los equipos dinamizadores de la estrategia digital, los equipos de ciclo o los departamentos, entre otros, pueden favorecer la difusión y el correcto cumplimiento de estas recomendaciones.

La educación en privacidad y seguridad debe ser continua, promoviendo una cultura de protección que se mantenga vigente y adaptada a los avances tecnológicos y los nuevos desafíos en el ámbito digital.



ANEXOS

Uso seguro y responsable de medios electrónicos en el centro educativo



Marca  si se cumple completamente,  si solo se cumple parcialmente o existe alguna duda, y  si no se cumple.

Se recomienda su cumplimentación al menos una vez al año como parte del plan de mejora del centro para conocer si el centro aplica buenas prácticas con respecto al uso de la tecnología.

1. Organización y formación del personal			
Todo el personal conoce las normas del Manual de uso de medios electrónicos de la Región de Murcia.			
Se han realizado sesiones formativas sobre uso responsable de equipos y seguridad digital.			
Existe una persona o equipo de referencia en el centro para dudas relacionadas con seguridad informática.			
Se revisan y actualizan periódicamente las políticas internas de uso de las tecnologías digitales del centro.			
Observaciones:			

2. Uso de equipos y dispositivos			
Todos los dispositivos del centro están configurados con usuarios personales o contraseñas seguras.			
El profesorado bloquea el equipo o cierra sesión cuando se ausenta de su puesto.			
Está prohibido modificar la configuración del hardware o instalar software sin autorización.			
Los equipos del centro se apagan al finalizar la jornada escolar.			
Los dispositivos personales no se usan para almacenar o tratar datos del alumnado sin autorización.			
Observaciones:			

3. Seguridad en el almacenamiento y tratamiento de datos			
Los datos personales se almacenan en ubicaciones seguras: red corporativa o nube institucional.			
No se almacena información sensible en carpetas locales no protegidas (como el escritorio del PC).			
Se realiza borrado seguro de la información cuando ya no se necesita.			
Solo se accede a la información para la que se ha recibido autorización expresa.			
Observaciones:			

4. Uso del correo electrónico y las plataformas			
Se utiliza exclusivamente el correo institucional para las comunicaciones escolares.			
No se reenvían cadenas, mensajes virales o enlaces sospechosos.			
Antes de enviar información sensible, se verifica que el destinatario es el correcto.			
El profesorado no utiliza redes sociales o apps de mensajería personal para enviar datos escolares.			
Observaciones:			

5. Gestión de incidentes y soporte			
El personal sabe a quién comunicar una incidencia o brecha de seguridad.			
Se notifican los incidentes técnicos en cuanto se detectan.			
Se siguen los protocolos indicados por la Administración tras una incidencia.			
Existe conciencia sobre las consecuencias legales y disciplinarias del uso indebido de los sistemas.			
Observaciones:			

PROTOCOLO

de actuación para la PROTECCIÓN DE DATOS PERSONALES



índice

1. Objetivos
2. Ámbito de aplicación
3. Marco normativo
4. Responsables
5. Registro de actividades de tratamiento
6. Información y derechos
7. Uso de plataformas y aplicaciones
8. Consentimiento y tratamiento de imágenes
9. Medidas de seguridad
10. Formación y concienciación
11. Gestión de incidencias y brechas de seguridad
12. Ejercicio de derechos
13. Supervisión y revisión



1. Objetivos

- Garantizar la protección de los datos personales del alumnado, familias, profesorado y personal del centro.
 - Regular el uso seguro de plataformas digitales y aplicaciones educativas.
 - Prevenir incidentes de seguridad mediante medidas organizativas y técnicas.
 - Integrar este protocolo en el Plan Digital de Centro (PDC).
-

2. Ámbito de aplicación

Este protocolo se aplica a:

- Alumnado y sus familias.
- Profesorado y personal no docente.
- Empresas y entidades colaboradoras (comedor, transporte, actividades externas).

Incluye todos los tratamientos de datos: matrícula, expedientes, uso de imágenes, plataformas educativas, servicios complementarios y actividades extraescolares.

3. Marco normativo

- Reglamento (UE) 2016/679 (RGPD).
 - Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
 - Orden de Estrategia Digital LIBRE (arts. 11 y 17).
 - Esquema Nacional de Seguridad (ENS).
 - Guías y recomendaciones de la AEPD.
-

4. Responsables

- Responsable del tratamiento: la Consejería de Educación / la dirección del centro.
 - Empresas externas y plataformas digitales: obligatoriamente en condición de encargados mediante contrato.
 - Delegado de Protección de Datos (DPD): designado por la Consejería de Educación (dpd@murciaeduca.es).
-

5. Información y derechos

- En la matrícula se incluyen cláusulas informativas normalizadas.
- El centro publica en su web la política de privacidad y el contacto del DPD.
- Se garantiza que alumnado y familias conocen sus derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad.



6. Registro de actividades de tratamiento

El centro mantiene actualizado un registro que incluye, entre otros:

- Gestión académica y expedientes (base jurídica: función pública educativa).
 - Matrícula y admisión (base jurídica: obligación legal).
 - Uso de imágenes y voz (base jurídica: consentimiento informado).
 - Plataformas educativas corporativas (@murciaeduca.es, Aula Virtual) (base jurídica: interés público).
 - Servicios complementarios (comedor, transporte) (base jurídica: ejecución de contrato/consentimiento).
-

7. Uso de plataformas y aplicaciones

- Se utilizan prioritariamente las plataformas corporativas de la CARM.
 - Los alumnos y los docentes se registran únicamente con cuentas @murciaeduca.es en el entorno educativo y profesional.
 - Aplicaciones externas: solo podrán usarse si son autorizadas por la Consejería y validado el tratamiento conforme a RGPD y ENS.
 - Se prohíbe el uso de cuentas personales (Gmail, WhatsApp, Dropbox personal) para datos escolares.
 - Desactivar funciones innecesarias (geolocalización, perfiles públicos).
-

8. Consentimiento y tratamiento de imágenes

- El centro solicita autorización expresa a las familias para el tratamiento de imagen en cualquier actividad o acción.
 - Las imágenes solo se usan en las finalidades autorizadas y se eliminarán cuando dejen de ser necesarias (web institucional, memorias, actividades).
 - Se evita la identificación innecesaria de menores en redes sociales.
-

9. Medidas de seguridad

- Contraseñas robustas, cambio periódico y nunca compartidas.
- Equipos y dispositivos bloqueados cuando no estén bajo vigilancia.
- Almacenamiento seguro (nube institucional, carpetas protegidas, copias de seguridad cifradas).
- Comunicación preferente por correo institucional. El uso de mensajería instantánea (WhatsApp, Telegram) solo en casos excepcionales y documentados.
- Prohibido almacenar información personal en dispositivos o nubes no autorizadas.
- Actualización y revisión constante de los procedimientos y documentación.



10. Formación y concienciación

- Formación inicial y periódica para todo el personal en protección de datos, ciberseguridad y uso responsable de medios digitales.
 - Formación en el uso, riesgos y recomendaciones sobre aplicaciones y plataformas.
 - Difusión de recursos de privacidad, seguridad y buen uso digital entre alumnado y familias.
-

11. Gestión de incidencias y brechas de seguridad

- Notificación inmediata al Centro de Atención a Usuarios (CAU) y comunicación al DPD en menos de 72 horas.
 - Registro de incidentes, evaluación de riesgos, contención y comunicación a las familias afectadas si procede.
 - Análisis de causas y adopción de medidas correctoras.
-

12. Ejercicio de derechos

Las familias y el personal pueden ejercer sus derechos mediante:

- Solicitud en Secretaría.
- Envío al correo institucional del centro.
- Contacto directo con el DPD (dpd@murciaeduca.es).

El centro responderá en un máximo de 1 mes.

13. Supervisión y revisión

- Revisión anual en Claustro y Consejo Escolar.
 - Actualización según cambios normativos, tecnológicos o incidentes.
 - Integración y coherencia total con el Plan Digital de Centro.
-

CONCLUSIÓN:

El presente protocolo es un modelo creado, a modo de ejemplo, que pretende cumplir con el artículo 3.4 de la Orden de Estrategia digital LIBRE, donde se recoge uno de sus principios básicos, “ Protección de los derechos fundamentales y seguridad digital respetando la privacidad y la seguridad de los datos personales”. Además, tal y como queda recogido en el artículo 11 de la Orden, sobre protección de datos personales y privacidad, la implementación de protocolos para la protección de los datos personales.



#DigitalProf



Financiado por
la Unión Europea
NextGenerationEU



MINISTERIO
DE EDUCACIÓN
Y FORMACIÓN PROFESIONAL



Plan de Recuperación,
Transformación
y Resiliencia

Región  de Murcia



BY



SA