

INSTRUCCIONES PARA EL TRATAMIENTO ADECUADO DE

LOS DATOS DE CARÁCTER PERSONAL Y DE SEGURIDAD DE LA INFORMACIÓN

Normativa de referencia:

- ◆ [Reglamento \(UE\) 2016/679 General de Protección de Datos.](#)
- ◆ [Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.](#)
- ◆ [Real Decreto 311/2022, de 3 de mayo, Esquema Nacional de Seguridad.](#)
- ◆ [Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.](#)
- ◆ [Decreto 70/2017, de 6 de junio, por el que se modifica el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.](#)
- ◆ [Orden de 3 de diciembre de 2020, por la que se establece la política de seguridad de las tecnologías de la información y comunicaciones de la Consejería de Educación y Deporte.](#)
- ◆ [Orden de 24 de junio de 2021, por la que se modifica la Orden de 3 de diciembre de 2020, por la que se establece la política de seguridad de las Tecnologías de la Información y Comunicaciones de la Consejería de Educación y Deporte.](#)
- ◆ [Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía.](#)

Todo trabajador del centro, en el desempeño de las tareas y funciones de su puesto de trabajo tiene acceso recursos de distinto tipo y, con frecuencia, a datos de carácter personal del alumnado,

de los tutores/as legales del alumnado y de otros trabajadores/as. Debes saber, por lo tanto, que estás sujeto a la normativa de protección de datos que protege los derechos de la ciudadanía en este sentido.

Todo el personal del centro debe ser consciente de la necesidad de garantizar la seguridad e integridad de los sistemas de información que utilicen y la confidencialidad de los datos personales que traten. Por ello, tienen la obligación de conocer y cumplir todas las medidas de seguridad conforme a las instrucciones y procedimientos establecidos por el centro.

¿Qué datos pueden recabar los centros educativos?

La normativa legitima a los centros a recabar datos de carácter personal para la función docente y orientadora de los alumnos en referencia a:

El origen y ambiente familiar y social.

Las características o condiciones personales.

El desarrollo y resultados de su escolarización.

Las circunstancias cuyo conocimiento sea necesario para educar y orientar a los alumnos.

Por tanto, se legitima a los centros educativos para recabar y tratar los datos de los alumnos y de sus padres o tutores, incluyendo también las categorías especiales de datos, como los de salud o de religión, cuando fuesen necesarios para el desempeño de la función docente y orientadora.

Pero también hay que tener en cuenta una serie de cautelas:

Los datos personales no podrán usarse para fines diferentes al educativo (función docente y orientadora).

El profesorado y resto del personal que acceda a los datos personales de los alumnos o de sus familias está sometido al deber de guardar secreto art. 5 LOPDGDD.

Cuando sea preciso obtener el consentimiento de los alumnos o de sus familias o tutores legales para la utilización de sus datos personales para finalidades distintas a las educativas, se debe

informar con claridad de cada una de ellas, permitiendo a los interesados oponerse a aquellas que así lo consideren.

El profesorado será especialmente cuidadoso con aquellos datos personales que son especialmente sensibles por revelar circunstancias o información de las personas sobre su esfera más íntima y personal. Requieren una especial atención por tu parte y debes adoptar las medidas técnicas y organizativas necesarias para evitar que su tratamiento origine lesiones en los derechos y libertades de los titulares de los mismos.

Forman parte de esta categoría de datos personales aquellos que:

1. Revelen ideología, afiliación sindical, religión y creencias.
2. Hagan referencia al origen racial, a la salud y a la vida sexual.
3. Se refieran a la comisión de infracciones penales o administrativas.
4. Datos biométricos y genéticos.

En el ámbito educativo es muy frecuente el tratamiento de datos relativos a la salud física o mental del alumnado, incluida la prestación de servicios de atención sanitaria que revelan información sobre su estado de salud y/o discapacidad física o psíquica.

También son datos especialmente sensibles los contenidos en los informes psicopedagógicos del alumnado.

Un caso especial: la publicación de contenido audiovisual

La Consejería dispone de un registro de actividades de tratamiento, en el cual se incluye como uno de los tratamientos el “Contenido audiovisual de las actividades de los centros y servicios educativos”.

Dicho tratamiento habilita el tratamiento de imágenes del alumnado, padres, madres y/o tutores de alumnos y personal del centro por parte de los centros docentes con la finalidad de la promoción y difusión en los sitios web de los centros y servicios educativos de las actividades culturales, recreativas, deportivas y sociales en las que participa el propio centro.

Para el cumplimiento de la normativa en materia de protección de datos de carácter personal tanto en la toma de fotografías y/o vídeo o cualquier contenido audiovisual como en su publicación en Internet requieren la solicitud de consentimiento, que debe ser inequívoco y prestado mediante una clara acción afirmativa y así como un conjunto de medidas que garanticen la protección de los mismos.

En consecuencia, el centro educativo que desee publicar contenido audiovisual de la comunidad educativa deberán:

Rellenar y mantener actualizado en Séneca el formulario que a tal efecto está disponible (apartado 'Centro' / 'Cuestionarios' / 'Seguridad y protección de datos' / 'Publicación contenido audiovisual').

Asegurar que la finalidad de la publicación es apropiada mediante la evaluación previa del tipo de foto, la pertinencia de su publicación y su objetivo.

Informar y solicitar consentimiento a las personas cuyas imágenes se tomen y publiquen. La captura de contenido audiovisual (fotografías, vídeo, etc.) como su publicación (Internet) requieren el conocimiento y consentimiento del afectado. En caso de fotografiar a un alumno menor de 14 años, se debe informar y recabar el consentimiento de sus padres o tutores, lo cual se puede hacer en la documentación del sobre de matrícula y/o autorizaciones específicas. Es necesario cumplir con estos derechos en los formularios de matriculación, contratación, etc. o en formularios ad-hoc previos al evento mediante un impreso que muestre la cláusula informativa del tratamiento, solicite el consentimiento e indique si la validez es puntual, anual o abarca la totalidad temporal del vínculo del afectado con el centro docente.

Cuando el afectado solicita la oposición o cancelación del uso de las fotografías se debe proceder al borrado de las imágenes o al pixelado de la imagen del afectado en caso de ser una foto de grupo.

Los centros docentes y el profesorado deben ser conscientes de que divulgar información personal en los sitios web que han creado o usan obliga a un cumplimiento riguroso de los principios fundamentales de protección de datos. En este sentido se recomienda que se publique el contenido

audiovisual en sitios que dispongan de mecanismos de acceso restringido (con nombre de usuario y contraseña).

1. Decálogo básico sobre el uso de aplicaciones informáticas (profesorado y PAS)

1. Usa las herramientas corporativas para la información y la comunicación con el alumnado y las familias: Helvia, Moodle Centros, Séneca-Pasen, Correo corporativo (@juntadeandalucía.es), Secretaría virtual, Portal Docente, G-suite corporativo (@g.educaand.es), Microsoft 365 corporativo (@m.educaand.es).

Debes evitar la utilización en tus dispositivos de servicios y aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas corporativas. Dichas aplicaciones podrían registrar datos de carácter personal, incluidas imágenes y calificaciones.

Debes tener en cuenta que las aplicaciones que más datos personales de los alumnos pueden llegar almacenar son los cuadernos de notas de los docentes (Idoceo, Additio, Teacher Aide), que guardan datos sobre el progreso y las calificaciones de los alumnos. Utiliza el Cuaderno del Profesor de la aplicación corporativa Séneca para mantener seguros los datos de tus alumnos y alumnas.

Aunque la mayoría de otras aplicaciones no recopilan datos personales más allá de los básicos de usuario, cualquier aplicación que incluya la identificación del alumno puede facilitar la elaboración externa de perfiles según las funcionalidades y la tipología de los datos recopilados amparándose en una supuesta mejora del servicio. Hay que tener en cuenta que las aplicaciones instalables en dispositivos móviles inteligentes son capaces de acceder a gran cantidad de datos de carácter personal almacenados en el propio dispositivo: número de identificación del terminal, agenda de contactos, imágenes o vídeos. Además, estas aplicaciones pueden acceder a los sensores del dispositivo, y obtener la ubicación geográfica, capturar fotos, vídeos o sonidos a través de ellos.

Las Autoridades europeas de protección de datos aprobaron conjuntamente en marzo de 2013 un dictamen sobre aplicaciones móviles para dispositivos móviles inteligentes. Dicho dictamen [puedes consultarlo aquí](#).

2. Debes solicitar, previamente a su uso, la autorización del centro para la utilización de herramientas o servicios no corporativos. Si se diera el caso de tener que recurrir a ellas, se autorizará únicamente el uso de aplicaciones no corporativas que ofrezcan información claramente definida sobre los tratamientos efectuados, las finalidades de los mismos y sus responsables, así como sobre la ubicación de los datos (siempre en un país del Espacio Económico Europeo o un país que ofrezca un nivel de protección equivalente), el periodo de retención y las garantías con relación a su seguridad.

En cualquier caso las aplicaciones que utilices deben permitir el control por parte de tutores o profesores/as de los contenidos subidos por los menores, en especial de los contenidos multimedia (fotos, vídeos y grabaciones de voz de los alumnos).

3. Debes obtener el consentimiento expreso de los alumnos/as (si son mayores de 14 años) o de los padres o tutores (si son menores de 14 años). Especialmente para el tratamiento de datos personales que puedan suponer un mayor riesgo, tal como el reconocimiento facial de menores de edad (que implica el tratamiento de datos biométricos).

4. Una vez obtenida la autorización del centro y el consentimiento del alumnado (y/o la familia), debes informar a los padres o tutores del comienzo de la utilización de dichas tecnologías en las aulas, así como de las Apps que traten datos personales de los alumnos y su funcionalidad.

5. Debes tener especial cuidado al publicar imágenes y vídeos mediante apps y herramientas en la nube para no poner en riesgo la intimidad de otras personas.

En particular, se considera ineludible que el usuario y las familias deban ser informadas de la utilización de sistemas de almacenamiento en nube. Recuerda que al utilizar sistemas de almacenamiento de documentos en nube tipo Dropbox o iCloud, debes evitar incluir datos personales sensibles, tales como datos relativos a la salud, contraseñas, datos bancarios, material audiovisual de contenido sensible, etc.

6. Lee y lee a tu alumnado la información sobre el servicio o aplicación con el que vas a trabajar (política de privacidad y condiciones de uso) antes de empezar a utilizarlo.

7. Al utilizar redes sociales debes configurar las opciones de privacidad en el perfil de usuario para permitir el acceso a la información publicada únicamente a un grupo de usuarios conocido y previamente definido.

8. Al manejar aplicaciones evita incorporar datos del domicilio de los menores y cualquier otro dato personal que pueda poner en peligro su seguridad (en cualquier tipo de aplicación, en el registro de usuarios, en los contenidos). Advierte al alumnado de no atender la demanda de las aplicaciones para recabar datos personales innecesarios.

9. Las contraseñas que utilicéis deben ser robustas, evitando las que sean fáciles de adivinar por otras personas, con suficientes caracteres y compuestas por mayúsculas, minúsculas, números y caracteres especiales. No se deben de facilitar nunca a otras personas.

10. El uso de aplicaciones de mensajería instantánea (como WhatsApp) entre profesores y familias o entre profesores y alumnos no se recomiendan en absoluto. No obstante, en aquellos casos en los que el interés superior del menor estuviera comprometido, como en caso de accidente o indisposición en una excursión escolar, y con la finalidad de informar y tranquilizar a los padres, titulares de la patria potestad, se podrían captar imágenes y enviárselas.

Más información:

[Guías, informes y documentos sobre los tratamientos de datos personales de las AAPP.](#)

2. Obligaciones generales

1. Asegúrate de que en todos los formularios o documentos (en papel o electrónicos) en que se recaben datos personales está bienvisible la cláusula de información relativa a la protección de datos según establece el artículo 13 del RGPD.

2. No solicites ni recabes más datos que los estrictamente pertinentes, necesarios e imprescindibles para el uso o finalidad de los mismos.

3. No trates ni reutilices los datos para otros usos o fines diferentes para los que se recabaron o solicitaron.

4. Solo debes tratar la información y datos personales que se precisen para la actividad educativa programada y no a otros datos o recursos, aunque estén disponibles y sean accesibles.

5. Guarda estrictamente la confidencialidad de la información a la que se tiene acceso: nunca divulgues, publiques ni reveles datos de carácter personal a terceras personas. En este sentido recuerda:

a) No ceder o comunicar datos personales a terceros salvo que sea necesario para el tratamiento, por obligación legal o por consentimiento expreso de la persona afectada.

b) No publicar listados en la página web o tableros de anuncios con nombres y apellidos y NIF/NIE completos sin anonimizar.

c) No grabar ni difundir imágenes sin el previo y expreso consentimiento de las personas afectadas. Para más información, [mira este enlace](#).

d) No enviar por email archivos o ficheros con datos personales fuera del ámbito del centro sin las medidas de seguridad que garanticen que dicha información solo sea accesible por su destinatario (p.ej. contraseña de acceso, cifrado de datos, etc.).

6. Borra los datos personales, o bloquea su acceso, cuando ya no sean relevantes para la finalidad para la que se recabaron.

7. Facilita el ejercicio de los derechos a los titulares de los datos personales que lo soliciten.

8. Comunica con la mayor brevedad posible cualquier incidencia, vulneración o quiebra de seguridad en el tratamiento de los datos personales a la Dirección del centro.

3. Uso y configuración de los equipos informáticos

1. Los equipos informáticos que el centro pone a disposición del profesorado y el alumnado no deben ser utilizados para fines particulares o privados, tan solo se permite su uso para el desarrollo de tareas académicas, investigadoras o profesionales.

2. No se podrán modificar la configuración de los equipos informáticos ni el software instalado a nivel corporativo.

3. Se debe evitar conectar sin adoptar las medidas de seguridad adecuadas los puestos de trabajo a redes o sistemas exteriores ajenos a la red corporativa (Andared_Corporativo).
4. Se debe evitar desactivar los filtros y mecanismos de seguridad de los equipos.
5. Activar el bloqueo automático de sesión de los equipos cuando no se utilicen durante un tiempo determinado (p.ej. 5-10 minutos de inactividad).
6. No instalar programas o software sin licencia o no corporativos en los ordenadores. Si fuera necesaria su instalación, deberá solicitarse al centro para que lo gestione.
7. No almacenar en el disco duro o memoria de los ordenadores documentos que contengan datos de carácter personal.
8. Los archivos temporales o las descargas de archivos que contengan datos personales se realizarán en un mismo directorio o carpeta de forma que no queden dispersos por todo el disco duro del ordenador para proceder periódicamente a su borrado cuando ya no sean necesarios.
9. No se deben sacar equipos fuera de las instalaciones del centro sin aplicar las debidas medidas de seguridad para proteger su contenido y archivos.
10. Cuando una incidencia y/o deficiencia pudiera suponer una vulneración o quiebra de seguridad en el tratamiento de los datos personales, se deberá poner en conocimiento de la dirección del centro a fin de que se adopten las medidas oportunas.

4. Control de cuentas de usuarios y contraseñas

1. Tanto las cuentas de usuario como los certificados digitales son personales e intransferibles. Debes ser consciente de que como usuario eres responsable de las acciones que se realicen con tu identidad en los sistemas de información.

En ningún caso, se deberán facilitar ni revelar a terceros u otros usuarios las claves, password o códigos (PIN, contraseña, etc.) que puedan ser necesarios para su acceso o activación debiendo mantenerlas en todo momento en secreto.

2. Se debe ser cuidadoso/a y diligente en la custodia y salvaguarda de tus claves privadas y contraseñas, debiendo informar a la mayor brevedad a la dirección del centro cuando haya razones para creer que una contraseña ha sido robada, comprometida o compartida por el alumnado o cualquier otro usuario.
3. Nunca reutilizar las contraseñas utilizadas en las distintas aplicaciones del centro en servicios proveedores de terceros o para usos privados y personales.
4. Cada usuario es responsable del control, confidencialidad y cambio de la contraseña de acceso a los equipos informáticos. Se recomienda:
 - a) Usar una contraseña diferente para cada cuenta o aplicación.
 - b) Cambiar la contraseña periódicamente.
 - c) La contraseña debe ser lo suficientemente larga y compleja para no ser adivinable por terceros. Preferiblemente deberá contener al menos 8 dígitos así como números, letras mayúsculas y minúsculas o algún signo de puntuación.
 - d) Es recomendable usar un programa de gestión de contraseñas (LastPass, Dashlane) para poder recordarlas y no tener que anotarlas en una libreta o cuaderno.

5. Internet y cuentas de correo electrónico corporativo

1. La utilización de Internet en el centro y el correo electrónico corporativo debe responder exclusivamente a fines profesionales, docentes o académicos, debiendo observarse el deber de diligencia en la utilización del mismo.
2. No acceder a páginas de intercambio y descarga de archivos P2P, páginas web inseguras, así como otros sitios susceptibles de contener virus o favorecer la ejecución de código dañino.
3. No se deben publicar o divulgar en internet, redes sociales, foros, etc., imágenes, videos o listados con nombres y apellidos y NIF/NIE completos sin anonimizar sin el consentimiento expreso de las personas afectadas o sin que lo habilite una ley.

4. No se deben enviar por e-mail archivos o ficheros con datos personales del alumnado o las familias sin las medidas de seguridad que garanticen que dicha información no sea inteligible ni manipulada por terceros durante la transmisión o que tan solo sea accesible por su destinatario (p.ej. contraseña de acceso, cifrado de datos, etc.).
5. Para evitar el correo masivo no solicitado, "spam", como regla general, solo se debe proporcionar tu dirección de correo electrónico corporativo a personas y/o entidades conocidas.
6. Nunca se facilitará la cuenta de correo electrónico corporativo del centro a personas no autorizadas o en foros, redes sociales o páginas web no institucionales.
7. En el caso de recibir correos electrónicos cuyo remitente y/o contenido sea dudoso, no abrir los archivos adjuntos.

6. La seguridad en los dispositivos móviles, smartphones y tablets proporcionados por el centro y que pudieran contener datos personales del alumnado y las familias

1. Activar el desbloqueo de tu dispositivo con contraseña o datos biométricos mejor que un patrón.
2. Mantener siempre el dispositivo, aplicaciones y el antivirus actualizados.
3. Desactivar la Wifi y el Bluetooth cuando no sean necesarios. No conectarse a redes Wifi públicas y abiertas sin adoptar las oportunas medidas de seguridad.
4. Modificar tu configuración de privacidad para limitar el acceso de las diferentes aplicaciones a tus datos. Controlar los permisos que habilitas en la descarga de aplicaciones o apps.
5. Evitar descargar y guardar en el dispositivo archivos con datos personales o confidenciales. Si es necesario conservarlos, hay que protegerlos con una contraseña de acceso.
6. Instalar o activar un servicio de localización para poder recuperar los dispositivos en caso de pérdida, extravío o sustracción.

7. Impedir la accesibilidad a los datos por personas no autorizadas

1. Custodiar la documentación y garantiza que los datos e información tratada desde el puesto de trabajo no pueda ser visible ni accesible por personas no autorizadas.

- a) Durante el trabajo, la pantalla del ordenador estará orientada para que la información sólo pueda ser visible por el usuario y no por terceras personas.
- b) No dejar a la vista documentos con datos personales sobre la mesa, fotocopadoras o impresoras, etc.
- c) Una vez que se haya finalizado el trabajo, los documentos en papel no deben quedarse en la mesa y deberán guardarse bajo llave en su archivador correspondiente o se destruirán.
- d) En los equipos de aula o aquellos que estén al alcance de terceros, nunca dejar desatendido el ordenador sin activar el sistema de bloqueo del que disponga el equipo (salvapantalla protegido por contraseña, bloqueo del terminal, etc.) con el fin de que se no visualicen datos en la pantalla o se pueda acceder al equipo sin autorización.

2. Asegurarse de que cuando el profesor/a se ausente de su puesto de trabajo, bien temporalmente o bien al finalizar la jornada, el ordenador queda apagado para evitar que se acceda al equipo y no quedan sobre la mesa documentos que contengan datos de carácter personal.

8. Trabajo fuera del centro

1. Cuando se trabaje con datos personales o sensibles de tu alumnado, se debe evitar simultanear la actividad personal o doméstica con la académica y profesional mediante el mismo usuario por lo que hay que definir perfiles diferentes de acceso en el sistema operativo para desarrollar cada tipo de tarea.

2. Cuando se trabaje con datos personales o sensibles del centro, se deberá evitar la conexión de los dispositivos portátiles a redes WIFI abiertas no seguras.

3. Se deberán implementar las medidas de seguridad preventivas que sean apropiadas para salvaguardar la integridad y confidencialidad de los datos personales cuando se trabaje con el fichero o documentos en papel fuera del centro o del puesto de trabajo habitual.

a) No se debe llevar ni transportar expedientes ni documentación en papel sin las correspondientes medidas de seguridad que garanticen su custodia y confidencialidad. Siempre que sea posible y los medios lo permitan, se recomienda escanear la documentación para convertir los documentos en papel a soporte electrónico.

b) No se deberá copiar ni transportar información en ordenadores portátiles, smartphones, tabletas, discos externos, pendrive, etc. sin las correspondientes medidas de seguridad (contraseña de acceso, cifrado de datos, etc.).

4. Cuando se hable por teléfono manejando datos personales de alumnado, familias y personal del centro, se evitará que se puedan escuchar conversaciones por parte de terceros ajenos retirándose a un espacio adecuado.

5. En las pausas o concluida la jornada de trabajo debe cerrarse la sesión de acceso y bloquear o apagar el uso del dispositivo para evitar accesos no autorizados por parte de terceros.

9. Destrucción de información y soportes

1. Si habitualmente trabajas con papel, es importante extremar las precauciones para evitar arrojar hojas enteras o en trozos en papeleras a los que alguien podría acceder y recuperar información de carácter personal.

2. La destrucción de la información que contenga datos de carácter personal, cualquiera que sea su soporte (ordenadores, CDs, disketes o en papel) deberá ser de tal forma que no pueda ser recuperada ni manipulada por terceras personas.

10. Sitios de interés

- [Agencia Española de Protección de Datos \(AEPD\)](#)
- [Instituto Nacional de Ciberseguridad de España \(INCIBE\)](#)

- [Centro Criptológico Nacional](#) (CCN-CERT)
- [Centro Criptológico Nacional](#) (CCN-CERT)