Región de Murcia
Consejería de Educación y Formación Profesional

I.E.S. MIGUEL DE CERVANTES
Avda. Miguel de Cervantes, 3 Tel. 968275161
30006197@murciaeduca.es

Unión Europea

📑 PROTOCOLO DE PROTECCIÓN DE DATOS PERSONALES

(Alineado con la Orden de 30 de enero de 2017) — En revisión
IES Miguel de Cervantes (Murcia)

(Actualización y armonización normativa para el personal de la Administración Pública Regional, con especial atención al ámbito educativo)

El presente documento constituye el **Protocolo Unificado de Uso de Medios Electrónicos y Protección de Datos Personales**, actualizado e integrado para su aplicación en la **Administración Pública Regional (APR)**, con especial atención al ámbito educativo.

Este protocolo **unifica y adapta** las disposiciones de la **Orden de 30 de enero de 2017 (Manual de Uso)**, el **Protocolo del IES Miguel de Cervantes** (como modelo de referencia sectorial) y la **Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD)**, que desarrolla y complementa el **Reglamento General de Protección de Datos (RGPD)**.

TÍTULO I. MARCO LEGAL, OBJETO Y ÁMBITO DE APLICACIÓN

Artículo 1. Objeto y fundamento legal

El presente protocolo tiene un doble objetivo:

a) **Adaptar** las pautas de conducta y uso de los medios electrónicos y sistemas de información de la Administración Pública Regional al marco jurídico vigente.
b) **Garantizar** los derechos digitales de la ciudadanía —personal, alumnado y familias— conforme a la normativa europea y nacional.

Se fundamenta en las siguientes disposiciones:

- **Reglamento (UE) 2016/679 (RGPD)**, relativo a la protección de las personas físicas en el tratamiento de datos personales.
- **Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD)**, de protección de datos personales y garantía de los derechos digitales.
- **Orden de 30 de enero de 2017**, por la que se aprueba el *Manual de Uso de Medios Electrónicos*, cuyas directrices se actualizan y mantienen.
- **Esquema Nacional de Seguridad (ENS)**, de aplicación obligatoria en todos los tratamientos de datos personales realizados por el sector público.

Artículo 2. Ámbito de aplicación

Las disposiciones de este protocolo son de aplicación **obligatoria** para todo el personal empleado público de las Consejerías y Organismos Autónomos, incluyendo al **personal docente de enseñanzas no universitarias**.

El resto de entes del **Sector Público Regional** lo aplicarán de forma **subsidiaria**, salvo que dispongan de normativa interna más específica o restrictiva.

TÍTULO II. PRINCIPIOS Y DERECHOS FUNDAMENTALES DEL TRATAMIENTO

Artículo 3. Principios de protección de datos

Todo tratamiento de datos personales deberá ajustarse a los principios recogidos en el RGPD:

1. **Minimización:** Solo se recabarán los datos estrictamente necesarios para la finalidad educativa o administrativa (por ejemplo, expediente académico o datos de contacto).

2. **Confidencialidad:** Todo el personal interviniente en el tratamiento de datos está sujeto al deber de confidencialidad, incluso tras la finalización de la relación laboral o administrativa.

3. **Licitud y transparencia:** La recogida y el tratamiento deberán informarse al interesado mediante el principio de información por capas, indicando la finalidad y la base jurídica del tratamiento.

Artículo 4. Consentimiento y menores de edad

1. **Validez del consentimiento:** Debe ser libre, específico, informado e inequívoco, manifestado mediante una declaración o acción afirmativa. Queda excluido el consentimiento tácito.

2. **Consentimiento de menores:** Los mayores de 14 años pueden consentir el tratamiento de sus datos personales. En el caso de menores de 14 años, el consentimiento deberá otorgarse por quien ostente la patria potestad o tutela.

3. **Protección digital del menor:** Los centros educativos garantizarán el interés superior del menor en la difusión de sus datos o imágenes en Internet y redes sociales, exigiendo consentimiento previo conforme al artículo 7 de la LOPDGDD.

Artículo 5. Ejercicio de derechos

Las personas afectadas (alumnado, familias y personal) podrán ejercer los **derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad**.

1. **Derecho de acceso:** Podrá facilitarse mediante sistemas de acceso remoto, directo y seguro a los datos personales.

2. **Derecho de supresión (“derecho al olvido”):** Toda persona puede solicitar la eliminación de sus datos publicados en redes sociales o servicios equivalentes. Si los datos fueron publicados durante la minoría de edad, el prestador deberá proceder a su supresión inmediata.

TÍTULO III. ORGANIZACIÓN Y RESPONSABILIDAD ACTIVA

Artículo 6. Roles y designaciones

1. **Responsables y encargados:** Determinarán las medidas técnicas y organizativas necesarias para garantizar y acreditar el cumplimiento del RGPD y la LOPDGDD.

2. **Delegado de Protección de Datos (DPD):** Todos los centros docentes deberán designar un DPD con las funciones establecidas en la normativa vigente.

3. **Funciones del DPD:** Actuará como interlocutor ante la AEPD, con acceso pleno a los datos personales y procesos de tratamiento, sin que pueda oponérsele el deber de confidencialidad.

4. **Intervención previa:** Antes de presentar una reclamación ante la AEPD, el afectado podrá dirigirse al DPD, quien resolverá en un plazo máximo de **dos meses**.

Artículo 7. Control, inspección y ciberseguridad

1. **Competencias de la Dirección General de Informática:**

    - Diseñar y operar sistemas de información que registren evidencias de uso conforme al ENS.

    - Establecer y ejecutar las medidas técnicas necesarias para garantizar la seguridad.

    - Revocar preventivamente credenciales o retirar dispositivos en caso de incidente grave.

    - Autorizar el uso de dispositivos personales (BYOD) bajo condiciones específicas de seguridad.

2. **Centros directivos:** Supervisarán el uso adecuado de los sistemas y la correcta asignación de permisos, evitando accesos innecesarios.

3. **Esquema Nacional de Seguridad (ENS):** Su aplicación es obligatoria para todos los tratamientos de datos personales en la APR.

Artículo 8. Protocolo de incidencias y brechas de seguridad

1. **Comunicación de incidentes:** Todo usuario deberá notificar al Centro de Atención a Usuarios (CAU) cualquier incidencia que afecte o pueda afectar a la seguridad de la información.

2. **Notificación de violaciones:** En caso de brecha de seguridad grave, el responsable deberá informar al DPD y, en su caso, a la AEPD en un plazo máximo de **72 horas**.

3. **Bloqueo de datos:** Cuando se solicite la rectificación o supresión, los datos deberán bloquearse y conservarse únicamente para fines legales o judiciales.

TÍTULO IV. NORMAS DE USO DE MEDIOS ELECTRÓNICOS

Artículo 9. Equipos y dispositivos

1. Los sistemas de información (equipos, red y correo) se destinarán exclusivamente a fines laborales o educativos.

2. Queda prohibida la instalación de software sin licencia o autorización, así como el almacenamiento de información personal ajena a las funciones del puesto.

3. El usuario deberá bloquear su equipo durante las ausencias y custodiar los documentos impresos que contengan datos confidenciales.

4. Se prohíbe desechar documentos con información personal sin garantizar su destrucción segura.

Artículo 10. Correo electrónico, claves y contraseñas

1. Las credenciales de acceso y los sistemas de firma no deben compartirse ni exponerse.

2. Las contraseñas deberán ser seguras y renovarse al menos **una vez al año**.

3. Se prohíbe responder a correos que soliciten credenciales (*phishing*) y utilizar el correo corporativo para fines personales.

4. Para el envío de información sensible, se recomienda el **cifrado de datos**.

Artículo 11. Aplicaciones externas y servicios en la nube

1. En el ámbito educativo, ningún docente podrá emplear aplicaciones que traten datos personales sin la aprobación previa del DPD.

2. Queda prohibido el uso de servicios o cuentas personales (por ejemplo, Google Drive o Dropbox privados, WhatsApp) para el tratamiento de datos académicos sensibles. Se promoverá el uso de **plataformas oficiales corporativas**.

Artículo 12. Vigilancia y control laboral

1. El uso de videovigilancia para control laboral se permitirá conforme al artículo 20.3 del Estatuto de los Trabajadores, previa información expresa y clara al personal.

2. Se prohíbe la instalación de cámaras o grabaciones en zonas de descanso, aseos, comedores o vestuarios.

3. Los sistemas de geolocalización deberán informar de forma clara y permitir el ejercicio de derechos por parte de los trabajadores.

4. El acceso del empleador a los dispositivos digitales solo podrá realizarse para verificar el cumplimiento de las obligaciones laborales o la integridad de los equipos.

TÍTULO V. GARANTÍA DE LOS DERECHOS DIGITALES

Artículo 13. Derechos digitales en el ámbito laboral

1. Los trabajadores tienen derecho a la **intimidad digital** en el uso de los dispositivos proporcionados por la APR. La Administración establecerá criterios de uso con participación de los representantes del personal.

2. Se reconoce el **derecho a la desconexión digital** fuera del horario laboral, garantizando el descanso y la conciliación de la vida personal y familiar.

3. La Administración elaborará una política interna de desconexión, previa audiencia de los representantes, que incluirá medidas formativas para prevenir la **fatiga informática**.

Artículo 14. Derecho a la educación digital

1. El sistema educativo debe asegurar la **integración plena del alumnado** en la sociedad digital, promoviendo la competencia digital y la educación en el uso responsable y seguro de las TIC.

2. El profesorado recibirá la formación necesaria para impartir una enseñanza digital segura, crítica y respetuosa con los derechos humanos.

🪶 *Diseñado con ChatGPT 5.0 bajo supervisión humana a fecha de 13/10/2025*

OpenAI (2025). *ChatGPT (versión GPT-5) [Modelo de lenguaje grande].* https://chat.openai.com/

Declaración de uso de IA:
Parte del contenido de este documento ha sido elaborado con el apoyo de la herramienta ChatGPT (OpenAI, modelo GPT-5, octubre de 2025), utilizada para la revisión gramatical y la mejora de estilo. Las ideas, interpretaciones y conclusiones son responsabilidad exclusiva del autor.
