



**GUÍA SOBRE LA POLÍTICA DE PROTECCIÓN DE DATOS
CIFP HOSTELERÍA Y TURISMO DE CARTAGENA**

*Un compromiso con la innovación, la ética y la calidad educativa
Versión 1.0 – noviembre 2025*

ÍNDICE

I. OBJETO Y ÁMBITO DE APLICACIÓN	3
II. PRINCIPIOS RECTORES DEL TRATAMIENTO DE DATOS	3
III. RESPONSABLES Y FIGURAS CLAVE EN LA PROTECCIÓN DE DATOS.....	4
IV. LEGITIMACIÓN PARA EL TRATAMIENTO Y TIPOLOGÍA DE DATOS	4
V. TRANSPARENCIA Y EL DEBER DE INFORMACIÓN	5
VI. DERECHOS DE LOS INTERESADOS (DERECHOS ARCO+)	5
VII. MEDIDAS DE SEGURIDAD, CIBERSEGURIDAD Y GESTIÓN DOCUMENTAL.....	6
VIII. PROTECCIÓN DE DATOS EN MENORES DE EDAD	7
IX. BIBLIOGRAFÍA.....	8

I. OBJETO Y ÁMBITO DE APLICACIÓN

El objeto principal de esta guía es proporcionar *esencialmente* un marco de actuación unificado para la gestión de datos personales dentro del CFP Hostelería y Turismo de Cartagena. Este centro, dedicado a las familias profesionales de Hostelería, Turismo e Industrias Alimentarias, debe *diligentemente* garantizar el derecho fundamental a la protección de datos de todos los colectivos que *activamente* participan en nuestra comunidad: alumnos, profesores, personal de administración y servicios (PAS), y proveedores.

Esta política es *absolutamente* aplicable a cualquier operación de tratamiento de datos personales que se lleve a cabo en el centro, ya sea mediante procedimientos automatizados o manuales, desde la recogida hasta la destrucción de la información. El cumplimiento de esta guía, basada *primordialmente* en el RGPD y las instrucciones autonómicas, se considera *imprescindiblemente* un componente clave de nuestra estrategia digital LIBRE y nuestro sistema de gestión de calidad (ISO 9001:2015).

II. PRINCIPIOS RECTORES DEL TRATAMIENTO DE DATOS

El tratamiento de datos en nuestro CFP se rige *estrictamente* por los principios establecidos en el RGPD, los cuales exigen una actitud *proactivamente* responsable (*accountability*).

En primer lugar, los datos se tratarán *transparentemente, lícitamente y lealmente*. El Centro *permanentemente* informará a los interesados sobre el tratamiento de sus datos con suficiente antelación.

En segundo lugar, se aplica *rigurosamente* el principio de **limitación de la finalidad**, lo que significa que los datos se recogen *únicamente* con fines legítimos y explícitos, principalmente para la función docente y orientadora, y no se tratarán *posteriormente* de forma incompatible con estos fines. De esta forma, si se recogen datos para la matrícula, no se utilizarán para la difusión de fotografías en la web sin consentimiento *adicionalmente* informado.

En tercer lugar, el principio de **minimización** nos obliga a que los datos sean *solamente* adecuados, pertinentes y limitados a lo necesario. Debemos revisar *periódicamente* la información recopilada para asegurar que no sea excesiva, evitando, por ejemplo, solicitar datos bancarios para actividades extraescolares.

Finalmente, los principios de **integridad y confidencialidad** demandan que los datos se traten *adecuadamente* garantizando su seguridad. El CFP adoptará medidas técnicas y organizativas adaptadas al riesgo. El personal debe **guardar secreto** sobre los datos, un deber que subsiste *incluso* tras la finalización de su relación con el centro.

III. RESPONSABLES Y FIGURAS CLAVE EN LA PROTECCIÓN DE DATOS

En nuestro CFP, la identificación de los actores responsables es *fundamentalmente* clara:

1. **Responsable del Tratamiento:** *Típicamente*, la Administración pública correspondiente, es decir, la Consejería competente en materia educativa de la Comunidad Autónoma de la Región de Murcia, ostenta esta responsabilidad, dado que somos un centro público. No obstante, el centro actúa *coherentemente* bajo estas directrices, analizando *detalladamente* qué datos trata y con qué fines.

2. **Delegado de Protección de Datos (DPD):** Como centro docente, estamos *inexcusablemente* obligados a designar un DPD. El DPD actúa *autónomamente* como informador, asesor y supervisor del cumplimiento normativo, y es *directamente* el interlocutor entre el centro y la Agencia Española de Protección de Datos (AEPD).

3. **Encargado del Tratamiento:** Cuando el CFP externaliza servicios (como algunas actividades extraescolares, Erasmus, etc.) que requieren el tratamiento de datos de nuestro alumnado o personal, las entidades contratadas son *inevitablemente* Encargados del Tratamiento. La relación debe formalizarse *siempre* mediante un contrato escrito que especifique *minuciosamente* las obligaciones, las medidas de seguridad y la instrucción de que los datos no se utilizarán para fines distintos a los previstos.

IV. LEGITIMACIÓN PARA EL TRATAMIENTO Y TIPOLOGÍA DE DATOS

La legitimación para tratar datos personales en nuestro CFP se basa *principalmente* en tres pilares:

1. **Cumplimiento de una Obligación Legal (Función Educativa):** La Ley Orgánica de Educación (LOE) *claramente* nos habilita para tratar los datos personales del alumnado que sean *estrictamente* necesarios para el ejercicio de nuestra función docente y orientadora. Esto incluye *naturalmente* datos identificativos, académicos e *incluso* categorías especiales de datos (como los de salud, particularmente importantes para alumnos con alergias alimentarias en los servicios de restauración).

2. **Relación Contractual:** Los datos relativos a nuestro personal (profesores y PAS) se tratan *legítimamente* en el marco de la relación laboral o administrativa, sin necesidad de su consentimiento *adicional*.

3. **Consentimiento:** Para aquellos tratamientos que *manifiestamente* exceden la función educativa y la relación contractual (como la publicación de fotografías en la web del centro o la comunicación de datos a terceros con fines ajenos a la docencia), se requiere *ineludiblemente* el consentimiento del interesado.

Dada la naturaleza de nuestro CIPF, que atiende a alumnos *mayoritariamente* mayores de 17 años, el umbral de consentimiento es *generalmente* el de la mayoría de edad. Los alumnos mayores de 14 años pueden *válidamente* consentir por sí mismos. El consentimiento debe ser *libre, específico, informado e inequívoco*, y se obtiene mediante una declaración o una acción afirmativa clara (evitando *completamente* el consentimiento tácito o las casillas premarcadas).

V. TRANSPARENCIA Y EL DEBER DE INFORMACIÓN

La escuela debe ser *totalmente* transparente respecto a los tratamientos de datos.

Cuando se recaben datos, se debe informar *inmediatamente* a los interesados (alumnos, padres o tutores) incluso si no se requiere su consentimiento. Esta información debe facilitarse *concisamente, transparentemente, inteligiblemente y fácilmente*. Para los alumnos, el lenguaje debe ser *convenientemente* adaptado a su nivel de comprensión.

La información proporcionada debe incluir *necesariamente*: la identidad del responsable, los datos de contacto del DPD, la finalidad y base jurídica del tratamiento, los destinatarios o categorías de destinatarios, el plazo de conservación (o los criterios para determinarlo), y la existencia y forma de ejercer sus derechos (ARCO+).

Se debe informar *específicamente* a la comunidad educativa sobre los riesgos del uso de tecnologías, incluyendo la Inteligencia Artificial (IA) y la necesidad de usar *siempre* plataformas y aplicaciones que garanticen la seguridad y privacidad (Consejería de Educación).

VI. DERECHOS DE LOS INTERESADOS (DERECHOS ARCO+)

El CIPF *garantiza absolutamente* los derechos de autodeterminación informativa del interesado, los cuales pueden ser ejercidos ante el responsable del Tratamiento. Estos derechos son *personalísimos* y, en nuestro CIPF, serán ejercidos *generalmente* por el propio alumno adulto.

1. Derecho de Acceso: Permite al interesado saber si sus datos están siendo tratados, la finalidad, los destinatarios y el plazo de conservación. El centro debe facilitar, si se solicita, una copia gratuita de los datos *oportunamente* en el plazo de un mes.

2. Derecho de Rectificación: Permite corregir datos inexactos o incompletos. Este derecho se aplica a datos identificativos, pero *manifiestamente* no se utiliza para modificar las calificaciones académicas o el contenido de informes psicopedagógicos, que se rigen *separadamente* por su normativa específica.

3. Derecho de Supresión (Derecho al Olvido): Otorga el derecho a que los datos sean suprimidos cuando ya no sean necesarios para los fines que se recogieron o si se revoca el consentimiento. No obstante, la información de los expedientes académicos *siempre* debe conservarse, ya que puede ser solicitada *posteriormente* a la finalización de los estudios.

4. **Derecho de Oposición:** El interesado puede oponerse al tratamiento de sus datos si existen motivos fundados relacionados con su situación personal.

5. **Derecho a la Limitación del Tratamiento:** Permite que se marquen los datos conservados para limitar *futuramente* su tratamiento bajo ciertas condiciones.

6. **Derecho a la Portabilidad:** El interesado tiene derecho a recibir los datos que haya facilitado en un formato estructurado y de uso común, y a transmitirlos a otro responsable si el tratamiento se basa en consentimiento o contrato y se lleva a cabo por medios automatizados.

VII. MEDIDAS DE SEGURIDAD, CIBERSEGURIDAD Y GESTIÓN DOCUMENTAL

El CIPF *inevitablemente* debe realizar un **Análisis de riesgos (PC-18)** sobre todos los tratamientos de datos que efectúa, especialmente al tratar datos sensibles o de colectivos vulnerables. Este análisis es *esencialmente* la base para determinar las medidas de seguridad organizativas y técnicas adecuadas.

Seguridad Digital y Uso de Aplicaciones: En un CIPF *notablemente* digitalizado con Aula ATECA y red Wi-Fi, la ciberseguridad es *crítica*.

1. **Apps y Plataformas:** Se debe priorizar el uso de la plataforma educativa del centro para la interacción. Los profesores deben solicitar *previamente* la autorización a través del centro a Consejería de Educación, para utilizar cualquier aplicación o herramienta de almacenamiento en nube (como Google Drive o OneDrive) que trate datos personales. Estas aplicaciones deben ofrecer *claramente* información sobre la ubicación de los datos (preferentemente dentro del Espacio Económico Europeo), el periodo de retención y la seguridad ofrecida.

2. **IA y Tecnologías Emergentes:** El uso de la Inteligencia Artificial (IA) en la formación profesional debe seguir *rigurosamente* los protocolos de la Administración. Cualquier herramienta de IA debe ser *pedagógicamente adecuada, ética y segura*, y las decisiones críticas basadas en IA deben ser *siempre* supervisadas y validadas por el profesorado.

3. **Brechas de Seguridad:** Si se produce una violación de seguridad (pérdida, destrucción o acceso no autorizado de datos), el responsable del Tratamiento debe notificar *sin dilación indebida* a la autoridad de control (AEPD) en un plazo *máximo* de 72 horas, salvo que sea improbable que constituya un riesgo para los derechos.

Videovigilancia (si procede): La videovigilancia del CIPF tiene una instalación *proporcional, necesaria e idónea* para el fin legítimo de garantizar la seguridad de personas e instalaciones.

Consecuentemente:

- Las cámaras solo deben cubrir la zona *mínimamente imprescindible*.
- Está *terminantemente* prohibida su instalación en baños, vestuarios o zonas de descanso.
- No existe grabación en aulas.
- Las imágenes se conservarán *solamente* durante el tiempo indispensable, que *generalmente* no debe superar un mes.

Gestión y Eliminación Documental: La documentación generada por el CIFP forma parte del Patrimonio Documental de la Región de Murcia. El proceso de eliminación de documentos se lleva a cabo *periódicamente* cuando se cumplan los plazos de conservación. Para documentos que contengan datos personales o confidenciales, la destrucción se realizará *cuidadosamente* mediante destructoras de papel o empresas especializadas, garantizando *plenamente* la imposibilidad de reconstrucción, a menudo siguiendo la norma DIN 66399. La eliminación de expedientes académicos está *ciertamente* prohibida mientras subsista su valor probatorio o mientras no se cumplan los plazos establecidos. Una vez destruidos los documentos, se levantará *oportunamente* un Acta de Eliminación.

VIII. PROTECCIÓN DE DATOS EN MENORES DE EDAD

Aunque nuestro CIFP atiende *mayormente* a alumnado que *claramente* ha superado los diecisiete años, ocasionalmente acogemos a estudiantes que son *legalmente* menores. La protección de datos para ellos no es *simplemente* una obligación legal, sino *innegablemente* un deber ético que asumimos con total responsabilidad. Reconocemos *irrefutablemente* que los menores constituyen un colectivo vulnerable; *consecuentemente*, su derecho a la privacidad debe ser amparado *fervientemente* con un grado de cautela *sensiblemente* superior.

Debemos considerar *detalladamente* que la legislación exige una actitud *proactivamente* responsable (accountability), y esta responsabilidad se eleva cuando se trata de estudiantes que, *evidentemente*, tienen una capacidad menor para comprender las implicaciones y riesgos de compartir su información personal.

En nuestro centro, el tratamiento de datos para cumplir con la función docente y orientadora está *estrictamente* legitimado por ley. Esto incluye *naturalmente* datos identificativos y académicos. *Particularmente*, debemos ser *extremadamente* cuidadosos cuando tratamos categorías especiales de datos, como la información relativa a la salud, *especialmente* aquella que es *necesariamente* relevante para gestionar alergias alimentarias en nuestros servicios de restauración. Adoptamos *diligentemente* medidas técnicas y organizativas adaptadas al riesgo para salvaguardar *adecuadamente* esta información sensible.

Respecto al consentimiento, la ley nos indica que los alumnos *válidamente* pueden consentir por sí mismos si han cumplido los 14 años. No obstante, cuando tratamos información que *manifiestamente* excede nuestra función educativa (como podría ser la publicación de fotografías en la web), la transparencia es *absolutamente* clave. Debemos informar, a principio de curso, tanto a los alumnos como a sus padres o tutores sobre el tratamiento de datos. Es *imprescindiblemente* importante que, al proporcionar esta información, el lenguaje sea *convenientemente* adaptado al nivel de comprensión de nuestros estudiantes más jóvenes, garantizando así que su consentimiento.

Finalmente, si empleamos tecnologías de vigilancia para garantizar la seguridad de personas e instalaciones, debemos ser *profundamente* respetuosos con su intimidad. La videovigilancia se usa *solamente* para cubrir la zona *mínimamente* imprescindible. La ley prohíbe *terminantemente* la instalación de cámaras en vestuarios o baños, y la

grabación en aulas solo se permite *excepcionalmente* ante un riesgo objetivo para los menores, *rigurosamente* fuera del horario lectivo.

IX. BIBLIOGRAFÍA

Agencia Española de Protección de Datos (AEPD)

Agencia Española de Protección de Datos. (2017). *Ayúdales a construir su futuro: Guía para Padres y Profesores*. Madrid, España: Autor.

Agencia Española de Protección de Datos. (2018). *Informe sobre la utilización por parte de profesores y alumnos de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas: Orientaciones para Centros Educativos*. Madrid, España: Autor.

Agencia Española de Protección de Datos. (s.f.). *Guía para centros educativos* (Guías Sectoriales AEPD I). Madrid, España: Autor.

Centro Integrado de Formación Profesional (CIFP) Hostelería y Turismo de Cartagena

CIFP Hostelería y Turismo de Cartagena. (s.f.). *Descripción CIFP Hostelería y Turismo Cartagena*. Cartagena, España: CIFP HT Cartagena.

Comunidad Autónoma de la Región de Murcia (CARM)

Consejería de Educación y Cultura de la Región de Murcia. (2017). *Instrucciones sobre el uso de videovigilancia en los centros docentes públicos no universitarios de la Comunidad Autónoma de la Región de Murcia*. Murcia, España: Autor.

Consejería de Educación y Formación Profesional de la Región de Murcia. (2025, 11 de septiembre). Orden de 8 de septiembre de 2025 por la que se regula el desarrollo de la estrategia digital en los centros docentes no universitarios sostenidos con fondos públicos de la Región de Murcia y se crea el sello de calidad digital LIBRE. *Boletín Oficial de la Región de Murcia*, 210, 23160–23176.

Secretaría General de la Consejería de Educación y Cultura de la Región de Murcia. (2019). *Resolución de la Secretaria General por la que se dictan Instrucciones para la gestión documental y organización de archivos de centros docentes públicos no universitarios de la Comunidad Autónoma de la Región de Murcia*. Murcia, España: Autor.