MESHER
CONSULTING DATA

Uso seguro de las plataformas educativas en la nube

Por Mesher Consulting Data

Las plataformas educativas en la nube no representan una herramienta neutra, pues permiten centralizar funciones como la gestión de aulas, tareas, comunicación, videoconferencia, almacenamiento y evaluación, implicando a su vez un tratamiento masivo y constante de datos personales de menores. Por otro lado, su implementación no puede calificarse como verdaderamente voluntaria para las familias y los alumnos, dado que el uso de la plataforma viene impuesto por la propia organización educativa al constituirse como el canal ordinario de trabajo para toda la comunidad escolar.

Claves a tener en cuenta

- ⚖️ Respeto a los derechos y libertades
- 📌 Determinación clara de la responsabilidad
- 📜 Base jurídica y limitación de finalidades
- 🔍 Evaluación de impacto y participación del DPD
- 🔎 Transparencia e información
- 📝 Contrato del encargado y control de subencargados
- 🌍 Garantías en transferencias internacionales
- 🛡️ Protección de datos desde el diseño y por defecto
- 🔐 Seguridad de la información
- 👤 Garantía de los derechos de las personas
- ✔️ Conclusión práctica para el centro

Respeto a los derechos y libertades

Este primer principio significa que toda decisión sobre la plataforma debe tomarse pensando antes en la protección del alumnado que en la comodidad tecnológica o en el coste económico. La gratuidad o popularidad de una herramienta no justifica una rebaja de garantías. Para el centro, esto exige valorar siempre si el uso previsto puede afectar de manera intensa a menores y si existe un riesgo desproporcionado para su privacidad, su autonomía o su exposición digital.

Determinación clara de la responsabilidad

El centro no puede actuar como si toda la responsabilidad recayera en el proveedor. Debe saberse quién es responsable del tratamiento y en qué supuestos el proveedor actúa solo como encargado o pasa a tratar datos para fines propios. Esta distinción es esencial, porque cambia las obligaciones de información, control y legitimación. Si la administración educativa pone la plataforma a disposición del centro, también debe quedar por escrito qué corresponde a cada nivel.

Base jurídica y limitación de finalidades

La función educativa legitima los tratamientos necesarios para enseñar, evaluar, tutorizar o comunicarse con familias, pero no abre la puerta a cualquier uso adicional. Servicios accesorios, publicidad, analítica comercial, perfilado o funcionalidades ajenas al aprendizaje no deben activarse en un entorno institucional dirigido a menores. El centro debe verificar que los datos solo se usan para finalidades educativas concretas y que los datos generados automáticamente por la plataforma no se explotan para intereses propios del proveedor sin cobertura jurídica suficiente.

Evaluación de impacto y participación del DPD

Antes de implantar la plataforma debe realizarse una evaluación de impacto en protección de datos, porque se trata de un tratamiento a gran escala de datos de menores mediante tecnologías en la nube. Esa evaluación no puede ser un trámite formal: debe analizar riesgos, roles, finalidades, categorías de datos, flujos internacionales y medidas de mitigación. El delegado de protección de datos debe intervenir desde el inicio, no cuando la plataforma ya está contratada y en funcionamiento.

Transparencia e información

Alumnado, familias y profesorado tienen derecho a entender de forma clara qué ocurre con sus datos. No es suficiente remitirles a políticas de privacidad extensas, genéricas o dispersas en varios enlaces. El centro debe asegurarse de que la información sea accesible, comprensible y específica: qué datos se recogen, con qué finalidad, durante cuánto tiempo, quién puede recibirlos y qué tratamientos realiza el propio proveedor para fines propios.

Contrato de encargo y control de subencargados

La relación con el proveedor debe apoyarse en un contrato de encargo sólido, comprensible y estable, que permita al centro conocer exactamente qué tratamiento se realiza y bajo qué condiciones. No son aceptables cambios unilaterales del proveedor en aspectos esenciales del servicio ni contratos fragmentados que impidan mantener la trazabilidad jurídica. Además, el centro debe conocer qué subencargados intervienen, dónde están ubicados y con qué funciones, y conservar capacidad real de oposición y de verificación.

Garantías en transferencias internacionales

No basta con que el proveedor afirme que cumple el RGPD: el centro debe saber si los datos salen del Espacio Económico Europeo, por qué motivo y con qué garantías. Deben analizarse todos los flujos, incluidos los derivados de subencargados y de datos recogidos automáticamente por la plataforma. Cuando no existan garantías suficientes o no se pueda determinar con claridad el recorrido de los datos, la recomendación práctica es no autorizar el uso de la herramienta.

Protección de datos desde el diseño y por defecto

La plataforma debe venir configurada, desde el inicio, para tratar solo los datos imprescindibles. Los servicios adicionales no vinculados a la finalidad educativa deben estar desactivados por defecto, y el centro debe revisar de forma periódica que esa configuración se mantiene. También debe extremarse la prudencia con imágenes, vídeos y posibles categorías especiales de datos, estableciendo protocolos internos claros para evitar usos excesivos o improcedentes.

Seguridad de la información

La seguridad no se reduce a tener contraseñas o copias de respaldo. Deben existir medidas técnicas y organizativas proporcionadas al riesgo, teniendo en cuenta que se trata de datos de menores y de un servicio esencial para la actividad educativa. El contrato debe prever la notificación rápida de brechas de seguridad, y en el ámbito público deben observarse además las exigencias del Esquema Nacional de Seguridad cuando resulten aplicables.

Garantía de los derechos de las personas

El centro debe poder atender de manera efectiva los derechos de acceso, rectificación, supresión, limitación, oposición y no ser objeto de decisiones automatizadas. Esto exige procedimientos claros, coordinación con el proveedor y capacidad técnica real para ejecutar lo solicitado. Además, si una persona ejerce el derecho de oposición en los casos legalmente previstos, la respuesta no puede traducirse en una desventaja o discriminación en el acceso a la educación.

Conclusión práctica para el centro

El decálogo no debe leerse como una mera advertencia jurídica, sino como una guía de decisión. Antes de contratar, renovar o mantener una plataforma, el equipo directivo debería poder responder afirmativamente a estas preguntas: **sabemos qué datos trata, para qué se usan, quién responde por cada tratamiento, qué riesgos existen, qué medidas los reducen y qué información se ha dado a la comunidad educativa**. Si alguna de estas respuestas no está clara, la herramienta no debería implantarse sin una revisión previa.

Decálogo para el Uso Seguro de Plataformas Educativas Digitales

10 principios básicos de protección de datos para administraciones y centros docentes al contratar plataformas digitales.

Esta guía establece un marco de cumplimiento para el uso de servicios en la nube en entornos escolares. Se centra en el interés superior del menor y define las responsabilidades legales de los centros como responsables del tratamiento de datos frente a los proveedores tecnológicos.

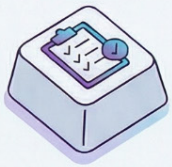
Gobernanza y Legitimación del Tratamiento

1. Interés Superior del Menor y Responsabilidad Proactiva

Las administraciones y centros son los responsables legales del tratamiento, priorizando siempre los derechos del menor.

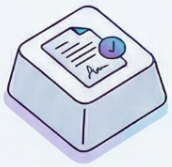
2. Misión en Interés Público vs. Fines Comerciales

El uso debe basarse en la función educativa, prohibiendo el tratamiento para fines publicitarlos o perfiles comerciales.



3. Evaluación de Impacto (EIPD) y Participación del DPD

Es obligatorio realizar una evaluación de rlesgos previa con el asesoramiento directo del Delegado de Protección de Datos.



4. Transparencia y Contratos de Encargo

Se requiere un lengueja ciaro para menores y contratos que impidan camblos unilaterales del proveedor.

Control Operativo, Seguridad y Derechos

5. Privacidad desde el Diseño y Seguridad (ENS)

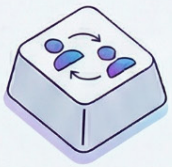
Las plataformas deben venir preconfiguradas con el mínimo de datos necesario y cumplir el Esquema Nacional de Seguridad.

6. Garantías Internacionales

Se deben validar las transferencias de datos fuera de Europa y asegurar el ejercicio de derechos.

7. Derechos de los Interesados (Acceso y Supresión)

Asegurar el ejercicio de derechos como el acceso y la supresión de datos.

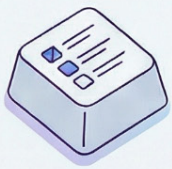


8. Claridad en los Roles del Proveedor

Encargado de tratamiento (servicios básicos) o Responsable (fines propios).

9. Tipos de Datas Claramente Definidos

Datos generados por el usuario vs. datos tecnicos recogidos automáticamente.



10. Diferenciación de Servicios

Diferenciar servicios educativos básicos de servicios adicionales u optativos.