

## EL RGPD UE 2016/679 EN APLICACIÓN

# Delegado de Protección de Datos: funciones, obligaciones y su impacto en el cumplimiento

El Delegado de Protección de Datos (DPD) es una figura esencial para garantizar el cumplimiento del Reglamento General de Protección de Datos (RGPD) y la LOPDGDD en las organizaciones. Su papel va más allá de una función formal, ya que supervisa, asesora y refuerza la cultura de privacidad en la empresa.

Las funciones del DPD están recogidas en el artículo 39 del RGPD. En primer lugar, debe informar y asesorar sobre las obligaciones legales en materia de protección de datos, ayudando a aplicar correctamente la normativa y evitando riesgos en la toma de decisiones.

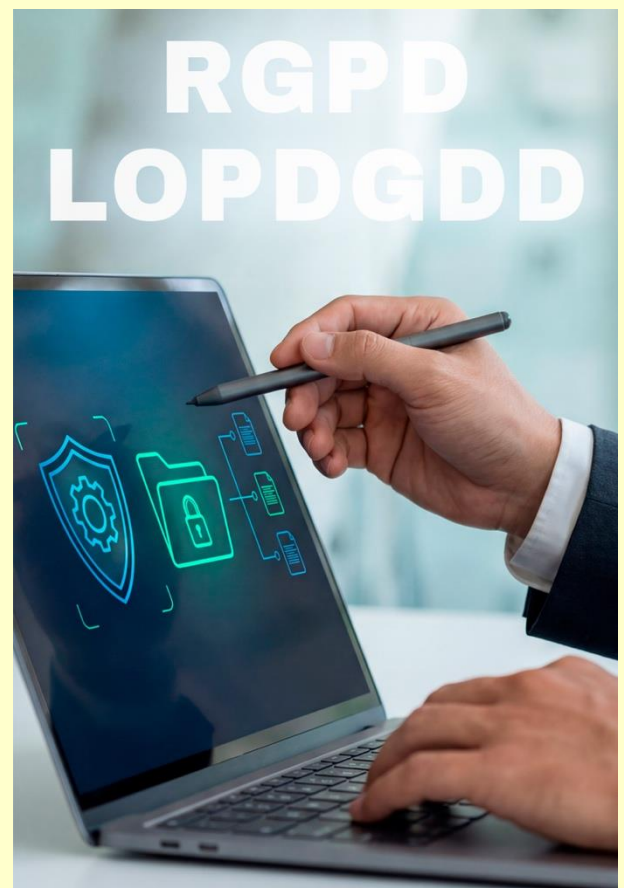
Además, debe supervisar el cumplimiento interno, revisando políticas, medidas de seguridad y formación del personal. No basta con disponer de documentación, sino que es necesario garantizar su aplicación efectiva.

Otra función esencial es el asesoramiento al responsable del tratamiento las evaluaciones de impacto en protección de datos (EIPD) cuando existen tratamientos de alto riesgo. También actúa como punto de contacto con la Agencia Española de Protección de Datos (AEPD), colaborando en inspecciones o consultas previas a la AEPD.

Por último, el DPD es el que asesora al responsable y atiende las peticiones de los interesados en el ejercicio de sus derechos.

### Contenido

1. Delegado de Protección de Datos: funciones, obligaciones y su impacto en el cumplimiento.
2. Incumplir una resolución de la AEPD supone una infracción muy grave en protección de datos.
3. Evaluación de impacto en Protección de datos: como identificar el alto riesgo según la AEPD.
4. Las Autoridades de Protección de Datos publican un decálogo de principios básicos para la contratación y el uso de plataformas educativas digitales.
5. Mecanismos de autenticación: cómo reducir ataques y accesos indebidos a los sistemas.



### IMPORTANTE

El DPD garantiza el cumplimiento, reduce riesgos legales y fortalece la confianza, siendo clave en la gestión responsable de datos personales.

## SANCIONES DE LA AEPD

# Incumplir una resolución de la AEPD supone una infracción muy grave en protección de datos

La Agencia Española de Protección de Datos, en su resolución [PS-004956-2024](#), sanciona a una entidad por un incumplimiento especialmente relevante: no ejecutar una resolución firme dictada por la propia autoridad de control.

El caso se inicia tras la reclamación de un interesado que ejerció su derecho de acceso ante la entidad sin obtener una respuesta adecuada. Ante esta situación, la AEPD estimó la reclamación y dictó una resolución en la que obligaba expresamente a la entidad a facilitar la información solicitada o, en su caso, a denegarla de forma motivada dentro de un plazo concreto.

El elemento determinante del expediente no es solo la falta inicial de respuesta, sino que la entidad ignoró completamente la resolución de la AEPD. A pesar de haber sido notificada correctamente y de recibir requerimientos adicionales para acreditar su cumplimiento, la entidad no realizó ninguna de las actuaciones reclamadas:

- no atendió el derecho del interesado.
- no justificó su negativa.
- no respondió a la AEPD.

Estas conductas suponen un incumplimiento directo de los poderes correctivos de la AEPD, vulnerando el artículo 58.2.c) del RGPD, tipificado como infracción muy grave.

Como consecuencia, la entidad fue sancionada con una multa de 225.000 euros, reducida a 180.000 euros por pago voluntario.

El responsable del tratamiento debe implantar medidas de seguridad efectivas, proporcionales al riesgo, y acreditarlas ante la autoridad de control.



### IMPORTANTE

La entidad incumplió durante más de un año una resolución firme de la AEPD, pese a recibir múltiples requerimientos de cumplimiento.

## LA AEPD ACLARA

# Evaluación de impacto en Protección de datos: como identificar el alto riesgo según la AEPD

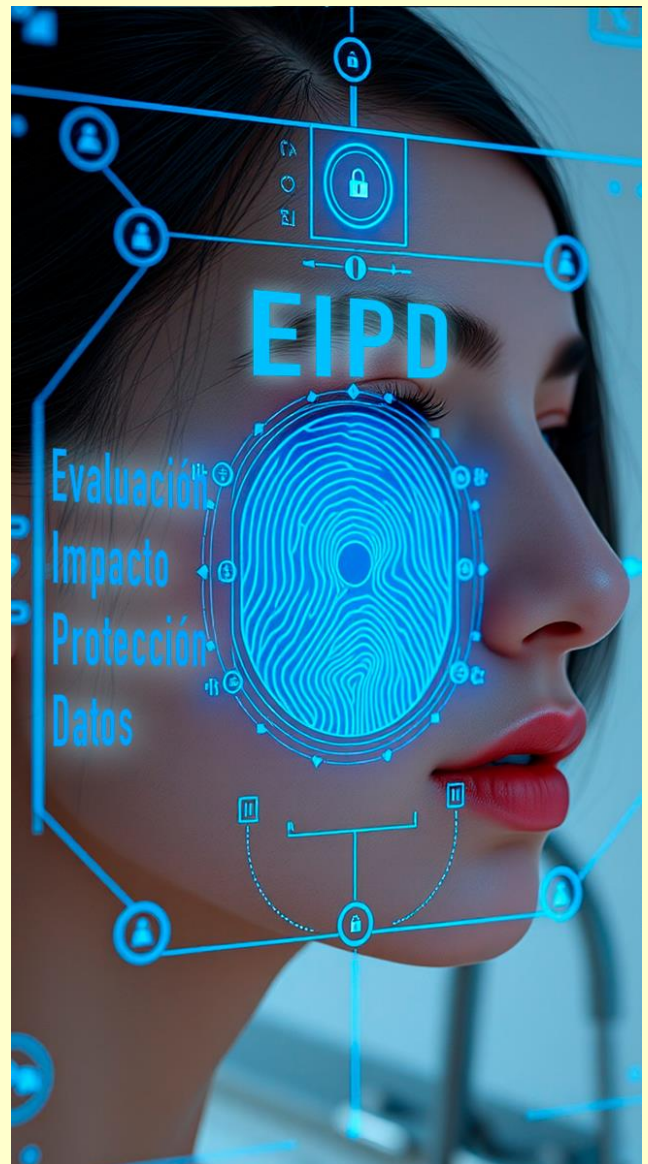
La Agencia Española de Protección de Datos (AEPD) [publicó una lista de tratamientos](#) que requieren obligatoriamente una Evaluación de Impacto en Protección de Datos (EIPD), en cumplimiento del artículo 35.4 del RGPD.

En este documento se concreta cuándo un tratamiento puede implicar un alto riesgo para los derechos y libertades de las personas, obligando al responsable a realizar un análisis previo.

La lista identifica supuestos en los que el riesgo se presume elevado. Entre ellos, los tratamientos que implican evaluaciones sistemáticas de aspectos personales, especialmente cuando incluyen perfiles o decisiones automatizadas. También se consideran de alto riesgo los tratamientos a gran escala de categorías especiales de datos, como los relativos a la salud o datos biométricos.

Asimismo, la AEPD incluye, entre otros, el uso de tecnologías nuevas o innovadoras, así como la observación sistemática de espacios públicos, como ocurre con determinados sistemas de videovigilancia.

Desde una perspectiva de cumplimiento, esta lista no es orientativa, sino vinculada a la obligación de evaluar riesgos antes de iniciar el tratamiento. El responsable debe analizar si su actividad encaja en estos supuestos y, en tal caso, realizar una EIPD que permita identificar, valorar y mitigar los riesgos, conforme al principio de responsabilidad proactiva del RGPD.



### IMPORTANTE

Cuando un tratamiento cumple dos o más criterios de riesgo, se presume alto impacto y resulta obligatoria la realización de una EIPD.

## ACTUALIDAD CIBERSEGURIDAD Y PRIVACIDAD

# Las Autoridades de Protección de Datos publican un decálogo de principios básicos para la contratación y el uso de plataformas educativas digitales

Fuente: [AEPD](#)

(23 de marzo de 2026).

La Agencia Española de Protección de Datos (AEPD), la Autoridad Catalana de Protección de Datos (APDCAT), la Autoridad Vasca de Protección de Datos (AVPD) y el Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA) han elaborado [un decálogo de cumplimiento en el que recogen de forma sistemática los principios básicos de protección de datos a tener en cuenta por las administraciones educativas y las empresas que ofrecen plataformas de servicios educativos en la nube](#), en la contratación y el uso de las mismas. Estos principios resultan también aplicables a los centros educativos públicos, concertados y privados.

La utilización de estas plataformas educativas digitales presenta riesgos y desafíos específicos para la protección de datos personales. Esto ha dado lugar a pronunciamientos por parte de las Autoridades de Protección de Datos, en el marco de sus respectivas competencias, dirigidos tanto a administraciones educativas como a centros docentes. Uno de los objetivos de estas orientaciones es **promover el cumplimiento proactivo de la normativa**, protegiendo a las personas usuarias de estos servicios en primer término, conformando un espacio de confianza y seguridad jurídica.

Las Autoridades de protección de datos destacan en el documento que las plataformas educativas digitales permiten al alumnado, profesorado y familias interactuar y colaborar con fines educativos, además de desarrollar las competencias digitales y facilitar la función docente. No obstante, también exponen que **la implantación de estas plataformas entraña una responsabilidad importante**, ya que supone un tratamiento masivo de datos personales entre los que destaca de forma muy relevante la información relativa a menores, que exige una protección específica.

Puede ver información relacionada en el siguiente enlace:

[Principios básicos para la contratación y uso de plataformas educativas digitales por las administraciones educativas y centros docentes.](#)

## EL PROFESIONAL RESPONDE

# Mecanismos de autenticación: cómo reducir ataques y accesos indebidos a los sistemas

Durante años, la contraseña ha sido el principal mecanismo de autenticación. Sin embargo, quienes trabajamos en ciberseguridad sabemos que, por sí sola, ya no es suficiente. La realidad de los incidentes diarios demuestra que una credencial comprometida puede abrir la puerta a todo un sistema si no existen barreras adicionales.

Por ello, tanto la ISO/IEC 27001 como el Esquema Nacional de Seguridad recomiendan avanzar hacia modelos de autenticación más sólidos, especialmente la autenticación multifactor. Combinar algo que el usuario sabe, algo que posee y, en determinados casos, algo que es, eleva de forma notable el nivel de protección frente a ataques automatizados y accesos no autorizados.

En entornos reales, esto se traduce en el uso de certificados digitales, aplicaciones de generación de códigos temporales o dispositivos físicos de seguridad. El ENS es especialmente claro al exigir factores reforzados en accesos remotos o a información sensible, mientras que la ISO 27001 subraya la necesidad de que estas decisiones se basen en un análisis de riesgos previo.

La clave no está en elegir soluciones coherentes con el contexto y el impacto potencial. Una autenticación bien diseñada no solo protege sistemas: protege el negocio, a las personas y la confianza depositada en la organización.



### IMPORTANTE

Las contraseñas no bastan; la autenticación multifactor, basada en riesgos, refuerza la seguridad y protege los sistemas.