

EL RGPD UE 2016/679 EN APLICACIÓN

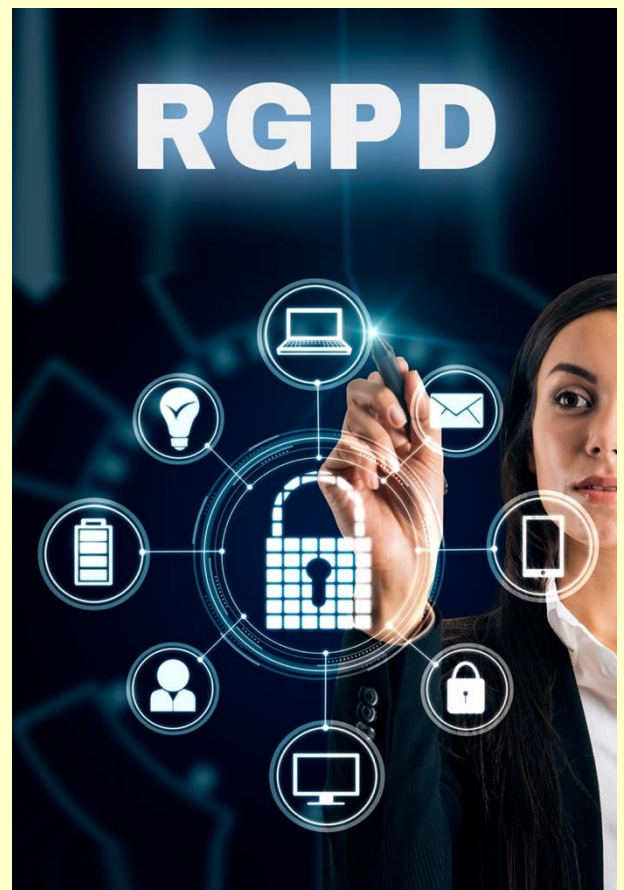
Principio de independencia y medios necesarios para el ejercicio de las funciones del DPD

El Delegado de Protección de Datos constituye una figura esencial dentro del modelo de cumplimiento en materia de protección de datos personales. Su posición no es solamente consultiva o formal, sino un elemento estructural del sistema de responsabilidad proactiva previsto en el RGPD. El artículo 38 del RGPD establece con claridad que el responsable y el encargado del tratamiento deberán garantizar que el DPD participe “de forma adecuada y en tiempo oportuno” en todas las cuestiones relativas a la protección de datos, lo que implica su intervención desde las fases iniciales de cualquier tratamiento que pueda generar riesgos para los derechos y libertades de los interesados.

La norma refuerza, además, su independencia funcional al disponer que el DPD “no recibirá ninguna instrucción” en el desempeño de sus funciones, que “no será destituido ni sancionado” por el ejercicio de las mismas y que “rendirá cuentas directamente al más alto nivel jerárquico” de la organización. Estas garantías no son meramente formales, sino que aseguran la objetividad y autonomía de su criterio técnico. Asimismo, el RGPD exige que se le proporcionen los recursos necesarios, acceso a la información y formación adecuada, evitando cualquier conflicto de intereses.

Contenido

1. Principio de independencia y medios necesarios para el ejercicio de las funciones del DPD.
2. Multada una empresa hotelera con 40.000 euros por dejar datos personales a la vista en el control de accesos.
3. *Fingerprinting* y cumplimiento normativo: lo que los responsables del tratamiento deben tener en cuenta (II).
4. La Agencia publica unas orientaciones sobre Inteligencia Artificial agéntica desde la perspectiva de protección de datos.
5. Nuevo escenario estratégico de la ciberseguridad en España.



IMPORTANTE

El Delegado de Protección de Datos debe actuar con independencia, recursos suficientes y autonomía, garantizando una supervisión eficaz del cumplimiento normativo del RGPD.

SANCIONES DE LA AEPD

Multada una empresa hotelera con 40.000 euros por dejar datos personales a la vista en el control de accesos

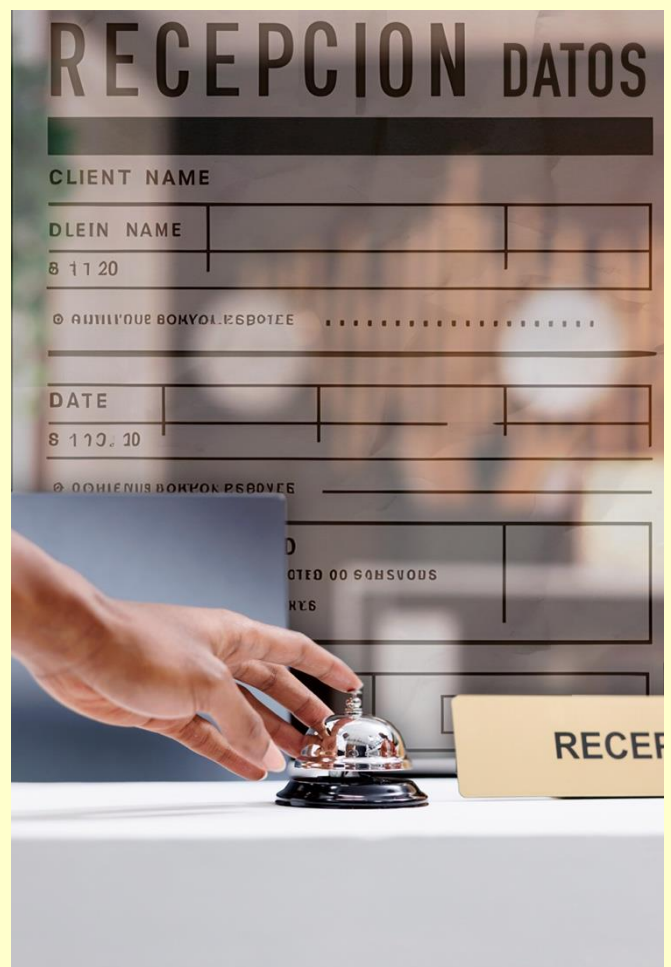
La Agencia Española de Protección de Datos, en su resolución [PS-00077-2024](#), sanciona a una empresa gestora de un complejo hotelero por no cumplir con el principio de confidencialidad de datos.

La reclamación, presentada inicialmente ante la autoridad de control sueca y posteriormente trasladada a la AEPD por su carácter transfronterizo, denunciaba la exposición indebida de datos personales en un complejo hotelero.

En concreto, se puso de manifiesto que el personal de seguridad, durante las labores de control de acceso a la comunidad de propietarios y al hotel, mantenía a la vista listados impresos con información personal de propietarios y huéspedes (nombre, apellidos, país, DNI, pasaporte) quedando accesibles a terceros y pudiendo incluso ser fotografiadas. Asimismo, quedó acreditado que la empresa de seguridad actuaba como encargada del tratamiento, bajo las instrucciones de la gestora hotelera, responsable del tratamiento en su condición de administradora de la comunidad. En el expediente se concluyó que la gestora del hotel no había implantado medidas técnicas y organizativas adecuadas para garantizar la confidencialidad de la información.

La conducta fue calificada como vulneración del principio de integridad y confidencialidad del artículo 5.1.f) del RGPD, imponiéndose una sanción económica de 40.000 euros y la obligación de adoptar medidas correctivas.

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



IMPORTANTE

La responsabilidad del tratamiento incluye el control efectivo sobre los encargados y la adopción de medidas reales, no meramente formales, para garantizar la confidencialidad de los datos personales.

LA AEPD ACLARA

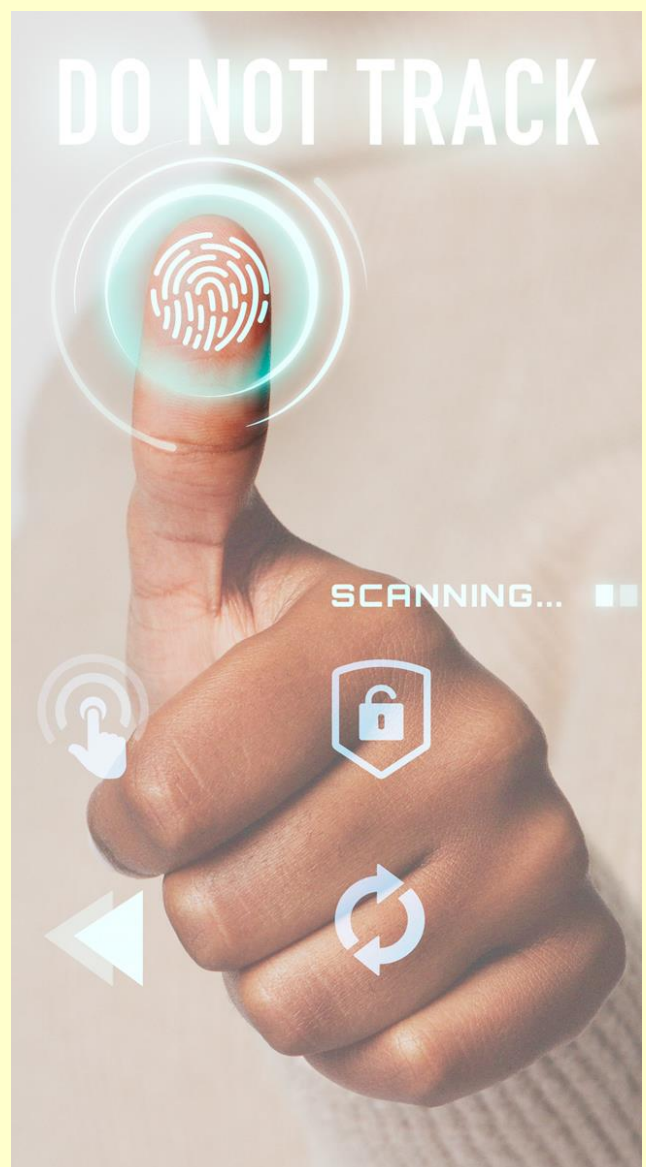
Fingerprinting y cumplimiento normativo: lo que los responsables del tratamiento deben tener en cuenta (II)

El [estudio de la AEPD](#) pone de relieve prácticas preocupantes, como ignorar la señal *Do Not Track* o utilizar estas técnicas sin evaluación previa de riesgos. Desde una perspectiva de cumplimiento, esto supone una vulneración del principio de responsabilidad proactiva.

El uso de técnicas de huella digital del dispositivo exige a los responsables del tratamiento una especial diligencia. El RGPD es claro: si mediante el *fingerprinting* se puede identificar directa o indirectamente a una persona, estamos ante un tratamiento de datos personales y deben cumplirse todas las garantías legales.

Pensemos, por ejemplo, en una web que utiliza *fingerprinting* para personalizar publicidad. Aunque el usuario no introduzca su nombre ni acepte cookies, su comportamiento puede ser seguido de forma persistente. En estos casos, no basta con alegar una finalidad técnica: es necesario informar de manera clara y obtener un consentimiento válido antes de iniciar el tratamiento.

Entre las buenas prácticas recomendadas destacan la minimización de datos, la limitación de técnicas intrusivas y la integración de la privacidad desde el diseño. Aquí, el papel del Delegado de Protección de Datos resulta clave, ya que puede ayudar a valorar si el uso del *fingerprinting* es realmente proporcional o si existen alternativas menos invasivas.



IMPORTANTE

El *fingerprinting* exige consentimiento previo, análisis de riesgos, y aplicación efectiva del principio de responsabilidad proactiva.

ACTUALIDAD CIBERSEGURIDAD Y PRIVACIDAD

La Agencia publica unas orientaciones sobre Inteligencia Artificial agéntica desde la perspectiva de protección de datos

Fuente: [AEPD](#)

(18 de febrero de 2026).

La Agencia Española de Protección de Datos (AEPD) ha publicado unas orientaciones sobre [Inteligencia Artificial agéntica desde la perspectiva de protección de datos](#). La IA agéntica son sistemas de IA capaces no solo de responder a preguntas, sino de **interactuar de forma autónoma para conseguir los objetivos**. La capacidad que tienen los sistemas de IA agéntica para operar con autonomía, enriquecerse con la información del entorno digital y ejecutar tareas complejas introduce **nuevos retos en muchos aspectos, entre ellos relacionados con la protección de datos personales**.

Estas orientaciones abordan las cuestiones de protección de datos que pueden surgir cuando **responsables y encargados de tratamiento** deciden utilizar sistemas de IA agéntica para implementar tratamientos de datos personales. La Agencia subraya que el conocimiento de esta tecnología, en continua evolución, es clave para adoptar decisiones informadas cuando se pretende implementarla en tratamientos de datos personales. En particular, defiende **aprovechar de forma proactiva las oportunidades que ofrece la IA agéntica** para una mayor protección de datos desde el diseño.

El texto se estructura realizando inicialmente una breve descripción de qué son los sistemas IA agénticos. A continuación, se analizan los aspectos de cumplimiento de la normativa de protección de datos, las posibles vulnerabilidades de estos sistemas y las amenazas específicas que pueden aprovecharse de esas vulnerabilidades. Finalmente, el documento enumera un conjunto de posibles medidas que podría adoptar un responsable o encargado para garantizar el cumplimiento de la normativa de protección de datos y reducir o eliminar los impactos que presenta la IA agéntica en relación con los derechos y libertades de las personas.

Puede ver información relacionada en el siguiente enlace:

[INTELIGENCIA ARTIFICIAL AGÉNTICA DESDE LA PERSPECTIVA DE PROTECCIÓN DE DATOS](#)

EL PROFESIONAL RESPONDE

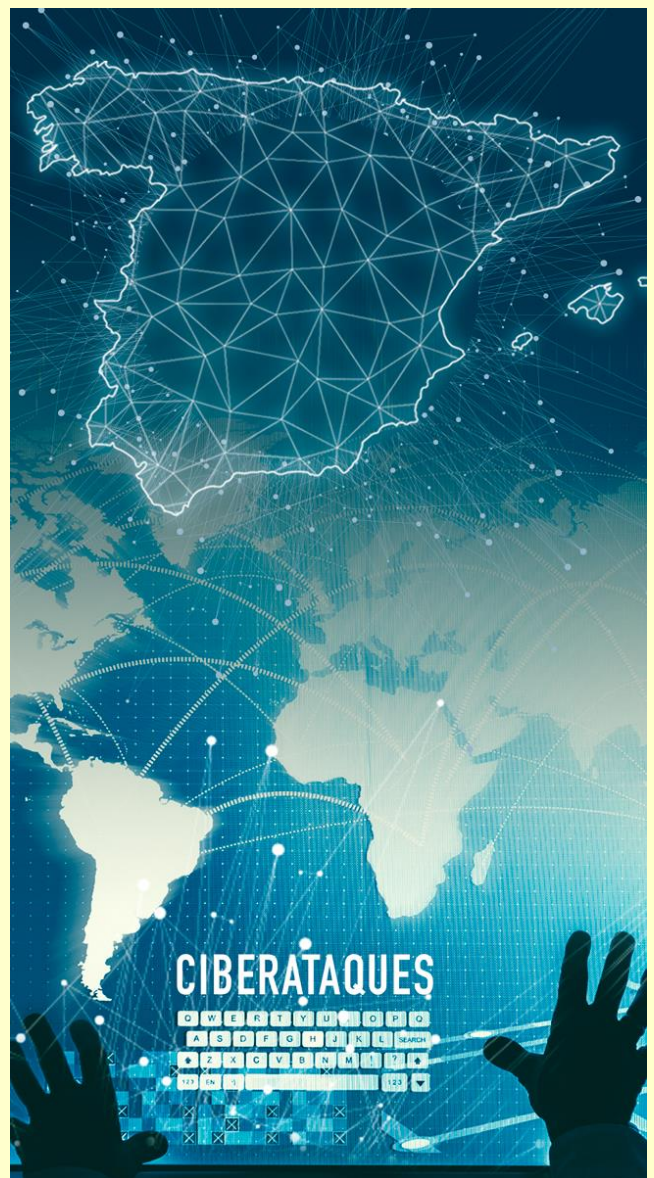
Nuevo escenario estratégico de la ciberseguridad en España

[El Balance de Ciberseguridad 2025 de INCIBE](#)

no deja lugar a dudas: estamos ante un escenario de riesgo creciente que exige una respuesta estratégica y madura por parte de empresas y ciudadanos. Los 122.223 incidentes gestionados —un 26% más que en 2024— y los 237.028 sistemas vulnerables identificados evidencian que la superficie de exposición digital continúa ampliándose a gran velocidad.

El fraude online, con 45.445 casos, se consolida como la principal amenaza, mientras que el phishing suma 25.133 incidentes. Estos datos no son meras estadísticas: reflejan una sofisticación cada vez mayor en las técnicas de ingeniería social y una explotación sistemática de la confianza digital. El cierre de 4.600 dominios fraudulentos demuestra que la respuesta institucional existe, pero la prevención debe reforzarse desde la base.

Especial atención merece el *malware*, con 55.411 incidentes registrados, incluidos 392 ataques de *ransomware*. Que el 85% de los sistemas infectados estén vinculados a dispositivos *IoT* confirma algo que venimos advirtiendo desde hace años: la conectividad sin seguridad es una vulnerabilidad estructural. Por último, hacer referencia a las 142.767 consultas atendidas por la Línea de Ayuda de INCIBE que reflejan una mayor concienciación social.



IMPORTANTE

La ciberseguridad es un pilar estratégico para el gobierno corporativo y garantía de la continuidad del negocio.