

## EL RGPD UE 2016/679 EN APLICACIÓN

### El derecho de acceso en la práctica: obligaciones, plazos y errores más frecuentes

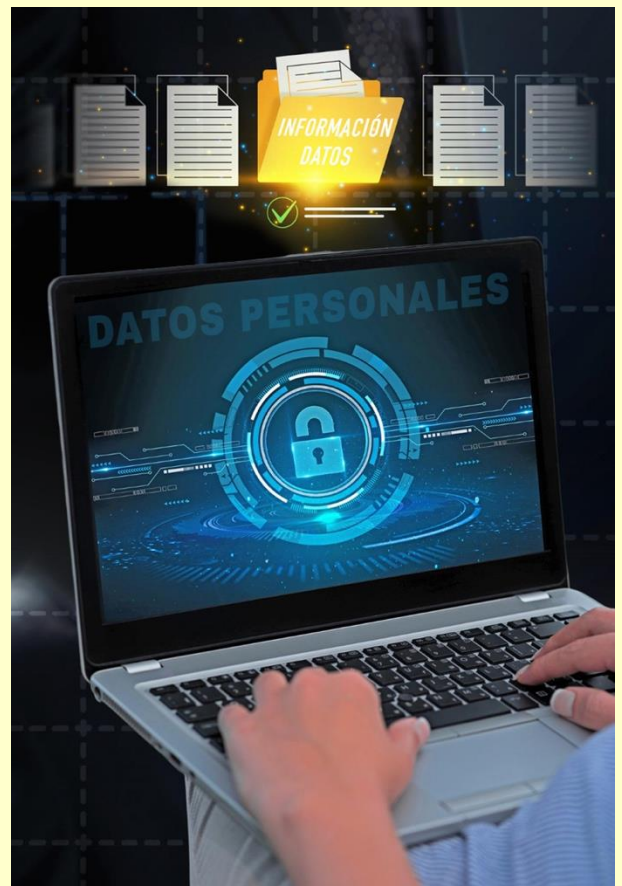
El derecho de acceso es uno de los pilares fundamentales del RGPD, ya que permite al interesado conocer si una organización está tratando sus datos personales y obtener información sobre dicho tratamiento. En la práctica, es también uno de los derechos que más reclamaciones genera ante la Agencia Española de Protección de Datos, especialmente cuando las respuestas son incompletas, genéricas o se producen fuera de plazo.

Tanto la AEPD como el Comité Europeo de Protección de Datos insisten en que el responsable del tratamiento debe facilitar una respuesta clara, comprensible y realmente útil para el interesado. No basta con confirmar que existen datos; es necesario informar sobre las finalidades del tratamiento, categorías de datos tratados, destinatarios, plazo de conservación y existencia de decisiones automatizadas, entre otros aspectos.

El ejercicio del derecho de acceso puede realizarse por cualquier medio que permita acreditar la solicitud. Una vez recibida, el responsable dispone de un mes para responder, pudiendo ampliar el plazo únicamente en supuestos complejos y siempre justificándolo. Además, la información debe entregarse de forma segura y verificando previamente la identidad del solicitante.

#### Contenido

- 1.El derecho de acceso en la práctica: obligaciones, plazos y errores más frecuentes.
- 2.Multa de 30.000 € por realizar videovigilancia con control laboral sin informar al personal laboral.
- 3.Datos biométricos, genéticos y tratamientos masivos: escenarios donde la EIPD resulta imprescindible (II).
- 4.La Agencia recibió más de 30.000 reclamaciones en 2025, un 64% más que el año anterior.
- 5.ENS y sector privado: adaptación y oportunidades en la gestión de la seguridad de la información.



#### IMPORTANTE

Gestionar correctamente el derecho de acceso exige procedimientos internos claros, trazabilidad documental y criterios jurídicos sólidos en cada respuesta.

## SANCIONES DE LA AEPD

# Multa de 30.000 € por realizar videovigilancia con control laboral sin informar al personal laboral

La Agencia Española de Protección de Datos, en su resolución [PS-00264-2024](#), sanciona a una entidad del sector industrial por un tratamiento ilícito de datos personales mediante un sistema de videovigilancia laboral con captación de sonido.

La reclamación ante la AEPD tiene su origen en la instalación de cámaras de videovigilancia en las oficinas, almacén y fábrica que, además de captar imágenes de los trabajadores durante su jornada laboral, permitían registrar conversaciones y sonidos sin informar adecuadamente a los empleados.

El reclamante denunciaba, asimismo, la existencia de una cámara situada junto a un puesto de trabajo desde la que podían escucharse conversaciones privadas, sin que dicha circunstancia apareciera reflejada ni en la cartelería informativa ni en la documentación entregada al personal.

De la investigación se constata que la entidad reclamada utilizaba cámaras con capacidad de grabación de audio y que únicamente había informado de la existencia de cámaras de seguridad para la vigilancia de las instalaciones, omitiendo tanto la finalidad de control laboral como la captación de sonido.

La AEPD sancionó a la entidad porque no acreditó riesgos específicos que justificaran la grabación de conversaciones en el entorno laboral ni la proporcionalidad de esta medida intrusiva.

El tratamiento de datos personales solo es válido cuando existe una causa legítima que justifique su utilización de forma proporcional y necesaria.



### IMPORTANTE

El RGPD obliga a informar de forma clara, previa y transparente sobre el tratamiento, finalidad, base jurídica y derechos del interesado.



## ACTUALIDAD CIBERSEGURIDAD Y PRIVACIDAD

# La Agencia recibió más de 30.000 reclamaciones en 2025, un 64% más que el año anterior

Fuente: [AEPD](#)

(6 de mayo de 2026). La Agencia Española de Protección de Datos (AEPD) ha presentado hoy su Memoria de actuación 2025, que recoge con detalle las cifras de gestión, un balance de las actuaciones realizadas, las acciones de colaboración e inspección puestas en marcha, los informes y procedimientos más relevantes del año, un análisis de las tendencias normativas y los desafíos para la privacidad, tanto en un plano nacional como internacional.

El año 2025 ha estado marcado por el inicio de una nueva presidencia y adjuntía en el organismo y la publicación del [Plan estratégico 2025-2030](#), que fija las líneas clave de actuación de la autoridad orientándose al fomento de la innovación responsable y la defensa de la dignidad en la era digital teniendo en cuenta los retos tecnológicos emergentes.

La Memoria refleja que en 2025 **se presentaron ante la Agencia 30.931 reclamaciones, lo que supone el número de reclamaciones más alto de la historia de esta Autoridad**, con un incremento del 64% respecto al año anterior. Este aumento evidencia un mayor conocimiento y concienciación de la ciudadanía tanto sobre sus derechos como de la posibilidad de reclamar ante la Agencia. A esta cifra se suman 1.118 casos (+36%) transfronterizos procedentes de otras autoridades de control europeas y 14 casos iniciados por iniciativa propia del organismo. Ello supone un total de **32.063 entradas de nuevos casos a Inspección**, destacando que no sólo supone un incremento exorbitado, sino que estos **son cada vez más complejos debido al impacto de las nuevas tecnologías** y las amenazas crecientes que suponen para la privacidad, y los procedimientos transfronterizos que deben llevarse a cabo en coordinación con otras autoridades europeas.

Tanto estas cifras como la mayoría de las recogidas en la Memoria en todas las subdirecciones y divisiones reflejan una carga de trabajo creciente que no se ha visto acompañada por un incremento proporcional en la evolución de la plantilla. En este sentido, la Agencia recoge en su Plan estratégico 2025-2030 la apuesta por una supervisión apoyada en la tecnología que prioriza la acción en las áreas de mayor impacto sobre la dignidad y los derechos de las personas, con medidas como la adopción de la inteligencia artificial con garantías y el desarrollo de sistemas avanzados de supervisión

Puede ver información relacionada en el siguiente enlace:

[Memoria Anual 2025](#)

## EL PROFESIONAL RESPONDE

# ENS para empresas: claves prácticas para entender el Esquema Nacional de Seguridad (I)

El aumento de los ciberataques contra organismos públicos y proveedores tecnológicos ha convertido la ciberseguridad en una prioridad estratégica. Por ello, a lo largo de los próximos boletines iremos abordando de forma práctica los principales aspectos del Esquema Nacional de Seguridad (ENS), analizando sus obligaciones, medidas técnicas y criterios de cumplimiento para organizaciones públicas y empresas privadas.

En este contexto, el Real Decreto 311/2022 regula el Esquema Nacional de Seguridad (ENS), el marco normativo que establece los requisitos mínimos de seguridad para garantizar la protección de la información y los servicios electrónicos en el sector público español.

El ENS tiene como objetivo crear un entorno seguro en el uso de medios electrónicos. Su aplicación afecta no solo a las administraciones públicas, sino también a empresas tecnológicas, proveedores *cloud*, consultoras IT y terceros que prestan servicios al sector público.

La normativa se basa en principios esenciales, como la seguridad integral, la gestión continua de riesgos, la prevención, la vigilancia y la capacidad de respuesta ante incidentes.

El cumplimiento del ENS también guarda una estrecha relación con el cumplimiento de otras normativas, como el RGPD.



### IMPORTANTE

El ENS garantiza seguridad, continuidad y confianza digital, convirtiéndose en un requisito esencial para organizaciones que gestionan información y servicios públicos.