



Uso de la inteligencia artificial. Protección de datos

La incorporación de sistemas de inteligencia artificial (IA), especialmente los denominados **agentes inteligentes**, está transformando la forma en que las organizaciones gestionan procesos y tratan datos personales. Estos sistemas, basados en modelos avanzados, permiten automatizar tareas, tomar decisiones y operar con cierto grado de autonomía, lo que aporta importantes beneficios en eficiencia y productividad.

En Escura, departamento de protección de datos, nos llegan un gran número de consultas sobre la inteligencia artificial.

Siendo este tema muy polémico y controvertido, la propia agencia ha publicado una guía titulada "Inteligencia artificial agéntica desde la perspectiva de protección de datos".

Hemos confeccionado un resumen en relación con los principales puntos de la guía, que no obstante usted encontrara íntegramente en el pie de la circular.

El uso de la inteligencia artificial implica nuevos retos en materia de protección de datos, ya que estos sistemas pueden acceder, procesar y compartir grandes volúmenes de información, incluyendo datos personales, tanto dentro de la organización como con terceros.

Los Principales riesgos que pone de manifiesto la guía son los siguientes:

- **Acceso excesivo a datos:** posibilidad de tratar más información de la necesaria, vulnerando el principio de minimización.
- **Falta de control y transparencia:** dificultad para entender cómo se toman decisiones automatizadas.
- **Interacción con múltiples servicios externos:** aumento del riesgo de transferencias de datos no controladas.
- **Almacenamiento y uso de memoria:** acumulación de datos personales sin una adecuada gestión o limitación temporal.
- **Autonomía de los sistemas:** ejecución de acciones sin intervención humana directa, con posibles impactos en los derechos de las personas.

TODAS LAS CIRCULARES DE ESCURA EN NUESTRO BLOG - <https://www.escura.com/es/blog/>

- **Errores y decisiones automatizadas:** riesgo de resultados incorrectos o sesgados que afecten a los interesados.

En la guía se destacan como las principales obligaciones para las organizaciones:

El uso de IA en el tratamiento de datos personales exige cumplir con la normativa vigente, especialmente el Reglamento General de Protección de Datos (RGPD).

- **Definir claramente responsabilidades** (responsable y encargado del tratamiento).
- **Garantizar la transparencia** en el uso de la IA y en el tratamiento de datos.
- **Asegurar una base jurídica válida** para el tratamiento.
- **Respetar los derechos de las personas** (acceso, rectificación, supresión, etc.).
- **Evaluar riesgos** mediante análisis y, en su caso, evaluaciones de impacto.
- **Controlar decisiones automatizadas**, especialmente cuando tengan efectos significativos.

Por todo ello, recomendamos adoptar las siguientes medidas par un uso seguro y conforme con la normativa:

- Aplicar el principio de **protección de datos desde el diseño y por defecto**.
- Limitar el acceso a datos y aplicar políticas **de minimización y control**.
- Establecer mecanismos de **supervisión humana efectiva**.
- Gestionar adecuadamente la **memoria y conservación de datos**.
- Implementar sistemas de **trazabilidad, auditoría y control**.
- Garantizar la **seguridad técnica y organizativa** de los sistemas.
- Formar y concienciar a los equipos en el uso responsable de la IA.

Para acceder a la guía puedes consultar el enlace.

[Consulta la guía.](#)

