



Cómo proteger la información corporativa ante el uso de la IA

La inteligencia artificial ha dejado de ser una materia desregulada con la progresiva aplicación del Reglamento (UE) 2024/1689 de Inteligencia Artificial ("Reglamento de IA"), ya abordado en anteriores circulares (["Reglamento Europeo de Inteligencia Artificial: obligaciones a partir del 2 de agosto de 2026"](#)), y el nuevo Reglamento (UE) 2026/1744, conocido como el Ómnibus Digital sobre la IA.

Con esta nueva regulación y el uso actual que se le está dando a la IA, las compañías que utilicen este tipo de herramientas se enfrentan a múltiples riesgos a tener en cuenta en sus sistemas de compliance penal: fuga de información confidencial y secretos empresariales, vulneración de la propiedad intelectual o industrial (propia o de terceros), toma de decisiones erróneas sin supervisión humana, entre otros.

Una de las primeras tareas a realizar en materia de compliance será la revisión del mapa de riesgos penales, es decir, llevar a cabo una nueva valoración de los riesgos corporativos, pues muchas empresas se habrán encontrado con nuevas vulnerabilidades que, en el pasado, o no existían o no se tenían en cuenta y en la actualidad son de un nivel elevado.

Después de determinar los riesgos que tiene cada entidad, deben adoptarse medidas de prevención o protocolos para reducir y, en su caso, eliminar estas vulnerabilidades. Un elemento básico es indicar, ya sea en el protocolo de uso de la IA o similar, qué tipo de archivos, datos personales sensibles o incluso sitios web, no están autorizados por la entidad para usarlos con la IA.

Documentos como planes estratégicos, listados de clientes, planos de productos que todavía no se han introducido en el mercado, entre otros, no deben introducirse en los sistemas de IA. En todo caso, y si se llevara a cabo por una determinada necesidad, debe hacerse una evaluación de lo que ello puede comportar para la compañía, pues ya ha habido entidades que, a través de un uso negligente de estas herramientas, han permitido una fuga de información considerable.

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



Las circulares de **Escura** tienen carácter meramente informativo, resumen disposiciones que por carácter limitativo propio de todo resumen pueden requerir de una mayor información. La presente circular no constituye asesoramiento legal.

©La presente información es propiedad de **Escura** quedando prohibida su reproducción sin permiso expreso.

La limitación de accesos a determinados archivos o servidores por unas personas que tengan unas credenciales de gran nivel es otro de los aspectos a considerar para evitar que se puedan materializar los riesgos anteriormente mencionados.

Todo ello, ha de complementarse con una formación constante a la plantilla para concienciar de lo que un mal uso puede comportar.

En **Escura** disponemos de un área de Compliance especializada en el asesoramiento a las empresas para identificar y evaluar los riesgos asociados al uso de la inteligencia artificial, así como a implantar las medidas necesarias para reducir vulnerabilidades, garantizar el cumplimiento normativo y minimizar riesgos legales.



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