

#4

Septiembre 2024

Como preservar la privacidad y los secretos empresariales en el contexto de la IA ¿Puede una IA en instancia empresarial preservar información para un grupo reducido de personas de la empresa?

Por Emilio Tovar



Desde la popularización de la inteligencia artificial en los últimos meses, ha surgido la inquietud sobre los datos utilizados para entrenar los algoritmos de inteligencia artificial:

👉 **¿se están filtrando secretos empresariales a algoritmos que ponen a disposición del público en general o de nuestros competidores el conocimiento acumulado durante décadas?**

👉 **¿Es posible que lo que hemos conocido como el “know-how” que dicho de una manera más sencilla es el saber como hacer las cosas se encuentre disponible para una gran masa de personas haciéndonos perder nuestra competencia diferencial?**

Ya hemos conocido que algunas grandes empresas han detectado que algunos de sus conocimientos más preciados han acabado en IAs de uso generalista y que eso las ha llevado a crear su propia instancia de conocimiento IA.

Algunas de las medidas que desde el Consejo de Administración debemos asegurar que se establecen son aquellas relativas a la existencia de las Políticas y de los Modelos de Gobierno que aseguren la privacidad y la seguridad de la información, la realización de las auditorías de acceso a la información y del uso indebido de los datos, y la formación y capacitación de los empleados en las políticas específicas de la empresa en relación con esta materia.

También es importante que como consejeros tengamos la seguridad de que los contratos que se suscriben incluyen los acuerdos de confidencialidad necesarios y especialmente cuando hay

compartición de información con consultores y proveedores externos que pudieran ser fuente de una fuga de información.

La empresa debe cumplir de modo estricto las regulaciones y leyes aplicables en materia de privacidad y protección de datos, como GDPR y otras normativas.

Samsung Electronics prohibió el uso de ChatGPT y otras herramientas de IA Generativa en mayo de 2023 después de conocer que uno de sus ingenieros había subido a ChatGPT código propiedad de Samsung Electronics ante el temor de que el código pudiera ser utilizado por su competencia: Microsoft y Google a través de OpenAI, la compañía propietaria de ChatGPT en la que Microsoft y Google detentan participaciones empresariales. A algunos la medida pudo parecerles alarmista pero la realidad es que la dirección de Samsung Electronics estaba ejecutando las acciones correctas protegiendo la propiedad intelectual de la compañía.

Hoy en día, muchas compañías se enfrentan al dilema de seguir progresando en la utilización y la monetización de la IA Generativa y dudan si utilizar instancias públicas o crear instancias privadas que en general suelen tener un mayor coste. Desde los Consejos de Administración, debemos transmitir a la empresa que como consejeros nuestra recomendación es primar la privacidad y la protección de la propiedad intelectual y que por ello es altamente recomendable la utilización de instancias privadas que la mayor parte de los grandes actores en el área de la IA Generativa proporcionan.

Otras grandes compañías como JP Morgan han restringido el uso de ChatGPT a sus empleados y Amazon advirtió también a sus empleados para que no alimentarán con información confidencial o código propiedad de la compañía a ChatGPT.

La clave no es el prohibir, la clave es al contrario, definir un uso adecuado de la IA Generativa que permita que nuestra empresa no se quede rezagada respecto a la competencia, desde el Consejo de Administración debemos asegurar que se definen las políticas adecuadas para que la IA Generativa sea una herramienta crucial para el desarrollo de nuevas capacidades que permitan adelantar a la competencia y que generen un entorno empresarial que facilite la reducción de costes y el aumento de los ingresos.

Una vez más, las nuevas tecnologías, implican cambios en las empresas a nivel organizacional, de talento, de tecnología y de organización de los datos.

Debemos asegurar que disponemos del talento necesario en nuestra empresa y como suele suceder con las nuevas tecnologías será muy conveniente incorporar talento del exterior. La organización debe dar cabida en una primera fase a un grupo de expertos que promuevan el uso correcto de la IA Generativa en la empresa y que posteriormente en una etapa de madurez permeará a toda la organización haciendo innecesaria la continuación de este grupo de expertos que mirando hacia atrás veremos como una herramienta para la movilización y la gestión del cambio en la organización. Los datos son fundamentales para alimentar nuestros modelos de IA y para ello es importante que la empresa haya racionalizado los datos, y su almacenamiento que será un paso previo para las cargas de datos en los entornos de nuestra IA para el entrenamiento de los algoritmos de IA. Nuestra organización de tecnología necesitará también disponer de un grupo de especialistas en IA capaces de gestionar y parametrizar las instancias de IA Generativa

que aun siendo instancias privadas dentro de una nube pública necesitarán a este grupo para que facilite que esté disponible esta capacidad en nuestra organización.

En cuanto al propio Consejo de Administración debemos incorporar el debate de la IA dentro de nuestro compromiso ESG asegurando que se cumplen las políticas de sostenibilidad también en el marco de la IA Generativa.

Hablábamos antes de Talento en la empresa, pero también es conveniente que el Consejo de Administración sea formado en IA Generativa y que se incorporen nuevos consejeros con conocimientos de IA que ayuden al Consejo en las tomas de decisiones relacionadas con la IA.

En cuanto a gobernanza, no parece que sea necesaria la creación de una comisión de IA en el Consejo de Administración, pero si el que haya un punto recurrente en la agenda del Consejo de Administración que permita a los consejeros tomarle el pulso a la implantación y el uso de la IA Generativa en la empresa.

Y volviendo al título de nuestro artículo,

👉 **¿todas estas medidas y actuaciones van a permitir preservar la privacidad y los secretos empresariales?**

💡 Desde luego la situación será mucho mejor con estas medidas que si no se hubieran tomado y por eso nuestra recomendación es aplicarlas tanto en la empresa como en el propio Consejo de Administración. Y sin más, solo cabe añadir que no debemos temer a la IA Generativa del mismo modo que no se debió temer en el siglo XIX a la máquina de vapor o a los vehículos automóviles y que aquellos que apostaron en aquel momento por una adopción temprana fueron líderes en sus sectores empresariales y del mismo modo aquellas empresas que apuesten por la IA Generativa serán líderes en sus sectores.

Temas relacionados: #innovación #IA #estrategia #organización #consejos #buengobierno



Emilio Tovar

CIBG - Comisión de Innovación

Industrial Engineer. Digital Transformation Program PADDB+ at The Valley Business Digital School. CPIM Certificate in Production and Inventory Control by the American Production and Inventory Control Society, (APICS).