GIRONA NOTICIES.COM
+ Periodisme

DLTCode lanza recomendaciones para un uso responsable de la inteligencia artificial en las empresas

Actualidad Empresarial | 20/05/2026 | 00:00

Google ha confirmado un primer caso documentado en el que ciberdelincuentes han hecho uso de la inteligencia artificial para descubrir una vulnerabilidad de software desconocida para poder explotarla y lanzar ataques masivos.

Empresas y trabajadores aún desconocen que compartir documentos con la IA puede comprometer información sensible de toda la organización.

Desde DLTCode lanzan una serie de recomendaciones para un uso responsable de la inteligencia artificial dentro de las empresas.

¿Puede la IA organizar y lanzar ciberataques autónomos a empresas y ciudadanos de a pie? Recientemente Google ha confirmado un primer caso documentado en el que ciberdelincuentes han hecho uso de la inteligencia artificial para descubrir una vulnerabilidad de software desconocida para poder explotarla y lanzar ataques masivos. Aunque fue bloqueado antes de su uso, este hecho marca un hito y la “punta del iceberg” en cuanto a cómo los ciberdelincuentes impulsan sus ciberataques, pero también supone un primer paso hacia las operaciones cibernéticas más autónomas. Desde DLTCode empresa especializada en ciberseguridad, formación y tecnología Deep Tech basada en IA y adherida al Grupo Armora, avisan de la importancia de adoptar medidas de seguridad dentro de las empresas a la hora de hacer uso de la IA para la ejecución de las tareas.

Ataques a empresas más rápidos y sofisticados

Hasta no hace mucho lanzar un ciberataque requería de preparación y altos conocimientos técnicos. Sin embargo, el uso de la IA ha cambiado este paradigma. Y es que los nuevos modelos de ataque permiten a los ciberdelincuentes automatizar tareas que antes realizaban manualmente como la búsqueda de vulnerabilidades, generación de malware, creación de campañas de phishing personalizadas, códigos maliciosos o ataques ya a gran escala. Esto ha permitido que los ataques sean cada vez más sofisticados, más rápidos y con mayor alcance. Y esto no acaba aquí, los expertos alertan ya de la aparición de agentes autónomos capaces de ejecutar campañas cibernéticas completas con una mínima intervención humana.

Las empresas no cuentan con protocolos de acceso y uso de la IA

Desde hace unos años y, con especial relevancia en 2025 y 2026, se ha observado un aumento significativo de la fuga de datos empresariales, pero también provenientes de las instituciones públicas. Por ello es preciso poner en énfasis cómo los empleados hacen uso de las herramientas a su alcance de IA y en la falta de información y protocolos de seguridad de las empresas ante su uso.

Hoy en día la gran mayoría de trabajadores hacen uso de la IA en su entorno laboral y, en

ocasiones, desde sus cuentas personales. Estas interacciones incluyen, a veces, datos sensibles de la empresa como contratos, código fuente, datos de clientes o documentación interna si ser conscientes del riesgo que esto supone tanto para las empresas como para los propios empleados. Como consecuencia, hacer un mal uso de la IA se está convirtiendo en un factor clave en las brechas de seguridad y la fuga de datos sensibles corporativos. De hecho, muchos trabajadores desconocen que compartir documentos con la inteligencia artificial puede comprometer información sensible de toda la organización.

Consejos para un uso responsable de las empresas

“El uso de la inteligencia artificial por parte de las empresas y sus trabajadores plantea retos crecientes en términos de control, seguridad y gestión de la información. Por ello, resulta fundamental establecer políticas y medidas comunes que regulen su utilización dentro de la organización. En este contexto, la formación y la concienciación continua de los empleados adquieren un papel clave para fomentar una cultura sólida de ciberseguridad, promover un uso responsable de la IA y garantizar la protección adecuada de los datos sensibles con los que trabaja la empresa”, afirma Fernando Mairata, CEO de DLTCode y presidente del Grupo Armora.

Para conseguirlo desde DLTCode recomiendan:

Establecer políticas claras a la hora de compartir información confidencial en herramientas públicas y gratuitas de IA sin garantías de seguridad.

Definir un catálogo de herramientas de IA evaluadas por la organización desde el punto de vista de la ciberseguridad, privacidad y cumplimiento normativo.

Gestionar el acceso a herramientas de IA bajo unos mismos criterios y limitar su uso en función de cada área o departamento.

La inteligencia artificial debe actuar como una herramienta de apoyo y nunca como sustituto de la supervisión humana.

Alinear las políticas internas de IA en función de los nuevos marcos regulatorios que vayan surgiendo en materia de transparencia, gestión del riesgo y protección de datos.

Por todo y como resumen, para garantizar un uso seguro y responsable de la inteligencia artificial, es preciso definir una política corporativa clara que regule el uso de estas herramientas dentro de la organización. Esto implica proporcionar a los empleados directrices y mecanismos que les permitan identificar riesgos asociados al uso no autorizado de IA, prevenir fugas de información y asegurar el cumplimiento normativo. Asimismo, se considera esencial impulsar programas continuos de formación y concienciación en ciberseguridad, protección de datos y uso responsable de tecnologías de inteligencia artificial.

Sobre DLTCode:

DLTCode, perteneciente al Grupo Armora, es una empresa de servicios profesionales que opera en consultoría estratégica, ciberseguridad, formación y desarrollo de Deep Tech basado en IA. Está dirigida por un equipo experimentado de consultores líderes y expertos en diferentes materias relativas a la tecnología, ciberseguridad, regulación y normativa, innovación disruptiva y liderazgo digital. Proporciona y gestiona software de ciberseguridad de nueva generación que ayuda a proteger las organizaciones frente a la amenazas actuales y emergentes.

Autor: Redacció

https://gironanoticies.com/empresarial/296214-dltcode-lanza-recomendaciones-para-un-uso-responsable-de-la-inteligencia-artificial-en-las-empresas.htm