



La IA generativa se metió a las empresas: panorama y riesgos de esta tecnología

Ciudad de México, 6 de mayo de 2024.- En tan solo un año, el paisaje corporativo ha sido radicalmente transformado por la inteligencia artificial generativa. De acuerdo con datos de [Netskope](#), el uso de aplicaciones de IA generativa en actividades empresariales creció del 2% al 10% el año pasado.

Este aumento no solo refleja una adopción masiva, sino también la incorporación de desafíos únicos y oportunidades sin precedentes para las empresas. La irrupción comenzó con el boom de OpenAI y su producto estelar, ChatGPT, el cual agregó más usuarios que cualquier otra aplicación, incrementando su popularidad de un 0% a casi el 7% de todos los usuarios empresariales hacia finales de año.

Ante ello, la comunidad de ciberseguridad empresarial, habitualmente cautelosa, ha tenido que determinar rápidamente si estas aplicaciones cumplen un propósito comercial legítimo y, de ser así, cómo habilitar su uso de manera segura. Desde la perspectiva de Netskope, esto generalmente significa poner freno a la integración indiscriminada de estas aplicaciones hasta completar una revisión de seguridad adecuada, lo que propicie una adopción informada y segura.

- El escenario actual de la IA

Los chatbots, encabezados por ChatGPT, ya son una herramienta prevalente en el ámbito empresarial. A finales de este año, de acuerdo con Netskope, se registró que el 6.7% de los usuarios empresariales interactuaron al menos una vez al mes con dicha aplicación, posicionándose como el chatbot más popular; mientras que Google Bard sigue detrás con solo un poco más del 10% de la base de usuarios de ChatGPT.

Estos chatbots, proyecta la compañía, continuarán ganando terreno por su versatilidad para apoyar funciones empresariales como la redacción de reportes y la recopilación de información.

En paralelo, los asistentes de IA más especializados, como los de escritura de código y programación, también están incrementando su popularidad. Grammarly, por ejemplo, se destaca como el segundo software de IA generativa más popular, utilizado por el 3.1% de los usuarios empresariales, con alternativas como QuillBot y Wordtune también entre los diez primeros.

Tabnine, que ayuda a los programadores a escribir código de manera más eficiente, es un ejemplo de cómo estos asistentes especializados están integrándose cada vez más en las herramientas comunes de escritura y programación, lo cual se espera que impulse aún más su adopción durante 2024.



- **Cinco riesgos clave de la IA generativa**

1. Seguridad de datos: Con la integración de IA generativa en flujos de trabajo corporativos, se elevan significativamente los riesgos relacionados con la seguridad de datos. El acceso no regulado a estas herramientas puede exponer información sensible a amenazas externas. La implementación de controles de acceso a aplicaciones y el uso de un enfoque Zero Trust para el acceso a las redes empresariales se vuelve clave.

2. Cumplimiento normativo: La utilización de IA en procesos empresariales debe alinearse con las normativas de protección de datos vigentes. Las empresas deben asegurarse de que el uso de estas tecnologías no infrinja regulaciones legales, lo cual podría acarrear sanciones o daños reputacionales.

3. Dependencia tecnológica: La rápida adopción de estas herramientas puede crear una dependencia peligrosa. La falta de diversificación en herramientas y procesos puede hacer a las empresas vulnerables a fallas en servicios específicos.

4. Gestión del cambio: Integrar IA generativa requiere cambios importantes en los procesos y en la cultura empresarial. La gestión efectiva de estos cambios es crucial para evitar resistencias internas y maximizar los beneficios de la tecnología.

5. Privacidad del usuario: Con el aumento de la interacción entre usuarios y aplicaciones de IA, la privacidad se convierte en un tema crítico. Es fundamental implementar políticas que protejan la información personal de los empleados y clientes que interactúan con estos sistemas.

Según las proyecciones de Netskope Threat Labs para 2024, si bien el número total de usuarios de aplicaciones de IA en las empresas se incrementará de manera menos acelerada que en 2023, la actividad de los usuarios fuera de la oficina será más intensa. Esto sugiere una tendencia hacia la optimización y un aprovechamiento más profundo de estas tecnologías para fines recreativos.

Este panorama nos ofrece una visión integral del crecimiento continuo y la evolución de la inteligencia artificial en el entorno empresarial, señalando tanto las oportunidades de integración como los desafíos a superar para una adopción más amplia y eficiente.

Acerca de Netskope

Netskope es la compañía líder mundial en SASE que ayuda a las organizaciones a aplicar los principios de confianza cero (zero trust) y las innovaciones de IA/ML para proteger los datos y defenderse de las ciberamenazas. Rápida y fácil de usar, la plataforma Netskope proporciona acceso optimizado y seguridad en tiempo real para personas, dispositivos y datos en cualquier lugar. Netskope ayuda a los clientes a reducir riesgos, acelerar el rendimiento y obtener una visibilidad inigualable de cualquier actividad en la nube, la web y las aplicaciones privadas. Miles de clientes confían en Netskope y en su potente red NewEdge para hacer frente a las amenazas cambiantes, los nuevos riesgos, los cambios tecnológicos, los cambios organizativos y de red, y los nuevos requisitos normativos. Para saber cómo Netskope ayuda a los clientes a estar preparados en su viaje SASE, visite <https://www.netskope.com/es/>