

## Desafío corporativo

### Es fundamental complementar la adopción de IA con una sólida estrategia de capacitación en ciberseguridad.

La importancia de mejorar la ciberseguridad en las empresas es más relevante que nunca en tiempos de Inteligencia Artificial (IA). La acelerada digitalización y el creciente uso de la IA en múltiples procesos corporativos han abierto nuevas oportunidades, pero también han incrementado la exposición a ciberataques más complejos y difíciles de detectar.

La transformación digital ha traído consigo un aumento en la cantidad de datos sensibles que las organizaciones manejan, lo que convierte a la ciberseguridad en una prioridad ineludible para garantizar no solo la protección de la información, sino también la continuidad del negocio.

Los "hackers" han evolucionado junto con la tecnología, utilizando herramientas sofisticadas para vulnerar sistemas y robar datos. La IA ha potenciado la capacidad de los atacantes para desarrollar malware inteligente, diseñar ataques de ingeniería social más persuasivos e incluso

automatizar campañas de phishing. Frente a esta realidad, las empresas deben adoptar un enfoque proactivo y adaptativo en sus estrategias de ciberseguridad, aprovechando precisamente la IA para mejorar sus defensas.

La IA puede ser un aliado poderoso al permitir la detección temprana de amenazas mediante el análisis en tiempo real de grandes volúmenes de datos. Esta tecnología facilita la identificación de patrones anómalos que podrían pasar desapercibidos para los enfoques tradicionales, permitiendo responder de manera más rápida y eficiente ante un posible incidente.

Además, esta herramienta permite automatizar tareas de rutina en la ciberseguridad, como la monitorización de redes o la actualización de políticas de seguridad, liberando así a los expertos para que se enfoquen en la toma de decisiones críticas y en la resolución de problemas más complejos.