

El equilibrio en la seguridad de la IA: del riesgo a la innovación

Guía del CISO para dominar el riesgo y el potencial de la IA

Basada en los resultados del *2025 Global GenAI Report* de NTT DATA





La creciente inversión en IA ya está transformando sectores enteros y afectando a la forma en que trabajamos.



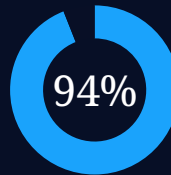
La adopción de la IA viene acompañada de nuevos riesgos de ciberseguridad.



Los CISO son conscientes de que necesitan una estrategia de ciberseguridad moderna e integrada.



de los CEO planean aumentar su inversión en IA generativa.



de los CEO aseguran que la IA generativa está haciendo que inviertan más en ciberseguridad.

¿Cómo pueden ayudar los CISO a sus organizaciones a aprovechar el potencial de la IA y, al mismo tiempo, proteger sus activos digitales de los riesgos que esta conlleva?

Deben buscar lo que llamamos el equilibrio en la seguridad de la IA.

1. ¿Tienes una estrategia de seguridad apta para la era de la IA?

La IA está transformando sectores enteros y potencia la ciberseguridad, no solo frente a las amenazas tradicionales, sino también frente a ciberataques con IA más sofisticados. No obstante, expone a las empresas a nuevos riesgos.

La IA generativa tiene potencial para transformar las empresas

95%

de los líderes de la C-suite afirman que la IA generativa está permitiendo un nuevo nivel de innovación en sus organizaciones.

En el top 3

Las organizaciones mencionan la mejora de la seguridad como uno de los tres principales beneficios que han observado tras sus implementaciones de IA generativa.



Pero el progreso conlleva nuevos riesgos de seguridad

88%

de las organizaciones se declaran muy preocupadas por los riesgos de seguridad asociados a la implementación de IA generativa.

Pero solo el 24%

de los CISO están totalmente de acuerdo en que su organización tiene un marco sólido para equilibrar el riesgo con la creación de valor.

2. Los riesgos relacionados con la IA

La rápida implementación de tecnologías de IA amplía la superficie de ataque e introduce nuevas y sofisticadas amenazas, por lo que la ciberseguridad debe ser una prioridad empresarial.

Los ataques con IA más habituales



Ataques antagónicos



Envenenamiento de datos



Sesgos algorítmicos

Gestión de datos, IA generativa y agentic AI



Aun así, los esfuerzos en este ámbito se están intensificando



La IA generativa conlleva nuevas vulnerabilidades de seguridad también por la complejidad de sus algoritmos avanzados.

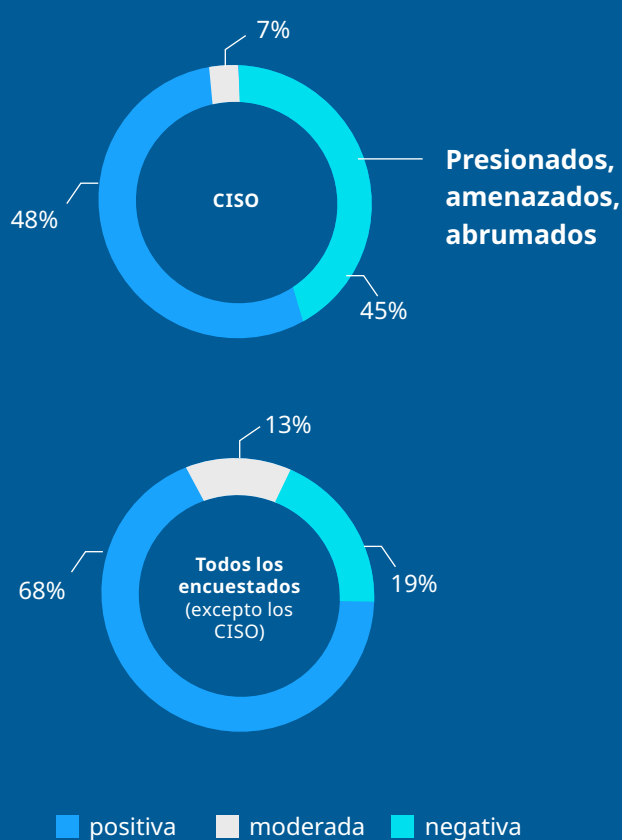


La Agentic AI trae consigo una nueva dinámica de trabajo y genera valor añadido, pero sin políticas de privacidad y gobernanza de datos bien definidas, su implementación acarrea riesgos considerables.

3. IA y seguridad: los CISO deben equilibrar las oportunidades y los riesgos

Existe una desconexión notable entre los objetivos estratégicos que fija la alta dirección y los obstáculos operativos a los que se enfrentan los CISO para preservar la responsabilidad, la seguridad, la privacidad y el cumplimiento en el despliegue de herramientas de IA.

Opinión predominante sobre la IA generativa



54%

de los CISO afirman que las directrices y políticas internas de sus empresas sobre uso responsable de la IA generativa no están claras, pero solo el 20% de los CEO comparten esta preocupación.

Solo el 38%

de los CISO están muy de acuerdo en que existe una alineación entre las estrategias de IA generativa y ciberseguridad de su organización. Sí lo piensa, en cambio, el 51% de los CEO.

El reto se complica...

71%

de los CISO afirman que los líderes de sus organizaciones no han marcado una dirección clara con respecto al uso responsable.

69%

admiten que sus equipos carecen de las habilidades necesarias para trabajar con esta tecnología en rápida evolución.

El desafío para el CISO es mayor cuando se carece de la infraestructura necesaria, o si esta está desactualizada o mal integrada

87%

creo que las infraestructuras antiguas obstaculizan el progreso de la IA generativa.

86%

afirman que los entornos en la nube son la infraestructura óptima para escalar la IA generativa de manera eficiente y rentable.

Aunque se mantienen cautos en su despliegue, los líderes de seguridad reconocen el valor de negocio de la IA generativa.

81%

de los líderes sénior con opiniones negativas sobre la IA generativa están de acuerdo, no obstante, en que esta tecnología mejorará la eficiencia y los resultados de negocio.

4. Cómo pueden los CISO gestionar los riesgos relacionados con la IA

Al elegir un partner de IA generativa, los CISO priorizan dos factores: la coinnovación y que la oferta de servicios de IA generativa sea end-to-end.

Áreas clave para gestionar los riesgos de la IA con un enfoque de varias capas



Mejorar la observabilidad



Desarrollar una política de seguridad de IA



Integrar seguridad por diseño



Garantizar la monitorización continua y la detección de amenazas



Gestión de riesgos y cumplimiento normativo



Fomentar la colaboración y la educación

Una estrategia de ciberseguridad potenciada por la IA y basada en plataformas refuerza las defensas de tu organización ante un panorama en el que las amenazas no dejan de evolucionar. Convierte la ciberseguridad en un activo estratégico que favorezca la innovación y te aporte ventaja competitiva.

NTT DATA permite a las organizaciones innovar de forma segura con soluciones impulsadas por IA y asegurar su crecimiento.

Contacta con un experto en IA y seguridad

Obtén el informe completo

Visita nttdata.com para saber más.

Somos un innovador global para servicios digitales tecnológicos y empresariales. Nuestro objetivo es ayudar a nuestros clientes en sus procesos de innovación, optimización y transformación para que puedan conseguir el éxito en sus proyectos. Somos Global Top Employer y contamos con expertos en más de 50 países, además de un sólido ecosistema de partners. NTT DATA forma parte del Grupo NTT.

