

Las 8 principales tendencias en ciberseguridad para 2026



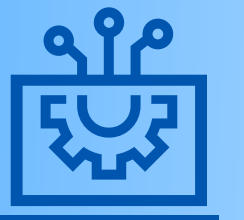
Proteger las nuevas fronteras

- 1 La IAM se adapta para habilitar y proteger los agentes de IA.
- 2 La criptografía poscuántica pasa del riesgo teórico a los planes de acción.
- 3 La IA agéntica requiere la supervisión de los programas.



Transformar la gobernanza

- 4 La IA y la ciberresiliencia redefinen las competencias del CISO.
- 5 La volatilidad regulatoria global impulsa esfuerzos de ciberresiliencia a gran escala.
- 6 La democratización de la IA impulsa la gobernanza colaborativa en seguridad de datos.



Normalizar la adopción de la IA

- 7 La IA generativa rompe las tácticas tradicionales de concienciación sobre ciberseguridad.
- 8 Las soluciones SOC impulsadas por IA desestabilizan las normas operativas.



Proteger las nuevas fronteras

- 1

La IAM se adapta para habilitar y proteger los agentes de IA.

El auge de la IA agéntica determina la aparición de nuevos retos que hacen aflorar brechas en algunos enfoques tradicionales de la IAM. Aunque hoy es posible aprovechar las prácticas fundamentales de la IAM aplicada a las máquinas, la mayor parte de las organizaciones aún presentan brechas de capacidad.
- 2

La criptografía poscuántica pasa del riesgo teórico a los planes de acción.

El ritmo acelerado de los proyectos de desarrollo de la computación cuántica aumenta la probabilidad de que la criptografía asimétrica convencional se vuelva insegura para 2030. Los responsables de ciberseguridad deben evaluar y adoptar lo antes posible las soluciones PQC, ya que poner remedio al problema requiere un esfuerzo sostenido durante varios años.



Transformar la gobernanza

- 3

La IA agéntica requiere la supervisión de los programas.

Los CEO y CIO siguen presionando para lograr una rápida adopción de la IA. A pesar de las inquietudes sobre la seguridad, los directores de seguridad de la información (CISO) no pueden permitirse ralentizar ni poner en pausa las iniciativas en materia de IA. Dado que aumentan los indicios de que se están adoptando agentes de IA no gestionados, los CISO deben ponerse rápidamente al día. Si no lo hacen, se arriesgan a automatizaciones “no autorizadas” que actúan con una excesiva capacidad en detrimento de la ciberseguridad requerida.
- 4

La IA y la ciberresiliencia redefinen las competencias del CISO.

El salto de la ciberprotección a la ciberresiliencia, junto con las necesidades urgentes en torno a la adopción y la protección ante la IA, están ampliando las responsabilidades de los CISO. Y este se extiende a la gobernanza de datos (protegiendo la IA en la sombra), las políticas en materia de IA (orientando los estándares de seguridad requeridos en la adopción de la IA), la privacidad y la gestión de la continuidad de negocio, además de la tecnología operativa o la seguridad de los sistemas ciberfísicos (CPS).
- 5

La volatilidad regulatoria global impulsa esfuerzos de ciberresiliencia a gran escala.

Los CISO se enfrentan a una compleja y creciente presión regulatoria a nivel global, que incluye las comunicaciones a la SEC, NIS2, DORA, la Ley de IA de la UE y la evolución de la legislación en APAC, echando por tierra cualquier esperanza de una gobernanza unificada. Si a esto se le suma el aumento de la agitación geopolítica y el auge del tecnonacionalismo, parece quedar claro que la ciberseguridad es actualmente un riesgo empresarial crítico que puede determinar la resiliencia de las organizaciones en todo el mundo.



Normalizar la adopción de la IA

- 7

La IA generativa rompe las tácticas tradicionales de concienciación sobre ciberseguridad.

La adopción acelerada de la IA generativa ha roto las tácticas tradicionales de concienciación sobre ciberseguridad y los esfuerzos de los CISO para reducir la exposición a riesgos de ciberseguridad. Los CISO deben pasar a programas de comportamiento y cultura de la ciberseguridad (SBCEP) para abordar las brechas específicas en las defensas provocadas por el uso de la “IA en la sombra” sin supervisión y por las técnicas de ataque potenciadas por IA generativa que son cada vez más difíciles de detectar para los empleados.
- 8

Las soluciones SOC impulsadas por IA desestabilizan las normas operativas.

Para adoptar la IA en el SOC con éxito, los líderes deben priorizar la mejora de las capacidades del personal en lugar de sustituir cargos. De esta forma se garantiza un buen funcionamiento de las operaciones a largo plazo, y, al mismo tiempo, se fomenta el desarrollo continuo de competencias. Mantener los procesos y cargos actuales sin adaptación provocará el fracaso de las organizaciones.

Descargo de responsabilidad. Estas tendencias no están enumeradas por orden de importancia.

Principales tendencias en ciberseguridad para 2026



Fuente: Gartner
© 2026 Gartner, Inc. o sus filiales. Todos los derechos reservados.

Insights prácticos y objetivos

Posiciona tu organización para el éxito. Consulta estos recursos y herramientas complementarios para líderes de ciberseguridad.

Insights

Gartner AI Hub

Explora los insights, los casos de uso y el asesoramiento experto sobre la IA en los que confían los directivos empresariales.

Más información ↗

Insights

Ciberseguridad e IA: mejora la seguridad y gestiona los riesgos

La expectación por la IA y las promesas de la ciberseguridad deben equilibrarse con la preocupación y los riesgos que conllevan. Estos son los aspectos en los que deberías enfocarte.

Más información ↗

Cómo ayudamos

Cómo colabora Gartner con los CISO

Descubre cómo proporcionamos los insights, el asesoramiento y las herramientas que necesitas para implementar tus principales prioridades estratégicas.

Más información ↗

Hoja de ruta

Crea una hoja de ruta de ciberseguridad resiliente para tu empresa

Crea una hoja de ruta de ciberseguridad resiliente, escalable y ágil.

Más información ↗

Hazte cliente ¿Ya eres cliente? Obtén acceso a más recursos en tu portal de cliente. [Inicia sesión](#)

[Obtén más información sobre Gartner para responsables de ciberseguridad](#)
[Síguenos en LinkedIn](#)

Fuente: Gartner
© 2026 Gartner, Inc. o sus filiales. Todos los derechos reservados. CM_GTS_4422300

Gartner