Licencias OnLine

TENDENCIAS

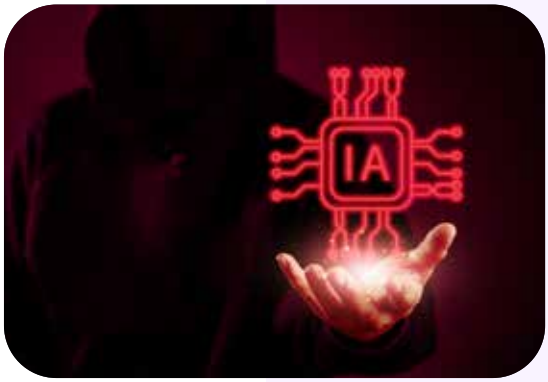
LOL 2027





Ciberseguridad en la era de la IA

La inteligencia artificial ingresó de lleno en la escena de la ciberseguridad.



Los atacantes la utilizan para:

- Acelerar el reconocimiento.
- Generar señuelos más convincentes.
- Automatizar partes de sus operaciones.

Los equipos de seguridad la incorporan para:

- Analizar más información.
- Detectar patrones.
- Investigar incidentes.
- Automatizar respuestas.

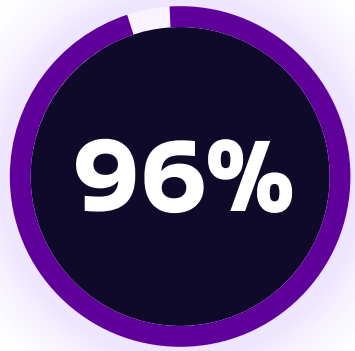


Del lado de las empresas, esto ya tiene consecuencias operativas concretas: los equipos tienen menos tiempo para detectar y contener un incidente.

Según un **estudio de EY** realizado entre 500 líderes senior de seguridad:



El 48% estima que **al menos una cuarta parte** de los incidentes de ciberseguridad sufridos por su organización durante el último año estuvo **habilitada por IA**.



El 96% considera que los ataques habilitados por IA representan una **amenaza significativa** para su organización.

Tendencia 1:
La velocidad obliga a automatizar.

01

Cada vez hay menos tiempo para detectar y contener un incidente.

¿QUÉ HACER? ▶▶ **Automatizar detección, priorización e investigación y reducir pasos manuales del SOC.**

Por eso, en 2027, la automatización será cada vez más importante en:



Escalar la automatización también exige condiciones. Sin datos confiables, la IA de seguridad pierde contexto.

IDC señala que las organizaciones que no prioricen datos de alta calidad y preparados para IA tendrán dificultades para escalar GenAI y soluciones basadas en agentes, con una pérdida de productividad estimada en **15%** en 2027.

Así, la calidad de los datos deja de ser un requisito técnico previo y pasa a ser una condición para escalar IA.

Al mismo tiempo, un agente que recibe información incompleta sobre activos, identidades, eventos o vulnerabilidades puede automatizar una decisión incorrecta a mayor velocidad.

Por eso cobrará cada vez más relevancia integrar la telemetría, no solo como fuente de información para el SOC, sino como una condición para que la automatización pueda operar con contexto.

Tendencia 2:
La IA amplía el perímetro de seguridad.

02

¿QUÉ HACER? ▶▶ **Inventariar las herramientas, modelos y agentes de IA, identificar qué datos utilizan y definir qué permisos y accesos necesitan.**

La superficie que deben proteger los equipos de seguridad se está ampliando:
Se suman otras capas asociadas a la IA.

redes · endpoints · aplicaciones · nube · datos · identidades · terceros

\+

modelos · agentes · copilotos · prompts · datos de entrenamiento

En la práctica, esto obliga a ampliar el inventario. Una estrategia de seguridad para 2027 necesita saber no solo qué dispositivos y aplicaciones existen, sino también:



¿Qué sistemas de IA están activos?

¿Qué datos utilizan?

¿Qué agentes pueden ejecutar acciones y con qué permisos?

Esto también implica detectar el uso de IA que ocurre fuera de los procesos formales. El concepto de **shadow AI** cobra relevancia porque dificulta conocer:

Qué herramientas están utilizando los empleados.

Qué información procesan

Qué aplicaciones tienen acceso a ella.



50%

De los esfuerzos empresariales de respuesta a incidentes de ciberseguridad se concentrarán en incidentes que involucren aplicaciones de IA construidas a medida en 2028.

(Fuente: Gartner)

Tendencia 3:
La identidad se vuelve más difícil de verificar.

03

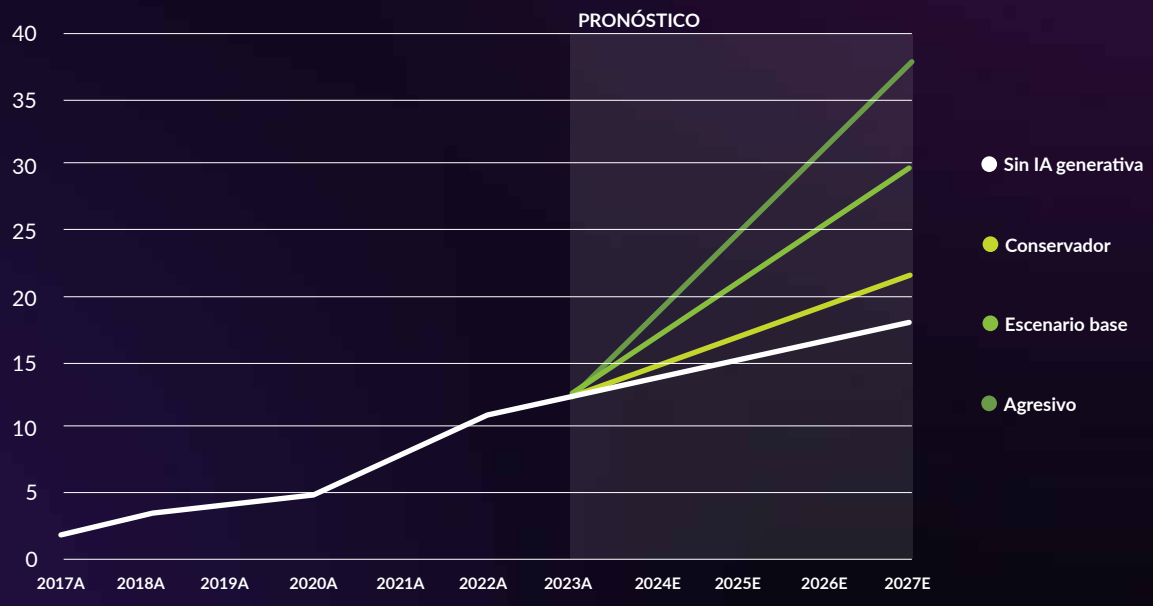
Deepfakes e identidades sintéticas complicarán la autenticación tradicional.

¿QUÉ HACER? ▶▶ **Reforzar la autenticación, incorporar controles de identidad adaptativos y plantear verificaciones adicionales para operaciones sensibles.**

En 2027 se potenciará otra tendencia que ya se observa: la fabricación de identidades con información real y contenido generado por IA. La expansión de la IA está haciendo más difícil distinguir entre una interacción legítima y una identidad construida artificialmente.

En tal sentido, el **Centro de Servicios Financieros de Deloitte** estima que el fraude habilitado por IA generativa en Estados Unidos podría pasar **de US$12.300 millones en 2023 hasta US$40.000 millones en 2027**, con un crecimiento anual compuesto del **32%**.

Ante semejantes cifras es preciso recordar que los deepfakes ya deberían ser considerados un problema para el costo del negocio.



80%

De las organizaciones experimentará ataques de phishing que utilicen identidades sintéticas en 2027. La técnica combina información personal real y contenido generado por IA para construir identidades falsas que aparentan ser legítimas.

(Fuente: IDC)

En consecuencia, ya no alcanzará con validar solamente usuario y contraseña. Dicho esto, las organizaciones necesitarán evaluar el contexto de la interacción y el riesgo de la operación.

Tendencia 4:
La IA empieza a actuar.

04

Los agentes pasan de recomendar acciones a ejecutarlas.

¿QUÉ HACER? ▶▶ **Definir permisos, autonomía, supervisión, trazabilidad y mecanismos de reversión.**

El avance de la IA agéntica introduce un nuevo problema porque, a medida que estos sistemas incorporan capacidad para **investigar incidentes**, **modificar configuraciones** o **ejecutar acciones**, surge la necesidad de **establecer límites** y **definir esquemas de gobernanza**.

De esta manera, la seguridad deja de ser una colección de herramientas. **Cloud**, **endpoints**, **identidades**, **datos**, **IA** y **terceros** están cada vez más conectados y las empresas avanzan hacia:



Arquitecturas integradas → Servicios gestionados → Monitoreo continuo

Oportunidad en seguridad de IA por segmento (millones de dólares estadounidenses), 2026-2027

Segmento	Gasto 2026	Crecimiento 2026 (%)	Gasto 2027	Crecimiento 2027 (%)
Seguridad de aplicaciones de IA	508	82.1	851	67.5
Control de uso de IA	433	86.6	749	73.0
Plataformas de gobernanza de IA	275	77.4	462	68.0
Gateway de IA	251	80.6	429	70.9
Otros en seguridad de IA	1,368	83.9	2,292	67.5
Total	**2,835**	**83.0**	**4,783**	**68.7**

U$S 4,8 mil millones

Será el tamaño del mercado global de seguridad de IA (securing AI) en 2027.

+68,7% vs. 2026

(Fuente: Gartner)

>90%

Del gasto mundial en ciberseguridad fluye a través de partners, incluyendo proveedores de servicios, integradores y resellers.

2/3

Del mercado direccionable total de ciberseguridad corresponde a servicios.

(Fuente: Omdia)

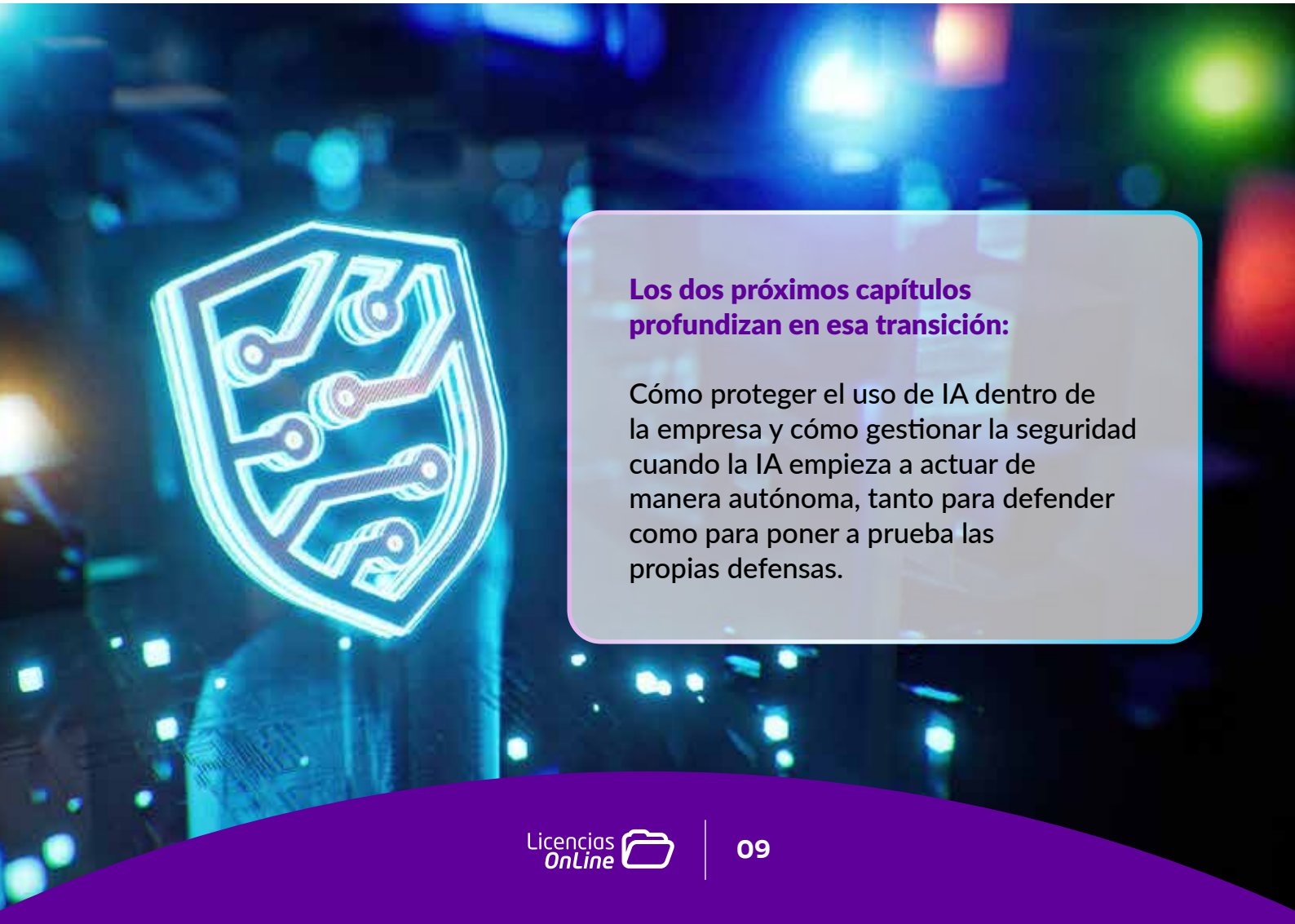
Esto refuerza el desplazamiento desde la venta de tecnología hacia capacidades de **integración**, **monitoreo** y **servicios gestionados**.

La ciberseguridad está pasando de proteger un conjunto relativamente estable de activos a gestionar un entorno dinámico, donde personas, datos, aplicaciones, modelos y agentes interactúan de manera permanente.

De cara a 2027, la agenda de ciberseguridad estará atravesada por dos cuestiones:

Protegerse de la IA.

Aprender a operar de manera segura con sistemas a los que las organizaciones empezarán a delegar decisiones y acciones.



Los dos próximos capítulos profundizan en esa transición:

Cómo proteger el uso de IA dentro de la empresa y cómo gestionar la seguridad cuando la IA empieza a actuar de manera autónoma, tanto para defender como para poner a prueba las propias defensas.

¿Tu organización o la de tus clientes es **AI Security Ready**?

Cuéntanos cuál es el principal desafío en ciberseguridad + IA y conecta con los especialistas de Licencias OnLine y las marcas líderes en protección de IA.

Además, accede a entrenamientos técnicos por marca. Te lleva menos de 2 minutos.

Conoce nuestro **portfolio de soluciones** en Ciberseguridad + IA.

CHECK POINT · f5 · paloalto NETWORKS · netskope · radware
A10 · Acronis · algosec · AppGate · ARCHER
arctera · CATO NETWORKS · celestix · citrixlatam · CLAROTY
eset · FIREMON · GFI Software · GROUP-IB · kaspersky
Microsoft · N-ABLE · opentext · OUTSEER · Progress
Qualys. · RAPID7 · RSA · SOPHOS · TANIUM
TEHAMA · TERAMIND · THALES Building a future we can all trust · Trellix · TrendAI
txOne networks · utimaco · LOL Educación · LOL Servicios



TENDENCIAS

LOL 2027

Licencias OnLine

www.licenciasonline.com