

Lenovo Work Reborn Research Series 2025

Reforzando el lugar de trabajo moderno.

Cómo evaluar con confianza y combatir amenazas de IA mientras transformás tu lugar de trabajo digital.

Lee más [>](#)

**Smarter
technology
for all**

Lenovo

Prepara tu lugar de trabajo para todo.

Para potenciar la productividad de los empleados con IA, los líderes de TI deben transformar el lugar de trabajo digital. Pero a medida que evolucionan las amenazas de seguridad, también necesitan transformar sus defensas para asegurarse de que nada detenga su progreso.

En nuestro primer informe Work Reborn, revelamos cómo la productividad y el compromiso de los empleados están entre las prioridades más urgentes de los líderes de TI. Al crear un entorno laboral más dinámico, mejorado con IA y personalizado, se permite que los empleados se centren en lo que mejor hacen: la resolución creativa de problemas y la colaboración humana.

También mostramos que los líderes de TI comprenden la necesidad de una transformación fundamental del lugar de trabajo digital para aprovechar la promesa de productividad de la IA: los entornos deben reinventarse para que la IA apoye necesidades individuales y la asistencia de TI debe rediseñarse para ofrecer experiencias fluidas e ininterrumpidas.

Ahora investigamos otro pilar vital de la transformación del lugar de trabajo digital en la era de la IA: la ciberseguridad.

La evolución de la IA ha generado nuevas amenazas, tanto desde actores externos como fuentes internas.

Nuestra última encuesta a 600 líderes de TI empresariales revela qué preocupaciones de seguridad impulsada por IA les quitan el sueño —y cuáles podrían estar subestimando.

Creemos que se necesita una respuesta en dos frentes para reforzar el lugar de trabajo moderno:

1. Escalar los esfuerzos para detectar nuevas amenazas adaptativas impulsadas por IA.
2. Reforzar las operaciones de seguridad utilizando la propia IA para proteger los activos más valiosos.

Este informe traza el camino para que los líderes de TI evolucionen sus defensas y adopten la IA en el corazón de su arquitectura de ciberseguridad, permitiendo una transformación que genere valor en el entorno de trabajo impulsado por IA de hoy.

Esperamos que disfrutes el reporte,

Rakshit



Rakshit Ghura

Vice President & General Manager
Lenovo Digital Workplace Solutions

Transforma tu lugar de trabajo sin interrupción por seguridad.

Nuestra investigación revela cómo las organizaciones deben evolucionar sus defensas de ciberseguridad para la era de la IA.

1. **Evaluar:** Identificar las nuevas amenazas de IA →

2. **Evolucionar:** Combatir IA con IA →

3. **Reforzar:** Bienvenido a Work Reborn →



EVALUAR

Identificando nuevas amenazas de IA.

Los líderes de TI están correctamente preocupados por los riesgos que plantea la IA —pero no todos confían en poder defenderse de ellos.

Comprender los riesgos de amenazas externas.

Los líderes de TI están alerta a los riesgos de ciberseguridad que surgen a partir de la IA. Les preocupa especialmente la amenaza que representan los ciberdelincuentes que utilizan IA, con más de seis de cada diez reconociendo que esto es una fuente creciente de riesgo de ciberseguridad.



de los líderes de TI **no están “muy confiados”** en su capacidad para hacer frente a los riesgos provenientes de ciberdelincuentes que utilizan IA.

Los líderes de TI tienen buenas razones para estar preocupados por el uso de la IA por parte de los ciberdelincuentes. En lugar de reemplazar las tácticas tradicionales, la IA las amplifica, ayudando a los atacantes a evadir los sistemas de detección mediante métodos más acelerados y dinámicos.

Los ataques generados por IA pueden evolucionar en respuesta a los mecanismos de defensa que encuentran. Pueden imitar comportamientos benignos y propagarse a través de múltiples dominios: la nube, dispositivos, aplicaciones y más.

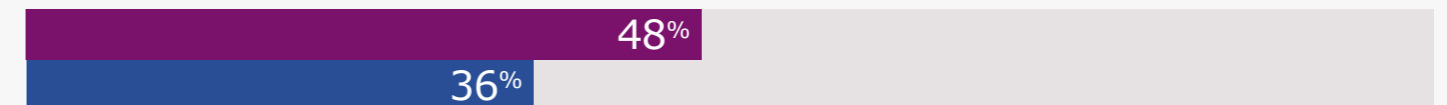
Dónde están creciendo los riesgos de ciberseguridad vs. la confianza de los líderes de TI para abordarlos:

- % que reporta un aumento “significativo” o “moderado” en el riesgo de ciberseguridad
- % “muy” o “algo” confiado en su capacidad para gestionar los riesgos

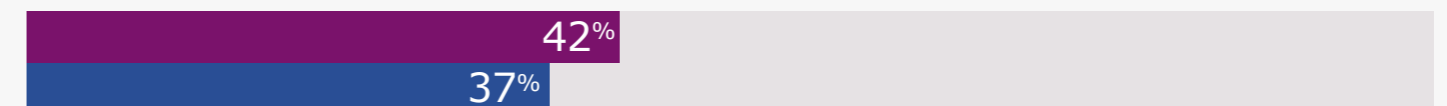
Uso de la IA por Ciberdelincuentes



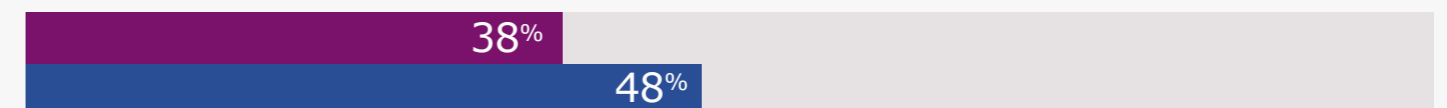
Uso de herramientas de IA públicas por empleados



Adopción de agentes de IA dentro de la organización



Desarrollo e implementación de soluciones de IA dentro de la organización





EVALUAR

Abordar las amenazas internas de IA

Identificar ataques con IA desde fuentes externas es solo una dimensión del desafío más amplio de seguridad de IA.

Más de 6 de cada 10



Líderes de TI coinciden en que los agentes de IA representan un nuevo tipo de amenaza interna para la cual no están completamente preparados.

Siete de cada 10



Están de acuerdo en que el uso indebido de la IA por parte de los empleados es un riesgo que deben abordar.

Menos de cuatro de cada 10



Confían en su capacidad para gestionar cualquiera de estos riesgos.

La IA está evolucionando rápidamente y las implicaciones de ciberseguridad asociadas apenas comienzan a hacerse visibles. Esto incluye la protección de la propia IA — incluidos modelos, datos de entrenamiento y prompts— lo que constituye otro objetivo clave de seguridad para los equipos de TI.

Pero aunque la confianza es baja cuando se trata de defenderse contra ataques externos impulsados por IA, los líderes de TI se sienten más seguros de su capacidad para gestionar los riesgos que provienen de iniciativas internas de IA.



Casi la mitad (48%)

of IT leaders feel 'very' or 'somewhat' confident in their ability to manage risks coming from the development and implementation of AI solutions within the organization.

Si las organizaciones han adoptado las medidas de ciberseguridad necesarias para proteger los sistemas internos de IA, esta confianza puede estar bien fundamentada. Pero también es posible que algunos estén subestimando los riesgos.

“Los líderes de TI están enfocados en la carrera por implementar múltiples iniciativas de IA —pero esto puede llevarlos a pasar por alto los posibles vectores de amenaza que surgen tras su implementación.



Tiago Da Costa Silva

Security Services Director
Lenovo Digital Workplace Solutions



EVALUAR

Nuevos riesgos requieren nuevos enfoques.

Las capacidades tradicionales de ciberseguridad ya no son suficientes para abordar los riesgos relacionados con la IA.

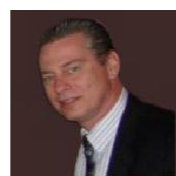
Los líderes de TI deben asegurarse de que sus capacidades de ciberseguridad estén evolucionando al mismo ritmo que los riesgos asociados a la IA. Y en muchos casos, estos riesgos exigen enfoques de seguridad completamente nuevos.

Por ejemplo, las medidas convencionales de protección de datos —como limitar el acceso en función del rol de una persona— ya no son suficientes cuando un sistema de IA puede escanear múltiples documentos para encontrar la respuesta a una consulta de un empleado.

Y los enfoques tradicionales de seguridad de endpoints —como los antivirus— solo pueden detectar amenazas una vez que han sido identificadas y definidas. La IA permite crear código malicioso mucho más rápido que antes, y facilita a los atacantes desarrollar malware polimórfico que muta para evitar la detección y se mezcla con la actividad normal.

Frente a estos nuevos riesgos, las empresas deben actualizar sus capacidades y reforzar la protección de sus activos más valiosos.

“La capacidad de la IA generativa para crear ataques polimórficos ha dado a los atacantes una ventaja asimétrica, permitiendo ataques más rápidos y evasivos que se camuflan dentro de la actividad normal y evaden los mecanismos tradicionales de detección. Incluso con Zero Trust implementado, los defensores deben asumir —y prepararse para— fallos en la detección”



David Majernik

Senior Offering Design Technologist
Lenovo

Factores de riesgo de ciberseguridad con IA.

Amenazas emergentes a tener en cuenta:

- Envenenamiento de modelos / envenenamiento de datos
- Manipulación de modelos de IA
- Fugas de datos privados de IA
- Accesos excesivos habilitados por IA
- Entradas adversariales para IA
- Malware impulsado por IA
- Denegación de servicio mediante sobrecarga de trabajo de IA
- Alucinaciones de IA y desinformación
- Fuga de datos mediante aplicaciones de IA
- Uso “en las sombras” de IA
- Riesgos en la cadena de suministro de IA
- Sesgos y riesgos éticos que derivan en incumplimiento regulatorio
- Ataques de fuerza bruta potenciados por IA

EVALUAR

Evaluación de tus habilidades defensivas.

Los líderes de TI comprenden la importancia de la protección de datos y la gestión de vulnerabilidades, identificándolas como las dos capacidades de ciberseguridad más relevantes para defenderse frente a las amenazas relacionadas con la inteligencia artificial. Sin embargo, no todos están plenamente seguros de que sus capacidades estén a la altura del desafío.

Falta de confianza.



Más de la mitad (54%) de los líderes de TI consideran que sus herramientas de protección de datos, procesos y competencias del personal no son plenamente suficientes para abordar las amenazas de ciberseguridad relacionadas con la inteligencia artificial. Aún menos confían en sus capacidades de análisis de vulnerabilidades y amenazas.



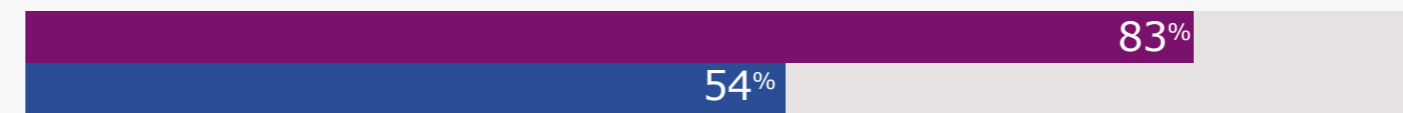
El 65% considera que sus capacidades actuales no son plenamente suficientes para afrontar las amenazas asociadas a la inteligencia artificial.

Y la mayoría comparte esta percepción respecto de sus capacidades en detección y respuesta a incidentes, así como en gestión de identidad y accesos.

Capacidades que los líderes de TI consideran importantes vs. capacidades en las que confían:

- % consideradas “críticas” o de “alta importancia” para abordar los riesgos asociados a la IA
- % capacidades actuales no totalmente suficientes para abordar los riesgos asociados a la IA

Protección de datos



Análisis de vulnerabilidades y amenazas



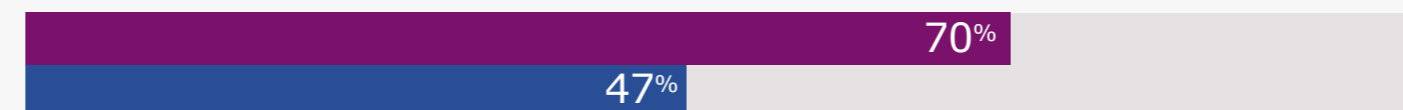
Detección y respuesta a incidentes

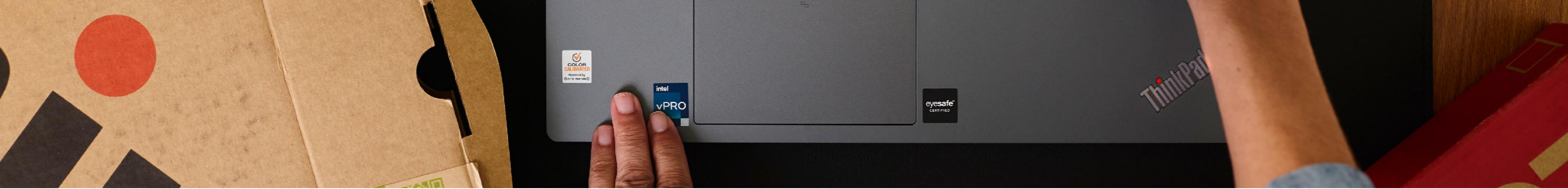


Gestión de identidad y accesos



Seguridad de endpoints





EVALUAR

Cómo comprender y mitigar los riesgos asociados a la IA

Recomendaciones para identificar y mitigar los riesgos impulsados por la inteligencia artificial, tanto de fuentes internas como externas.



Para amenazas externas.

Reconozca las amenazas emergentes impulsadas por la IA provenientes de fuentes externas y adopte medidas proactivas para proteger sus sistemas.

Reevalúa tus sistemas de seguridad.

Dado el bajo nivel de confianza de los líderes de TI en sus capacidades de ciberseguridad, es imperativo que las organizaciones obtengan una visión clara de sus actuales capacidades defensivas frente a las amenazas de IA. Esto comienza con revisiones dinámicas de la postura y la tecnología de ciberseguridad de la organización, para garantizar que el nivel de riesgo se mantenga dentro de los márgenes aceptables para el negocio.

Superar las amenazas.

Los atacantes ahora operan a velocidad de máquina, tardando solo segundos en obtener ventaja y causar daños irreversibles antes de que las defensas tradicionales puedan reaccionar.

Las organizaciones deben ir más allá del monitoreo aislado y adoptar un enfoque nativo de IA para la interpretación inteligente de señales: la capacidad de traducir en tiempo real señales multidominio en respuestas coordinadas e inteligentes.

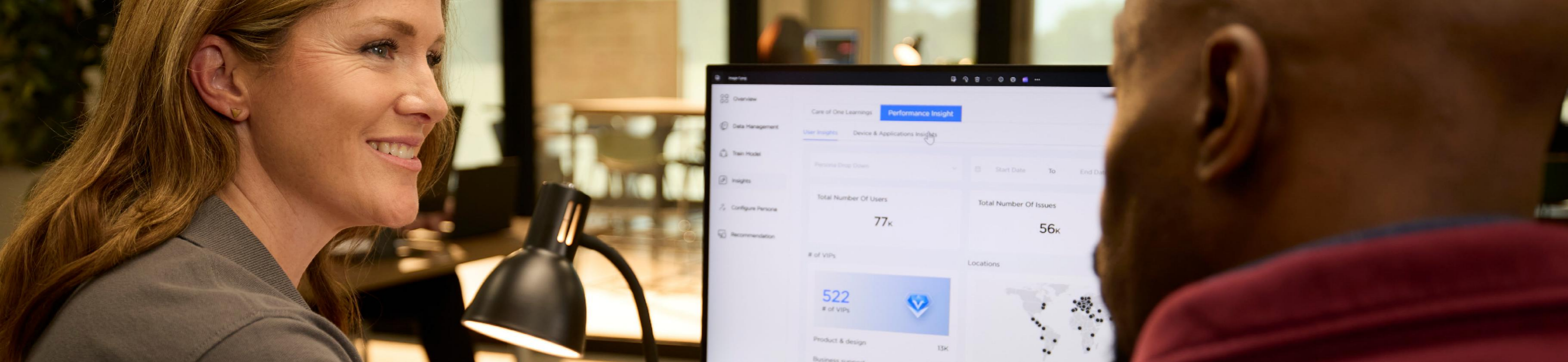
Al unificar la arquitectura de telemetría y consolidar el análisis contextual en todos los niveles, las organizaciones pueden detectar, comprender y actuar antes de que las amenazas se materialicen.

Reducir las vulnerabilidades humanas.

Identificar amenazas impulsadas por inteligencia artificial requiere ir más allá de los programas tradicionales de concientización estática.

Por ejemplo, los atacantes avanzados pueden utilizar ingeniería social potenciada por IA, como suplantaciones de voz o video mediante deepfakes, para engañar a los empleados y obtener información sensible o credenciales.

Así como los empleados deben ser capaces de reconocer un posible correo de phishing, también deben ser entrenados para identificar y mitigar amenazas sofisticadas basadas en IA.



Para amenazas internas.

Identifique los puntos débiles que pueden desarrollarse con los sistemas y prácticas de la IA internas, a menudo pasados por alto por los sistemas tradicionales de ciberseguridad.

Establezca políticas claras del uso de IA.

Los empleados pueden no ser conscientes de que ingresar información sensible en un sistema público de IA podría hacer que esos datos estén disponibles para otros usuarios fuera de la organización.

Deben establecerse políticas y controles explícitos que orienten a los empleados y prevengan comportamientos riesgosos.

Audite accesos de derecho.

A menos que los privilegios de acceso a los datos de IA se controlen cuidadosamente, los agentes de IA podrían comprometer las medidas internas de protección de datos o ser tomados por atacantes que busquen extraer información sensible rápidamente.

El riesgo de fuga de datos implica que las organizaciones deben reforzar sus mecanismos de monitoreo y garantizar que tanto los sistemas de IA como los empleados solo accedan a la información estrictamente necesaria.

Proteja el ciclo de desarrollo de la IA.

Desarrollar e implementar sistemas de IA dentro de la organización introduce nuevos tipos de riesgos.

Por ejemplo, si ciberdelincuentes manipulan los datos de entrenamiento de una solución de IA orientada al cliente, podrían ocasionar daños significativos a la reputación y al cumplimiento normativo.

Los organizadores deben establecer controles y verificaciones internas que impidan la manipulación de los sistemas de IA



EVOLUCIONAR

Combatiendo la IA con IA.

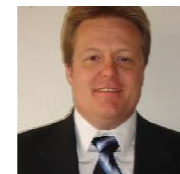
Para enfrentar los riesgos de ciberseguridad de la IA, los líderes de TI deben aprovechar todo el potencial de la propia IA.

Mejorar la reactividad.

En un entorno de seguridad donde la velocidad de ataque supera la capacidad de respuesta de los humanos, es fundamental aprovechar la IA para respaldar y ampliar la toma de decisiones humanas.

Los sistemas de ciberseguridad integrados en IA también permiten a los equipos de seguridad interactuar con sus herramientas utilizando una interfaz de lenguaje natural, en lugar de rastrear múltiples pantallas para acceder a la información que necesitan para tomar una decisión urgente.

“Desde una perspectiva de seguridad, cuanto más holística sea su visión de lo que está ocurriendo, más rápido podrá detectar cuando algo está saliendo mal”



Mikkel Seiero

Líder global de los servicios de seguridad
Lenovo

Lograr una visibilidad unificada.

En una arquitectura de ciberseguridad empresarial tradicional, las capacidades como la protección de datos o el análisis de vulnerabilidades son entregadas por equipos separados que utilizan herramientas especializadas.

Los adversarios habilitados para IA generativa pueden explotar los puntos ciegos entre estas funciones, minimizando la observabilidad de estos ataques.

Para hacer frente a estos ataques, los equipos de ciberseguridad necesitan una visión holística de la postura de seguridad de la empresa, una que atraviese dominios y se base en múltiples conjuntos de herramientas. La extracción de inteligencia, una puntuación dinámica de la postura de seguridad y medidas automatizadas de la vista agregada solo es posible aprovechando la IA.

“La visibilidad es el primer paso para la seguridad de la IA: a través de una visibilidad completa de todos los módulos y aplicaciones de IA, sus funcionalidades y el monitoreo continuo del uso, protegemos los datos confidenciales, hacemos cumplir el cumplimiento de la seguridad y defendemos a la organización contra las amenazas emergentes impulsadas por la IA”.



Kamrul Hasan

Arquitecto de ciberseguridad
Lenovo

EVOLUCIONAR

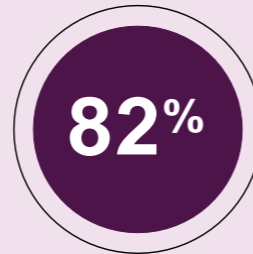
Las barreras para integrar la IA con la ciberseguridad.

Para defenderse de futuras amenazas, los equipos de TI deben utilizar la IA en todas sus defensas digitales en el lugar de trabajo. Pero llegar allí no es sencillo.

Nuestra encuesta muestra que las empresas ya han hecho avances en la adopción de la IA en la ciberseguridad. Por ejemplo, casi la mitad está utilizando la IA y la automatización de forma intensiva en áreas como seguridad de endpoints y gestión de identidades y acceso (IAM). Sin embargo, dado que menos de la mitad confía plenamente en que sus capacidades de seguridad son totalmente adecuadas para afrontar los riesgos de la IA, queda claro que aún no existe un amplio margen de mejora.

Y fortalecer con éxito las medidas de ciberseguridad con IA no se reduce simplemente a implementar las como herramientas adecuadas. Para muchas organizaciones, existen barreras sustanciales que deben superarse antes de lograrlo.

Barrier #1: Entornos de TI complejos.



de los líderes de TI dicen que la "complejidad del entorno de TI" es una de las principales barreras para la seguridad impulsada por IA.

Nuestra encuesta revela que la barrera más común es la complejidad del entorno de TI. La mayoría de las organizaciones empresariales cuentan con un ecosistema de TI —incluido su conjunto de herramientas de ciberseguridad— que ha evolucionado durante muchas décadas. Esto puede implicar la presencia de herramientas heredadas que no son compatibles con las nuevas plataformas impulsadas por IA.

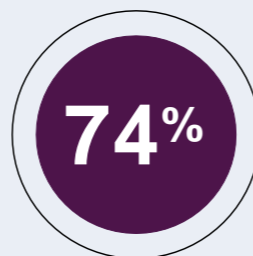
Barrera #2: Falta de personal especializado en ciberseguridad.



de los líderes de TI dicen que la "falta de personal calificado dentro de la función de ciberseguridad" es una de las principales barrera para la seguridad impulsada por IA.

La segunda barrera más común es la falta de personal calificado dentro de la función de ciberseguridad. Esto no es sorprendente: tanto las habilidades de IA como las de ciberseguridad tienen una gran demanda y son escasas. Encontrar empleados con experiencia en ambos campos es extremadamente desafiante. Esta escasez se ve agravada por la creciente carga de los analistas de seguridad, que operan en un entorno de alto estrés y cognitivamente exigente a medida que se enfrentan a adversarios cada vez más avanzados.

Barrera #3: Costo de las soluciones/presupuesto limitado.



de los líderes de TI dicen que el "costo de las soluciones / presupuesto limitado" es una de las principales barreras para la seguridad impulsada por IA.

Las herramientas avanzadas, el personal calificado y la inversión continua en la preparación para la IA requieren un compromiso significativo de recursos. Para muchas organizaciones que ya están bajo presión presupuestaria, la asignación de fondos a tecnologías emergentes puede ser difícil de priorizar, especialmente cuando las herramientas existentes aún funcionan, incluso si están desactualizadas.



EVOLUCIONAR

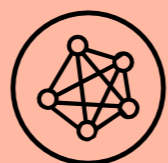
Cómo transformar tus defensas.

Recomendaciones: pasos prácticos que las organizaciones pueden tomar para defenderse de las amenazas impulsadas por la IA.



Construye una visión holística.

Con complejos complejos patrimonios de TI y equipos de seguridad sobrecargados, la fragmentación de las herramientas genera ineficiencias, costes ocultos y una visibilidad limitada de las amenazas. La consolidación de la telemetría entre usuarios, endpoints, aplicaciones e infraestructura en la nube ayuda a reducir la expansión de herramientas y los costos de capacitación, al tiempo que crea la vista unificada necesaria para detectar y responder a las amenazas impulsadas por IA de manera más rápida y efectiva.



Adopta herramientas versátiles.

Las grandes empresas a menudo tienen sistemas críticos para el negocio que se ejecutan en plataformas heredadas que no pueden migrar fácilmente. Para tocar en las capacidades de ciberseguridad impulsadas por IA, las empresas deben integrar soluciones y herramientas de seguridad que admitan una amplia gama de sistemas operativos, incluidos aquellos que de otro modo podrían haber perdido soporte.



Impulsa tu equipo de seguridad con socios experimentados.

Las amenazas de IA se mueven rápidamente, mientras que mejorar las habilidades de los equipos internos requiere dinero y tiempo. Ampliar sus capacidades trabajando con socios experimentados le brinda acceso a las habilidades que necesita hoy, a la escala que requiere el desafío.



Bienvenido a Work Reborn, reforzado.

Proteger el lugar de trabajo digital en la era de la IA en evolución requiere una reinvencción completa de cómo las empresas monitorean, comprenden y responden a las amenazas de ciberseguridad, y cómo defienden sus activos digitales.

Para invertir la situación frente a las amenazas de la IA generativa, las empresas deben:

- **Mejorar las capacidades de detección.**

Dada la capacidad de las amenazas impulsadas por IA para escapar a la detección, las organizaciones deben redoblar sus esfuerzos para proteger sus activos de alto valor. Estos incluyen los propios sistemas de IA: los agentes, modelos, datos de entrenamiento e indicaciones que impulsan estos sistemas de IA son objetivos cada vez más valiosos para los actores maliciosos.

- **Aprovechar las capacidades de la IA.**

Las organizaciones también deben adoptar una postura de seguridad más adaptable, abordando las amenazas en tiempo real siempre que sea posible. Esto solo puede ser logrado aprovechando las mismas capacidades de IA que usan los atacantes, equipando a los equipos de seguridad con la información, el contexto y las recomendaciones rápidas que necesitan.

Este enfoque doble ofrece mejores resultados comerciales:

Aumento de la productividad.

La incorporación de IA en las operaciones de seguridad puede fortalecer la productividad de los trabajadores de seguridad. Security Copilot de Microsoft, un asistente de IA para equipos de ciberseguridad, puede aumentar la productividad de los equipos de SecOps entre un 23 % y un 47 %, según una evaluación de Forrester Research.¹ Y, según el propio análisis de Microsoft, los conflictos de políticas de dispositivos se pueden resolver un 54 % más rápido² y los incidentes se pueden resolver un 30 % más rápido³ mediante el uso de Security Copilot.

Costos reducidos.

Transformar sus defensas tiene una variedad de beneficios para el resultado final. Por ejemplo, crear una visión holística de sus operaciones de seguridad utilizando IA reduce los costos de capacitación necesarios para permitir que los equipos de seguridad utilicen las herramientas subyacentes. También puede minimizar los costos de mantenimiento al optimizar la cantidad de herramientas que se utilizan y brinda la oportunidad de subcontratar funciones no diferenciadas a socios con la escala para entregar de manera rentable.

Transformación sin interrupciones

Quizás lo más importante es que reestructurar la ciberseguridad para la era de la IA en rápido movimiento puede brindarle la confianza para adoptar completamente la transformación digital del lugar de trabajo. Nuestra encuesta anterior encontró que las preocupaciones de seguridad de los líderes empresariales se encuentran entre las barreras más comunes para la adopción de IA. Y, como hemos visto, estas preocupaciones no son infundadas. Por lo tanto, cualquier transformación del lugar de trabajo digital liderada por IA debe ir acompañada de una actualización de ciberseguridad.

¹ [New Technology: The Projected Total Economic Impact™ Of Microsoft Security Copilot, Forrester Research](#), November 2024

² [Security Copilot: Evidence of Productivity Gains in Live Operations](#), Microsoft Corporation, March 2025

³ [Generative AI and Security Operations Center Productivity: Evidence from Live Operations](#), Microsoft Corporation, November 2024



¿Listo para transformar tu lugar de trabajo de forma segura?

Evalúe con confianza las amenazas de IA y asegúrese de estar seguro a medida que moderniza su lugar de trabajo digital.

Comienza [Aquí](#).

La visión es tuya. Alcáncela con Lenovo.

Metodología.

Para este estudio, Lenovo encuestó a 600 líderes de TI en abril y mayo de 2025. La muestra de la encuesta incluyó encuestados de EE. UU. (17%), Canadá, Reino Unido, Francia, Alemania, India, Japón, Singapur, Brasil, México (8% cada uno), Australia (4%) y Nueva Zelanda (4%). Entre los encuestados se encontraban líderes de TI de empresas con al menos 1.000 empleados y de una variedad de sectores.

**Smarter
technology
for all**

Lenovo