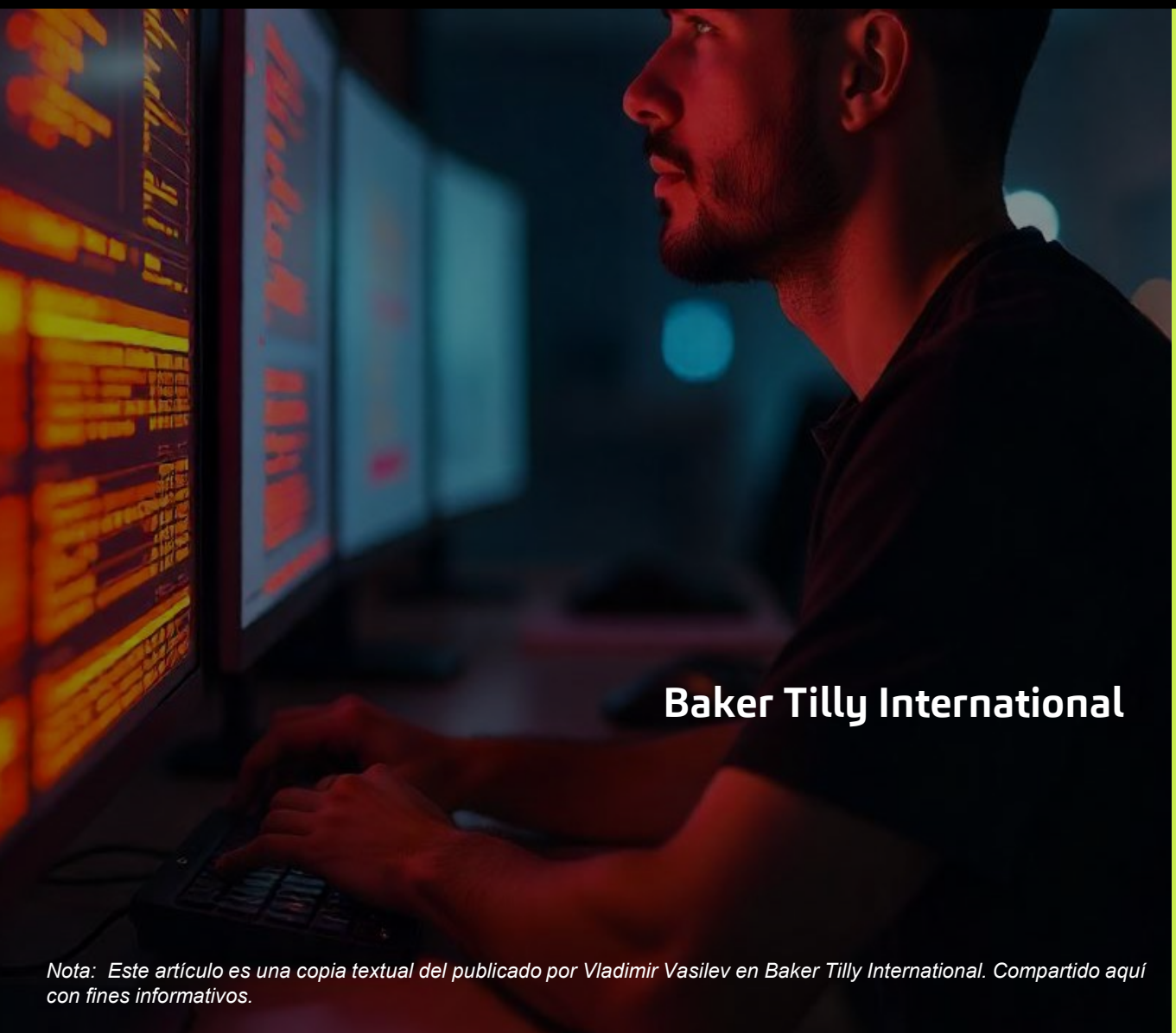
bakertilly
DIGITAL

IA vs IA



Baker Tilly International

Nota: Este artículo es una copia textual del publicado por Vladimir Vasilev en Baker Tilly International. Compartido aquí con fines informativos.

Es una escena familiar que se repite todos los días en las empresas: un empleado recibe un correo electrónico que parece provenir de un colega de confianza y sigue las instrucciones sin pensarlo dos veces.

Tal vez hagan clic en un enlace, descarguen un archivo o envíen una respuesta rápida, todas ellas tareas rutinarias, hasta que, sin saberlo, abren la puerta a un ciberataque.

Dado que el 95% de las violaciones de ciberseguridad son causadas por errores humanos y el costo promedio de una violación ahora asciende a US$4 millones , se trata de un error simple y común, con grandes consecuencias.

5 millones de dólares estadounidenses

El coste medio de una filtración de datos en 2024: un aumento del 10 % con respecto a 2023 y el promedio más alto registrado. (IBM)

Y no son sólo las pequeñas empresas las que están sintiendo la presión.

Tan solo este mes, los ciberataques derribaron los sistemas de tres importantes minoristas del Reino Unido con unos días de diferencia: un duro recordatorio de que las organizaciones de todos los tamaños necesitan estar preparadas.

Para el gigante minorista M&S, el ataque interrumpió todos los pedidos en línea a través de su aplicación y sitio web y borró 1.000 millones de libras de su valor . Las previsiones sugieren que la normalidad podría tardar meses.

Días después del ataque a M&S, un ciberincidente en desarrollo en Co-op obligó al minorista británico a desconectar algunos de sus sistemas informáticos para contener el ataque. Un día después, los grandes almacenes de lujo Harrods se vieron obligados a restringir el acceso a internet en sus instalaciones tras un intento de acceder a sus sistemas.

20-25

El número de ataques importantes de ransomware cada *día* en 2004, aumentó de solo cinco al *año* en 2011. *(*New York Times)

Pero para muchos, la amenaza no es un hecho aislado: es implacable.

Amazon.com defiende más de mil millones de ciberataques cada día , lo que equivale a más de 11.500 por segundo.

“La velocidad y simplicidad de acceder a grandes modelos de lenguaje e IA están desatando una era de ciberamenazas sin precedentes, y los ciberdelincuentes son cada vez más inteligentes”, afirma Vladimir Vasilev, líder digital de Baker Tilly (República Dominicana).

¿Pero la buena noticia? Las defensas también se están volviendo más inteligentes.

«Desde la detección inteligente de amenazas hasta los filtros de correo electrónico adaptativos, las herramientas de ciberseguridad más eficaces hoy en día se basan en una IA que aprende, evoluciona y responde en tiempo real», afirma el Sr. Vasilev.

“El futuro de la seguridad no es humano contra IA, sino IA contra IA”.

Chico malo

Las estafas en línea solían ser torpes y fáciles de detectar, pero la IA generativa ha cambiado eso, advierte Vasilev.

La IA ha potenciado la ingeniería social. Hablamos de correos electrónicos que imitan a la perfección a alguien de confianza, sistemas que buscan vulnerabilidades y deepfakes que pueden manipular de forma convincente tanto la imagen como el sonido. Estas no son solo amenazas teóricas: facilitan enormemente engañar a las personas para que revelen datos confidenciales o su acceso.

Según Vasilev, plataformas como ChatGPT han transformado el panorama con su capacidad de generar texto fluido y similar al humano a gran velocidad.

“En las manos equivocadas, eso significa estafas más creíbles, más noticias falsas virales e incluso clones de voz que pueden engañar al ojo o al oído más perspicaz”.

Y mirando hacia el futuro, advierte, el verdadero punto de inflexión podría ser la IA autónoma.

Una vez que las máquinas empiezan a tomar decisiones de forma independiente, los riesgos aumentan significativamente. Estos incluyen actuar sin supervisión humana, ser vulnerables a ataques informáticos maliciosos, tomar decisiones sesgadas o erróneas, generar incertidumbre sobre la responsabilidad cuando se producen errores y exponer los datos personales a un mayor riesgo.

La IA es un arma de doble filo: las mismas herramientas que ayudan a los ciberdelincuentes también se utilizan para defenderse de ellos.

“No se trata simplemente de la tecnología en sí, sino de cómo y quién la utiliza”.

292

El número promedio de días necesarios para identificar y contener las infracciones que involucran credenciales robadas. (IBM)

Buen chico

Las organizaciones que utilizan ampliamente la IA y la automatización en ciberseguridad ahorran un promedio de 2,22 millones de dólares estadounidenses en comparación con las que no lo hacen. Por lo tanto, no sorprende que más de dos tercios de las empresas ahora confíen en esta tecnología para detectar y detener ciberataques.

“La IA simplemente supera a los humanos cuando se trata de manejar y analizar volúmenes masivos de datos”, explica Vasilev.

“Y eso es exactamente lo que se necesita para hacer frente a las ciberamenazas actuales”.

Estas herramientas no duermen.

Buscan anomalías, analizan patrones de comportamiento y responden en tiempo real, a menudo con una mínima intervención humana.

Al aprender el comportamiento habitual de los usuarios, la IA puede detectar rápidamente lo inusual, bloqueando cuentas o alertando a los administradores antes de que se produzcan daños reales. El aprendizaje automático impulsa un software antivirus más inteligente, una inteligencia de amenazas más precisa y defensas más rápidas y adaptables.

“La IA se está convirtiendo rápidamente en el aliado más poderoso de la ciberseguridad”, afirma Vasilev.

“En el futuro, podría ser capaz de predecir amenazas, corregir vulnerabilidades automáticamente e incluso desarrollar nuevas formas de defensa que aún no hemos imaginado”.

Pero como la misma tecnología que fortalece las defensas también empodera a los atacantes, el Sr. Vasilev advierte que las organizaciones deben evolucionar junto con ella: capacitar a los equipos para detectar amenazas impulsadas por IA, proteger sus propios sistemas de IA y usar la IA para defenderse contra ataques impulsados por IA.

Pero hay un gran desafío: el talento.

“Solo alrededor del 12% de los profesionales de la ciberseguridad tienen formación formal en IA o aprendizaje automático”, señala Vasilev.

Esa es una brecha importante, ya que para tener éxito en ciberseguridad hoy en día, no basta con ser un experto en seguridad; también se necesita ser un experto júnior en IA. Es necesario comprender los diferentes tipos de aprendizaje automático, saber cómo funcionan las herramientas de IA (y dónde fallan) y mantenerse al día sobre los crecientes riesgos y las normas en torno a la IA generativa. Ya no es opcional, es la base.

Y la presión va en aumento. Ante la escasez mundial de talento en ciberseguridad, muchas pequeñas empresas también tienen dificultades para costear herramientas de seguridad avanzadas basadas en IA. Al mismo tiempo, un panorama regulatorio en constante evolución exige una formación continua, lo que ejerce una presión adicional sobre unos recursos ya limitados.

"Es como correr en una cinta que no para de acelerar", dice el Sr. Vasilev. "Agotador, pero esencial".

Un acto de equilibrio

Para la mayoría de las empresas, los datos son su joya de la corona y, cuando se utiliza IA, protegerlos debe ser una prioridad absoluta, explica Vasilev.

“Eso significa establecer límites claros: la información confidencial no debe introducirse en las herramientas de IA y los empleados necesitan orientación sobre qué es seguro compartir.

Es fundamental concienciar a los empleados sobre los diversos métodos que utilizan los ciberdelincuentes para acceder a información confidencial. Es igualmente importante comprender cómo funcionan modelos como ChatGPT y cómo interactuar con ellos de forma responsable para evitar problemas como el envenenamiento por IA.

La IA es potente: puede escribir, codificar, analizar y automatizar, y está contribuyendo a la innovación en sectores que van desde la educación hasta la sanidad y las finanzas. Pero no es infalible, afirma el Sr. Vasilev.

“Piénselo menos como un genio y más como un asistente brillante: increíblemente útil pero que requiere supervisión.

Si se usa con prudencia, puede liberar un enorme potencial: desde ayudarnos a trabajar con mayor rapidez e inteligencia hasta generar nuevas ideas. Si se usa sin cuidado, puede causar graves riesgos.

“En última instancia, cuanto más inteligentemente utilicemos la IA, mejor podremos aprovechar sus fortalezas y evitar sus debilidades”.

1 de cada 3

Porcentaje de filtraciones que involucraron datos ocultos, lo que demuestra que la proliferación de datos dificulta su rastreo y protección. (IBM)

La era de la rendición de cuentas

Con más de 170 regulaciones de protección de datos propuestas o promulgadas en los últimos dos años , está claro que la era de la responsabilidad de la IA ha comenzado, y las reglas se están endureciendo.

“Los organismos reguladores de todo el mundo están implementando nuevos marcos y estándares para frenar el uso indebido y promover una IA responsable”, afirma Vasilev.

La Ley de IA de la UE —la primera de su tipo— entró en vigor en agosto de 2024 y se aplicará plenamente en 2026, centrándose en los sistemas de alto riesgo con requisitos más estrictos.

En Estados Unidos, el Instituto Nacional de Estándares y Tecnología ha desarrollado un marco de gestión de riesgos para gestionar mejor los riesgos asociados a la IA para las personas y las organizaciones.

“Actualmente, no existe una regulación general que rija cómo debe desarrollarse la IA, pero las aplicaciones específicas, en particular aquellas que plantean riesgos potenciales, están siendo objeto de un escrutinio cada vez mayor”, señala el Sr. Vasilev.

Plataformas como TikTok y Meta ya se están adaptando mediante la implementación de herramientas para detectar y etiquetar contenido generado por IA, lo que ayuda a los usuarios a identificar cuándo algo no es real.

Inteligencia calculada

A medida que la IA redefine tanto las herramientas de defensa como las tácticas de ataque, la concientización, la responsabilidad y la implementación inteligente son fundamentales.

Las organizaciones que invierten en comprender y orientar el uso de la IA (en ciberseguridad y más allá) estarán mejor posicionadas para aprovechar su potencial y, al mismo tiempo, mantenerse protegidas contra sus riesgos.

“El futuro de la IA en los negocios no se trata solo de innovación; se trata de confianza, vigilancia y encontrar el equilibrio adecuado”, afirma Vasilev.

442%

El aumento de los ataques de phishing de voz entre el primer y el segundo semestre de 2024. (Crowdstrike)

Vladimir Vasilev
Líder Digital
Baker Tilly (República Dominicana)

bakertilly

Desde
1986

Auditores y Consultores

- División de Auditoría
- División de BPO – Outsourcing
- División de Impuestos
- Ver más

Baker Tilly Consulting

- Central de Consultas Empresariales
- Prevención del Lavado de Activos y Corrupción
- Precios de Transferencia
- Revisión de Ventas LAP
- Implementación NIIF
- Ver más

Baker Tilly Digital

- Ciberseguridad
- Robótica de procesos
- Inteligencia corporativa
- Tax Analytics
- Ver más

Certificación ISO 9001:2015

Alcance: Auditoría Financiera
Auditoría Tributaria
Outsourcing Contable

Central: +51 206 6700
Central Celular: 981 881 842
Email: noles@bakertilly.pe
Dirección: Calle Amador Merino Reyna 339, San Isidro – Torre América, Piso 7
Página web: www.bakertilly.pe