LITORALPRESS

Fecha: 31-07-2025
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Noticia general
Título: **Ciberseguridad hoy La Inteligencia Artificial en el centro de las estrategias**

Pág. : 10
Cm2: 559,5
VPE: $ 788.837

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

ESPECIAL

Ciberseguridad & IA

Ciberseguridad hoy

La Inteligencia Artificial en el centro de las estrategias

La Inteligencia Artificial (IA) dejó de ser una promesa futura en el ámbito de la ciberseguridad: hoy es una herramienta concreta, en uso y en evolución constante. Así lo señalaron los representantes de integradores nacionales, parte del ecosistema de Fortinet, que participaron de una nueva Mesa de Trabajo de Revista Gerencia. En esta instancia, abordaron las principales oportunidades, así como desafíos y riesgos del uso de la IA en seguridad digital, junto a la evolución de este mercado.

LITORALPRESS

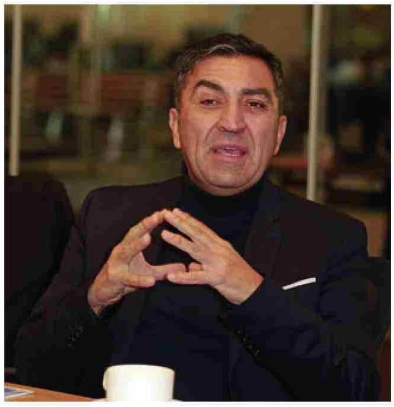
Fecha: 31-07-2025
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Noticia general
Título: **Ciberseguridad hoy La Inteligencia Artificial en el centro de las estrategias**

Pág. : 11
Cm2: 551,6
VPE: $ 777.708

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

ESPECIAL

Ciberseguridad & IA



Roberto Jiménez, TCAM Technology.

Pablo Quiero, INNOVA-NET.

Elio Sorrentino, NEC.

El creciente volumen y sofisticación de los ataques ha convertido a la ciberseguridad en una preocupación constante para las organizaciones. ¿Qué tan enfocadas están hoy las empresas en este tema? Para Roberto Jiménez, Gerente General de TCAM Technology, la respuesta es clara: el interés ha crecido significativamente en los últimos años, especialmente en sectores más regulados. "Yo creo que hoy las empresas están muy interesadas en ciberseguridad. La banca fue pionera, en parte por todos los estándares de cumplimiento que debe seguir, muchos de ellos provenientes de EEUU. En Chile hemos avanzado bastante, aunque todavía hay un déficit importante de profesionales en el área, lo que hace difícil encontrar talento. Aun así, para las grandes compañías ya es evidente lo que pierden cuando no invierten en seguridad", señala.

A juicio de Pablo Quiero, CEO de Innova-Net, cada vez más, los presupuestos se están orientando hacia ciberseguridad. "Y es que la transformación tecnológica ha alcanzado un nivel crítico. Hoy, cualquier empresa que no esté digitalizada tiene muy pocas probabilidades de éxito. Y si está digitalizada, necesariamente debe tener seguridad. Las nuevas tecnologías de digitalización de datos están empujando a las compañías a asumir un rol aún más relevante en este ámbito", indica.

En este contexto, los asistentes coinciden en que la IA está redefiniendo tanto las estrategias defensivas como ofensivas en ciberseguridad, y que su incorporación no es optativa, sino esencial para enfrentar un entorno de amenazas cada vez más sofisticadas y masivas. "Ya no se trata de si vamos a ser atacados, sino de cuándo, y cómo estaremos preparados", resume Elio Sorrentino, BDM Datacenter & Security de NEC.

El avance de la legislación también está impulsando un cambio cultural dentro de las organizaciones, jugando un rol en esa transformación. Según Constanza Retamal, Gerente Comercial de E-Money, "la Ley de Ciberseguridad ha generado un punto de inflexión. Ahora los directorios están obligados a involucrarse, y personas que antes no trataban directamente con temas tecnológicos o conceptos más técnicos deben empezar a entender cuáles son los riesgos específicos para su negocio, y dejar de ver la ciberseguridad como un gasto, sino como una inversión estratégica. Si no invierto aquí, ¿cuál es el costo real de sufrir un ataque?", afirma.

Además, este cambio -agrega- ya está forzando a nuevas áreas dentro de las compañías a involucrarse en temas de seguridad digital, muchas de las cuales antes quedaban al margen de los procesos tecnológicos. "En algún momento, esto se traspasará transversalmente a todas las áreas y a todas las compañías", advierte.

Una amenaza en expansión: Ataques más rápidos, diversos e invisibles

Uno de los puntos más destacados en el análisis de los proveedores fue el vertiginoso aumento en la velocidad y volumen de los ataques. Según cifras de FortiGuard Labs, los intentos de ciberataques en Chile pasaron de 6.000 millones en 2023 a más de 26.000 millones en 2024, lo que refleja no solo un alza en cantidad, sino también en sofisticación. "Eso no solo indica que hay más ataques, sino que las herramientas para automatizarlos se han multiplicado y perfeccionado", agrega Juan Pablo Arias, Gerente de Ingeniería de Fortinet.

"Ya no se espera un ataque por semana: ocurren cada pocos minutos o incluso segundos", advierte Jaime Aguilera, Gerente Comercial de NLT Secure. Agrega que "la nueva Ley de Ciberseguridad pone a la concientización como un eje clave. Porque al final del día, la voz más débil seguimos siendo nosotros, los humanos".

LITORALPRESS

Fecha: 31-07-2025
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Noticia general
Título: **Ciberseguridad hoy La Inteligencia Artificial en el centro de las estrategias**

Pág. : 12
Cm2: 541,2
VPE: $ 763.103

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida


Constanza Retamal, E-MONEY.


Juan Pablo Arias, FORTINET.


Jaime Aguilera, NLT SECURE.

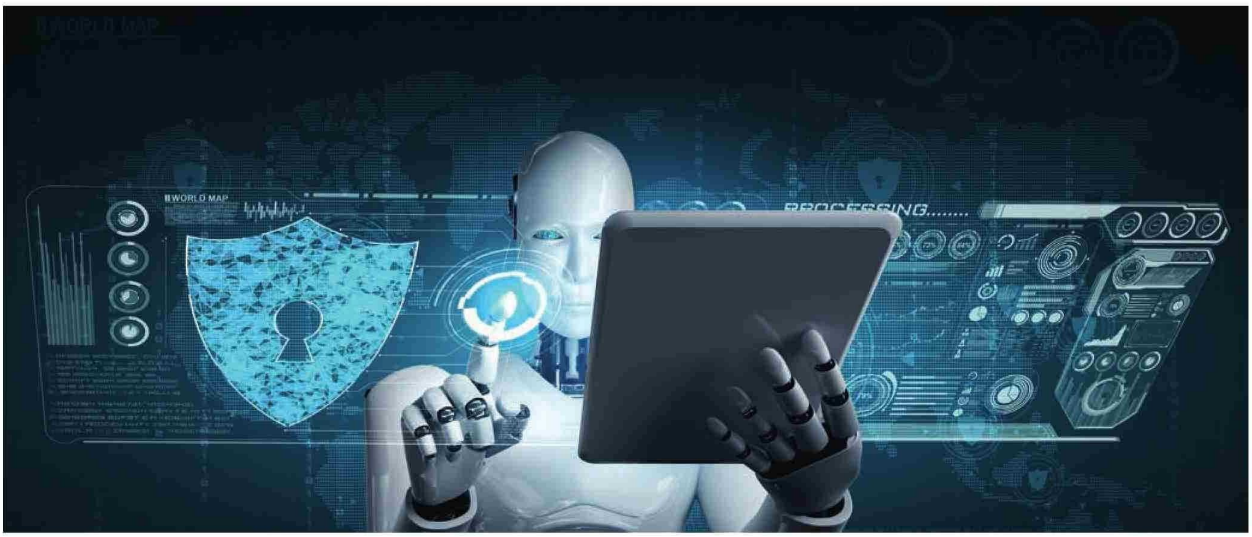
El uso de IA por parte de los atacantes ha democratizado el acceso a herramientas que antes eran exclusivas de expertos, detalla el profesional de NEC. Hoy, incluso un niño podría ejecutar un ataque utilizando algoritmos automatizados sin siquiera entender las consecuencias, como señala el ejecutivo de Innova-Net. Esta masificación de herramientas ha hecho que la superficie de ataque crezca exponencialmente, afectando a empresas de todos los tamaños y sectores.

En los últimos meses, los ataques se han vuelto más complejos, utilizando IA para confundir al usuario final. "Más que el eslabón débil, el usuario es el menos preparado", explica Roberth Castellanos, Gerente de TI de Netics. Destaca que con herramientas que generan imágenes falsas y correos creíbles en segundos, el phishing alcanza un nuevo nivel de sofisticación.

A ello se suma un fenómeno preocupante: la creciente invisibilidad del ataque. Según el profesional de Fortinet, los nuevos vectores de amenazas pueden pasar desapercibidos incluso para usuarios expertos. "Cuando impulsamos planes de concientización, antes le decíamos al usuario: 'Fíjate en la ortografía, en la coma, en el punto'. Esa recomendación ya no va. Hoy es extremadamente difícil distinguir entre algo real y algo falso", agrega. Los ataques actuales utilizan lenguaje perfecto, imágenes realistas y hasta perfiles falsos generados con IA. El ojo humano ya no es suficiente para detectarlos.

Múltiples vectores

Uno de los ejemplos más conocidos sigue siendo el ransomware, que continúa entre los métodos más utilizados por los cibercriminales.



LITORALPRESS

Fecha: 31-07-2025
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Noticia general
Título: **Ciberseguridad hoy La Inteligencia Artificial en el centro de las estrategias**

Pág. : 13
Cm2: 559,7
VPE: $ 789.222

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

ESPECIAL

Ciberseguridad & IA

Roberth Castellanos, NETICS.

Leonardo Leiva, EDATA CHILE.

Matías Vergara, NOOVUS.

Sin embargo, como se señaló en la conversación, no es el único.

"El ransomware es solo uno de los vectores actuales. También siguen existiendo ataques clásicos, como las inyecciones de código, pero ahora vemos cómo la IA está siendo usada activamente para potenciar los ataques. Así como se utiliza para proteger, también se está usando para vulnerar. Estamos frente a una pelea entre la IA del lado bueno y la IA del lado malo", plantea Leonardo Leiva, Líder de Área Networking OT de Edata Chile.

"Hoy en día, hasta un termómetro o un refrigerador conectado puede ser un vector de ataque. Hay tantos dispositivos con acceso a Internet que uno ni siquiera imagina que podrían representar un riesgo. Pero sí, perfectamente podrían vulnerar la red Wi-Fi de una casa a través de un electrodoméstico", advierte la profesional de E-Money.

El uso masivo de credenciales robadas representa también otro frente de riesgo: "Algunos minimizan el impacto de que se filtren, por ejemplo, 25 millones de cuentas. Pero cuando se cruzan esos datos, se generan tendencias y patrones que incluso pueden alimentar nuevos ataques potenciados por IA. Por eso es fundamental contar con herramientas como las de Fortinet que permiten analizar esos patrones de uso y detectar, por ejemplo, qué usuarios están más expuestos", precisa el ejecutivo de NLT Secure.

> *"La IA está siendo utilizada en ambos frentes: tanto para fortalecer la ciberseguridad como para potenciar ataques más sofisticados. El desafío está en cómo cubrirse bien y protegerse en esta pelea entre la IA del lado bueno y la del lado malo"*

Gracias a estas capacidades, hoy es posible identificar si un mismo usuario aparece reiteradamente en incidentes, lo que permite anticipar vulnerabilidades y reforzar la seguridad de forma más dirigida. "Si 'x' persona vuelve a aparecer en un próximo reporte, se genera una alerta. Y si aparece tres, cinco o diez veces en cuatro meses, claramente hay que actuar sobre ese usuario. Y hoy existen herramientas para hacerlo", concluye.

La IA como aliada

En la otra vereda, la IA también se ha convertido en un soporte crucial para los defensores. Su capacidad para analizar volúmenes masivos de datos en tiempo real, detectar patrones anómalos y automatizar respuestas ha aliviado significativamente la carga de los Centros de Operaciones de Seguridad (SOC).

Además, los falsos positivos o alertas mal configuradas pueden saturar a los operadores de seguridad, generando fatiga y aumentando el riesgo de omisiones. Según el ejecutivo de Edata Chile, "si configuras mal un parámetro, puedes llenarte de falsos positivos. Y la IA está siendo utilizada en ambos frentes: tanto para fortalecer la ciberseguridad como para potenciar ataques más sofisticados. El desafío está en cómo cubrirse bien y protegerse en esta pelea entre la IA del lado bueno y la del lado malo".

Al respecto, Elio Sorrentino advierte que cuando se produce una alerta real -una alarma positiva-, la atención del operador se concentra en esa sola incidencia. "Pero si tienes siete, ocho, veinte, treinta alertas activas, alguien tiene que estar mirando el resto. Y ahí

LITORALPRESS

Fecha: 31-07-2025
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Noticia general
Título: **Ciberseguridad hoy La Inteligencia Artificial en el centro de las estrategias**

Pág. : 14
Cm2: 572,2
VPE: $ 806.802

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

"Los equipos deben tener la capacidad de operar y entender estas herramientas, combinando el conocimiento humano con la superautomatización que ofrece la IA"

es donde entra la IA, porque tiene la capacidad de procesar volúmenes de información que ningún ser humano puede manejar en tiempo real", afirma.
Además, los proveedores destacan la necesidad de simplificar la operación de plataformas de seguridad, especialmente en un contexto donde las empresas trabajan con muchas herramientas distintas. Sobre este punto, Juan Pablo Arias explica que hoy muchas organizaciones utilizan decenas de soluciones diferentes para abordar problemas específicos, y que el verdadero desafío no está en la cantidad de herramientas, sino en su integración efectiva.
"La clave está en cómo se integran todas esas soluciones y, sobre todo, en cómo el operador puede gestionarlas de forma sencilla. Hoy los fabricantes están incorporando PROMPTs que permiten interactuar en lenguaje natural con la plataforma, lo que reemplaza las antiguas líneas de comando y las consolas rígidas. Eso es un avance muy potente", comenta.
Además, prácticamente todas las herramientas tecnológicas actuales ya funcionan con IA. Lo que antes era un diferenciador, hoy es un estándar. Si una compañía no tiene soluciones como CDR (detección y respuesta basada en comportamiento), está quedando atrás. "Pero también hay un desafío: los equipos deben tener la capacidad de operar y entender estas herramientas, combinando el conocimiento humano con la superautomatización que ofrece la IA", agrega.

El avance de una herramienta accesible

El uso de esta tecnología ya es una práctica instalada que sigue perfeccionándose. Así lo explica Pablo Quiero,

LITORALPRESS

Fecha: 31-07-2025
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Noticia general
Título: Ciberseguridad hoy La Inteligencia Artificial en el centro de las estrategias

Pág. : 15
Cm2: 568,7
VPE: $ 801.804

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

quien destaca que tanto Fortinet como otras soluciones líderes del mercado han incorporado herramientas de IA de forma nativa, especialmente a través de agentes inteligentes que asisten a los operadores en el análisis de grandes volúmenes de información en tiempo real.

"Hoy la idea es tomar decisiones lo más rápido posible. Nosotros mismos desarrollamos un avatar de IA multipropósito, que permite interactuar por voz con el sistema y ejecutar acciones sin necesidad de comandos. Eso hace que la respuesta ante incidentes sea mucho más rápida y eficiente", señala.

Otro punto a favor de esta tecnología, además de su impacto en la eficiencia operativa, es que se trata de una herramienta accesible: "Si tuviéramos que desarrollar los servicios que hoy entregamos sin Inteligencia Artificial, nuestros costos en recursos humanos serían cuatro o cinco veces más altos", según el profesional de NEC.

Concuerda el ejecutivo de Netics: "Las soluciones basadas en IA, dependiendo del fabricante, han resultado ser bastante accesibles en términos de costos. Además, han permitido reducir significativamente la carga operativa, aumentando la productividad del operador".

En ese mismo sentido, Matías Vergara, Senior System Engineer de Noovus, complementó que estas herramientas no solo apoyan el análisis dentro del SOC, sino también en todo el ciclo de respuesta ante incidentes. "La IA ayuda a visualizar qué está pasando, a correlacionar cientos de logs, y luego a traducir toda esa información en reportes claros y útiles para el cliente. Ya no se trata solo de detectar, sino de entregar información comprensible. Y esto ya se está utilizando ampliamente, incluso a nivel de políticas públicas, como el programa lanzado por la Unión Europea junto con NIS2, que busca masificar el uso de tecnologías avanzadas como IA en ciberseguridad y estandarizarlo en frameworks como NIS, PCI o ISO 27001", explica el ejecutivo de Noovus.

> *"Para una estrategia de ciberseguridad sólida, hay que tener claro qué necesito proteger y cómo lo voy a proteger ¿Cuál es la información clave de mi negocio y cómo me afecta un ataque?"*

Cimientos de una estrategia sólida

Consultados sobre las claves para construir una estrategia de ciberseguridad sólida, los expertos coinciden en la necesidad de comenzar por lo esencial. "Hay que tener claro qué necesito proteger y cómo lo voy a proteger ¿Cuál es la información clave de mi negocio y cómo me afecta un ataque?", señala Roberth Castellanos. Y agrega: "No es lo mismo atacar a un banco que a una farmacia de barrio, por eso cada organización debe construir su cultura de seguridad desde sus propias prioridades". Concuerda el profesional de TCAM Technology, quien afirma que: "Siempre hay que partir por un diagnóstico: entender la situación actual y saber a dónde queremos llegar. Las herramientas como Fortinet son fundamentales, pero no bastan por sí solas. Todo debe ir acompañado de procesos y personas capacitadas para operar esas tecnologías".

Al respecto Jaime Aguilera agrega que el primer paso para toda organización es identificar su driver de valor: "¿Qué mueve su negocio? A partir de ahí, se puede definir una estrategia de ciberseguridad según el nivel de madurez, evaluado mediante un assessment o levantamiento, como los frameworks NIST o NIS2. Pero lo más importante es estar consciente de que los ataques ocurrirán. La pregunta ya no es si sucederán, sino cuándo".

En la misma línea, Matías Vergara recalca la importancia de implementar un marco de gobernanza: "Hay que construir una estrategia de GRC -Gobierno, Riesgo y Cumplimiento- para definir hacia dónde vamos y cómo nos mediremos. No se puede evolucionar sin tener claro contra qué estándares o marcos normativos estamos evaluando nuestro avance".

Más allá de las plataformas tecnológicas, contar con servicios que garanticen la observabilidad y una respuesta proactiva es esencial. Así lo destacó el profesional de Innova-Net: "Podemos tener las mejores herramientas, pero si el cliente no cuenta con un servicio que le permita ver lo que está pasando y reaccionar a tiempo, terminará siendo atacado".

Para Constanza Retamal, "toda estrategia parte por saber qué tengo y cuáles son mis riesgos. A partir de eso, puedo definir procedimientos, controles técnicos y recién ahí empezar a hablar de soluciones y tecnologías". Según Leonardo Leiva es necesario adoptar las herramientas, entenderlas y operarlas estratégicamente. "La invitación es a adoptar la herramienta, aprender de ella y ponerla en práctica. Con procesos bien definidos, se puede sacar verdadero provecho", asevera.

En un entorno digital cada vez más hostil, la IA ya no es una opción, sino un habilitador esencial para una ciberseguridad eficaz, adaptable y transversal.