DIARIO FINANCIERO®

Fecha: 25/08/2025 Audiencia: 48.450 Sección: ESPECIALES
Vpe: $2.919.231 Tirada: 16.150 Frecuencia: DIARIO
Vpe pág: $7.443.240 Difusión: 16.150
Vpe portada: $7.443.240 Ocupación: 39,22%

BRAND CORNER
WWW.DF.CL

PATROCINADO POR
Summit País Digital 2025

EL ROL DE LA IA EN LA RESILIENCIA ANTE CIBERATAQUES

La innovación en ciberseguridad será uno de los ejes que analizará la XIII edición del Summit País Digital. Sobre ello, el director de tecnología de SOLA para Trend Micro, Jhony Varela, plantea que la clave es usar la IA para el trabajo repetitivo y que el equipo humano gobierne.

En un mundo marcado por el auge y la masividad de uso de las nuevas tecnologías, la inteligencia artificial (IA) se ha vuelto un arma de doble filo para la seguridad informática. Mientras los cibercriminales la utilizan para desarrollar ataques cada vez más sofisticados, las organizaciones buscan la forma de explotar su potencial para automatizar su detección y respuesta.

Jhony Varela, director de tecnología de SOLA para Trend Micro.

El director de tecnología de SOLA para Trend Micro, Jhony Varela, explica que, en ese sentido, "la clave es usar la IA para que haga el trabajo pesado y repetitivo, y que el equipo humano tome las decisiones finas en la práctica".

Así, esta tecnología puede utilizarse, por ejemplo, para ordenar las alertas y priorizar una cantidad determinada de casos de acuerdo a su nivel de importancia e impacto en el negocio, para resumir incidentes en leguaje simple —qué pasó, a quién afecta, qué hacer— o disparar acciones seguras con aprobación humana como "aislar un equipo, bloquear un acceso, forzar un cambio de credenciales", dice Varela. Además, delinea que una vez que la Ley Marco de Ciberseguridad esté operativa, muchas compañías deberán "reportar incidentes al CSIRT nacional en tiempos acotados", por lo que la IA puede ayudar a acelerar el proceso de prellenado de los campos de reporte para que luego el analista los revise y envíe por el portal oficial.

A sus ojos, si bien prevenir todo es imposible, "lo que sí es posible es volver a operar rápido", asegura el ejecutivo. Sobre el nivel de preparación y resiliencia de las organizaciones locales, menciona que ven avances en el país, "pero la madurez es desigual", precisa, haciendo alusión a que muchas empresas aún confían en que "hay respaldo", cuando lo que vale actualmente es lograr una verdadera restauración y saber cuánto tardan en ello.

Para Varela, una organización preparada en este ámbito se reconoce porque tiene copias inmutables probadas, "un plan B de identidad" —es decir, si caen las cuentas privilegiadas, de igual manera puede levantar servicios esenciales— y un simulacro ejecutivo donde negocio, TI y comunicaciones practican juntos. "Si puedes demostrar que en horas o pocos días retomas la operación, que sabes a quién llamas primero y qué enciendes antes, estás del lado resiliente", puntualiza.

Desafíos

Ante la inminente entrada en vigor de la Ley Marco de Ciberseguridad, Varela asegura que el mayor desafío "no es técnico, es de organización". Y, para evaluar los riesgos a los que estas se exponen sin caer en tecnicismos, menciona que se deben utilizar "cuatro lentes": exposición (qué tiene la organización y qué se ve afuera), probabilidad (qué es más factible que exploten), impacto (cuánto duele al negocio) y madurez (qué tan bien previenen, detectan, responden y se recuperan). "Con eso construyes un índice de riesgo que el directorio entiende —un termómetro que sube o baja en minutos, horas o días— y lo combinas con escenarios simples (ransomware, terceros, identidad) expresados en pesos", complementa el ejecutivo.

Asimismo, destaca que actualmente cuentan con una plataforma de ciberseguridad capaz de dar visibilidad, priorizar y cuantificar el riesgo de forma proactiva y predictiva, y de sostener una evaluación continua que permite decidir qué hacer primero y mostrar, con datos, cómo va bajando el riesgo en cada iteración.