LITORALPRESS

Fecha: 25-08-2025
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: EL ROL DE LA IA EN LA RESILIENCIA ANTE CIBERATAQUES

Pág. : 31
Cm2: 636,5
VPE: $ 5.640.082

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

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.

LA TECNOLOGÍA COMO MOTOR DE LA GESTIÓN DE LA SEGURIDAD PÚBLICA

Las oportunidades que trae el uso integrado de tecnologías de detección y prevención, comunicación segura y respuestas automatizadas para el fortalecimiento de la seguridad pública, es parte de lo que el gerente general de SONDA Chile, Javier Larenas, abordará en el Summit País Digital 2025.

La seguridad pública enfrenta hoy el desafío de adaptarse a un entorno cada vez más complejo, donde la coordinación y el uso compartido de información entre las instituciones es crucial para el manejo de hechos delictuales.

Javier Larenas, gerente general de SONDA Chile.

Al analizar la contingencia nacional en este ámbito, el gerente general de SONDA Chile, Javier Larenas, plantea que uno de los principales desafíos que enfrenta el país es la fragmentación de los sistemas de seguridad entre distintas instituciones, ya sean públicas o privadas, pues "esta falta de interoperabilidad limita la capacidad de respuesta coordinada y eficiente ante incidentes". A ello, añade que aún existe una brecha en la infraestructura tecnológica utilizada y en la adopción de herramientas que permitan operar soluciones avanzadas, a través de la capacitación de los equipos humanos.

En ese contexto, Larenas asegura que han identificado que para lograr una visión unificada del territorio y una respuesta más rápida y efectiva, es fundamental integrar plataformas que permitan la interoperabilidad de sistemas diversos. "Un ejemplo reciente es la iniciativa de la Subsecretaría de Prevención del Delito a través de SITIA, en la que, con el apoyo de SONDA, se conectaron cámaras de vigilancia de municipios, autopistas y centros comerciales, con la central de Carabineros, generando una red colaborativa de monitoreo", destaca el ejecutivo.

Actualmente, hay múltiples tecnologías disponibles para prevenir, anticipar y responder de forma eficiente a incidentes de seguridad, dice Larenas, y hace énfasis en que la compañía utiliza cuatro soluciones claves para resolver este tipo de desafíos: Smart Platform, IoT Platform, Event Manager, Asset Manager y Urban Monitor. Estas aportan funcionalidades como monitoreo y seguimiento en tiempo real, mediante cámaras inteligentes y sensores conectados; análisis e inteligencia de datos, que permiten anticipar patrones de riesgo y tomar decisiones informadas; sistemas de comunicación y alerta temprana, que facilitan la coordinación entre instituciones; identificación y control de acceso, para proteger espacios críticos; y control territorial y gestión de emergencias, que permiten actuar rápidamente ante situaciones críticas. "Estas herramientas no solo mejoran la eficiencia operativa, sino que también promueven una gestión proactiva de la seguridad pública", complementa el gerente general de SONDA Chile.

Lo que se necesita

Para implementar este tipo de soluciones de forma segura y escalable en el país, "es fundamental avanzar hacia una coordinación y eventualmente modificaciones a las normativas vigentes, que faciliten la interoperabilidad tecnológica entre organismos públicos y privados, respetando los estándares de seguridad y protección de datos", afirma Larenas.

Además, expresa que se requiere una coordinación interinstitucional robusta, con protocolos claros de colaboración y uso compartido de información. A modo de ejemplo, el ejecutivo señala que es clave poder contar con capacidades de identificación de identidad de personas en línea cuando se realizan controles para detectar si tienen órdenes de detención pendientes o en el caso de vehículos con encargo por robo.

"Es importante que aparte de Carabineros, las municipalidades pudieran tener acceso a consulta de estos datos", añade, en caso, por ejemplo, de que se realice una identificación biométrica de personas que no portan su identificación.

A sus ojos, se trata de establecer marcos de gobernanza tecnológica, que faciliten la adopción de innovación sin comprometer la privacidad ni la seguridad de los ciudadanos.

Diario Financiero
https://www.df.cl

Web
https://summit.paisdigital.org/