LITORALPRESS

Fecha: 10-10-2024
Medio: El Mercurio
Supl. : El Mercurio - Innovacion
Tipo: Noticia general
Título: **“Chile es uno de los países de América Latina que más esfuerzos ha puesto en desarrollar políticas públicas y fortalecer su infraestructura digital”**

Pág. : 4
Cm2: 933,2

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

CARLOS SEISDEDOS, CEO DE MAGNETO INTELLIGENCE:

“Chile es uno de los países de América Latina que más esfuerzos ha puesto en desarrollar políticas públicas y fortalecer su infraestructura digital”

Para el experto en ciberseguridad y ciberinteligencia, este último concepto es clave para que las organizaciones o empresas estén preparadas o incluso puedan prevenir un posible ataque. A nivel país, ve con buenos ojos los avances que se han dado, pero asegura que aún hay camino por recorrer: “Es fundamental implementar una serie de acciones estratégicas que refuercen su capacidad de proteger el ciberespacio y mejorar su preparación frente a amenazas emergentes”.

MARIA JESÚS COLOMA

Carlos Seisdedos, CEO de Magneto INTelligence.

Hoy en día la mayoría de la información circula en el mundo digital, lo que implica un mayor cuidado del ciberespacio y, por ende, avances e inversiones principalmente destinadas en materia de ciberseguridad. No obstante, hay un concepto previo con el que se puede contar de manera de ser proactivos y preventivos ante un ataque y es por medio de la ciberinteligencia.

El español Carlos Seisdedos, CEO de Magneto INTelligence, cuya experiencia se centra en el análisis criminal y la ciberinvestigación, con un enfoque particular en el uso del ciberespacio por parte del cibercrimen y los ciberterroristas, se ha especializado en esta materia y la define como “capa por encima de la ciberseguridad que permite analizar información de forma previa y así prevenir o estar más preparados frente a un ataque”.

Sobre este tema, sus implicancias, sus avances y cómo está Chile al respecto profundiza Seisdedos, quien además es investigador y analista de inteligencia especializado en seguridad internacional y digital.

—¿Qué es la ciberinteligencia?

“Por defecto, muchas veces las personas asocian la palabra inteligencia a espías, al lado negativo y no tiene nada que ver. Cuando hablamos de ciberinteligencia, lo que estamos hablando es que hay un superior que tiene una incertidumbre sobre algo y, en ese caso, la inteligencia lo que va a hacer es ayudar a tener certezas para tomar una decisión a través de toda la información que se pueda recopilar, analizar, procesar y ayudar a solventar o minimizar la toma de decisión. Pero, sobre todo cuando hablamos de ciberinteligencia, es proactividad. No vamos a esperar que pase algo, sino que vamos a tomar las medidas correctas. Vamos a tomar las medidas suficientes para obtener esos datos que nos ayuden a adelantar”.

—¿Cuál es la diferencia entonces entre ciberinteligencia y ciberseguridad?

“Principalmente, desde mi punto de vista, cuando hablamos de ciberseguridad, estamos hablando de herramientas o técnicas que lo que intentan es que nuestro entorno y organización sean seguros. Esto para prevenir ataques o como mínimo tener una capacidad de reacción en el caso de sufrir uno. En cambio, con la ciberinteligencia estamos hablando más allá de la fase para detener un ataque. Es una capa por encima de la ciberseguridad que nos va a ayudar a hacer una interconexión de toda esa información para poder analizarla en contexto. No únicamente de forma aislada.”

—¿Qué beneficios tiene para las organizaciones o empresas contar con cibertinteligencia?

“Al final lo que esto facilita es, por un lado, a nivel de ciberseguridad, ampliar la capacidad de anticipación de la empresa frente a posibles ataques, porque con ciberinteligencia es posible adelantarse a un potencial ataque. Lo que nos permite hacer es una monitorización activa del ciberespacio para así detectar campañas incipientes que puedan dañar a la empresa o la organización. Por ejemplo, con la herramienta de ciberinteligencia se puede detectar previamente si habrá una campaña de desinformación contra de la empresa. Al percatarse de eso se pueden tomar alternativas para tomar acciones legales, por ejemplo, o hacer algo antes de que esto ya esté operando y sea mucho más difícil detenerlo”.

—¿Cuáles son los costos monetarios para adquirir o avanzar en una mayor ciberinteligencia?

“Hay un gran desconocimiento sobre le ciberinteligencia, porque muchas veces se cree que implica comprar más herramientas, más aparatos y que sean más gastos. Sin embargo, por defecto esos aparatos ya los tienes, pero el que realmente proporciona la ciberinteligencia es el analista y eso no es algo caro. Seguramente lo que se paga por licencias u otras nuevas herramientas es el sueldo de tres analistas en un año. El problema es que hay desconocimiento, porque lo primero que hay que hacer es proporcionar esos datos a un analista que te proporcione inteligencia. Por ejemplo, muchas veces se cree que por comprar dos o tres herramientas se tiene un Ferrari, pero lo que se tiene en realidad son las piezas del Ferrari. Acá lo que verdaderamente se necesita es un analista de inteligencia que sea capaz de montarte esas piezas de una forma conjunta para que realmente sea un Ferrari”.

—¿Hay profesionales capacitados para desarrollar la ciberinteligencia o se debe avanzar en esa formación?

“Muchas veces en vez de gastarte el dinero en herramientas tan grandes, es mejor coger un analista y prepararlo. Porque al final la mayoría de las empresas tiene personal que está trabajando en ciberseguridad. En ese caso se les debiese dar una capacitación específica, en la que se puedan añadir habilidades de análisis y metodología de ciberinteligencia. No se trata de cambiar a los profesionales, sino que muchas veces los tenemos, pero tenemos que capacitarlos en otros ámbitos”.

—¿Cómo debieran avanzar los países para contar con una mayor cibertinteliengencia?

“Para que los países puedan avanzar hacia una mayor capacidad en ciberinteligencia, es crucial adoptar una estrategia multidimensional. En primer lugar, es imperativo invertir en la formación continua y especialización de profesionales en ciberinteligencia y ciberseguridad. Esto, puede lograrse mediante programas educativos formales, certificaciones especializadas y talleres de alto nivel que no solo incrementen el número de expertos, sino que también optimicen las competencias de los equipos existentes. Por otro lado, la colaboración internacional es otra pieza clave. Establecer alianzas estratégicas con otros países y organismos globales facilita el intercambio de información y lecciones aprendidas, permitiendo a los países fortalecer sus capacidades y adoptar las mejores prácticas frente a las amenazas emergentes”.

DIFERENCIAS REGIONALES

—¿En qué se diferencian Europa y América Latina en esta materia?

“Europa y América Latina presentan diferencias significativas en el desarrollo de la ciberinteligencia, debido a la infraestructura, la legislación, la cooperación internacional y la formación de profesionales en cada región. En Europa, los países han avanzado considerablemente en la creación de infraestructuras tecnológicas más sólidas y homogéneas, lo que les permite tener una mejor respuesta a las amenazas cibernéticas. En cambio, América Latina muestra capacidades desiguales entre sus países, lo que dificulta una respuesta uniforme y eficaz ante los incidentes de ciberseguridad”.

—Entonces, ¿cómo debiera avanzar América Latina?

“Para que América Latina pueda avanzar y alcanzar un nivel similar al de Europa en ciberinteligencia, es fundamental priorizar la capacitación de sus profesionales, con programas educativos especializados y certificaciones de alto nivel que sigan el modelo europeo. Además, los países de la región deben desarrollar políticas públicas claras y coherentes que regulen la ciberseguridad y promuevan la cooperación entre el sector público y privado. También es esencial fortalecer la cooperación internacional, tanto dentro de América Latina como con otras regiones, para compartir conocimientos y recursos que mejoren la capacidad de respuesta ante incidentes. Aumentar la inversión en tecnología avanzada e infraestructura también es clave. Los gobiernos y empresas deben implementar soluciones de ciberinteligencia basadas en inteligencia artificial y análisis de datos para proteger mejor sus infraestructuras críticas. Además, se debe promover una cultura de ciberseguridad a todos los niveles, concienciando a la ciudadanía y al sector privado sobre los riesgos cibernéticos y las mejores prácticas para mitigarlos”.

—¿Como ve a Chile en particular en materias de ciberseguridad y ciberinteligencia?

“Chile ha mostrado avances significativos en el campo de la ciberseguridad y la ciberinteligencia en los últimos años, es uno de los países de América Latina que más esfuerzos ha puesto en desarrollar políticas públicas y fortalecer su infraestructura digital. Aunque enfrenta retos importantes, ha demostrado un compromiso claro por mejorar su resiliencia frente a las amenazas cibernéticas”.

—¿En qué se ve reflejado ese avance?

“Uno de los pasos más importantes ha sido la creación de la Red Nacional de Ciberseguridad, que ha permitido coordinar esfuerzos entre diferentes organismos del Estado y el sector privado para enfrentar los riesgos cibernéticos. Este enfoque colaborativo es clave para garantizar una respuesta rápida y eficiente ante incidentes de seguridad. Además, Chile ha trabajado en la actualización de su marco legal, incluyendo la modernización de su Ley de Protección de Datos Personales, un paso fundamental para alinear su normativa con estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.”

—Y específicamente en materia de ciberinteligencia, ¿Cree que en Chile hay avances?

“En cuanto a la ciberinteligencia, Chile ha ido desarrollando capacidades en la recolección y análisis de datos para anticipar y mitigar ciberamenazas, aunque aún tiene margen para fortalecer esta área. La creación de capacidades de análisis más avanzadas, la integración de herramientas de inteligencia artificial y *machine learning*, y el desarrollo de talento especializado son aspectos que pueden potenciar el crecimiento de la ciberinteligencia en el país”.

—¿Qué recomendaciones podrías hacer para avanzar y mejorar en esta materia?

“Para que Chile continúe avanzando en ciberseguridad y ciberinteligencia, es fundamental implementar una serie de acciones estratégicas que refuercen su capacidad de proteger el ciberespacio y mejorar su preparación frente a amenazas emergentes. Algunas recomendaciones claves serían, la inversión en tecnología avanzada, ya que Chile debe seguir invirtiendo en tecnologías emergentes como la inteligencia artificial (IA), *machine learning* y análisis de *big data* para mejorar la capacidad de detección y respuesta a ciberamenazas. Asimismo, es crucial que se desarrollen programas educativos y de certificación para formar profesionales especializados en ciberseguridad y ciberinteligencia, fomentando así la capacitación continua de los analistas actuales y asegurando que estén al día con las últimas tecnologías y amenazas. También es relevante la promoción de una cultura de ciberinteligencia transversal, fortaleciendo las capacidades técnicas y creando conciencia en todos los niveles de la sociedad sobre la importancia de la ciberinteligencia como elemento proactivo. Por último, la colaboración público-privada es esencial para compartir información y recursos en tiempo real, permitiendo una respuesta más rápida y efectiva a los incidentes cibernéticos, estableciendo marcos formales de colaboración, como grupos de trabajo conjuntos o centros de intercambio de información. Todo esto permitirá que Chile pueda mejorar su postura en ciberseguridad”.