LITORALPRESS

Fecha: 23-01-2025
Medio: El Mercurio
Supl. : El Mercurio - Innovacion
Tipo: Noticia general
Título: La nube bajo ataque: el desafío de proteger datos en un mundo digital

Pág. : 6
Cm2: 921,9
VPE: $ 12.110.023

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

POR UN LADO IMPULSA LA TRANSFORMACIÓN DIGITAL, PERO TAMBIÉN CONLLEVA RETOS CRÍTICOS EN SEGURIDAD

La nube bajo ataque: el desafío de proteger datos en un mundo digital

Con un crecimiento exponencial en el uso de la nube, expertos advierten sobre las amenazas emergentes y comparten estrategias para garantizar la seguridad de los datos en un entorno virtual cada vez más complejo. **FERNANDA GUAJARDO**

La transformación digital ha alcanzado un nuevo nivel con la adopción masiva de la tecnología en la nube, que permite a las empresas optimizar procesos, escalar sus operaciones y acceder a herramientas avanzadas como la inteligencia artificial (IA). Sin embargo, este avance también ha generado un panorama desafiante en materia de ciberseguridad. Cuatro expertos analizan los beneficios y riesgos de esta tecnología clave para el futuro de las organizaciones.

UN HABILITADOR DE TRANSFORMACIÓN DIGITAL

Ángel Izurieta, *country manager* de Google Cloud Chile, destaca que "la nube ha pasado de ser una simple opción a un motor esencial para la transformación digital de las empresas". Según el ejecutivo, esta tecnología facilita la integración de la IA en sectores diversos como la minería, el retail y las telecomunicaciones, permitiendo una mejora significativa en la eficiencia y la toma de decisiones. Empresas chilenas como Camanchaca ya han adoptado agentes de IA generativa para optimizar sus procesos operativos, ejemplificando el potencial de esta tecnología.

El impacto de la nube también se refleja en la manera en que las empresas gestionan sus recursos humanos y financieros. Izurieta señala que "el uso de la IA y la nube en conjunto permite automatizar procesos rutinarios, liberando así recursos para centrarse en la innovación y la estrategia". Este cambio no solo mejora la competitividad de las empresas, sino que también les permite adaptarse más rápidamente a las demandas del mercado.

Además, destaca que la nube ha permitido a empresas de menor tamaño acceder a tecnologías que anteriormente solo estaban disponibles para grandes corporaciones. Esto, dice, democratiza el acceso a herramientas avanzadas y fomenta la innovación en sectores como las *startups*, que encuentran en la nube un aliado para escalar sus modelos de negocio de manera eficiente y rentable.

Sin embargo, Izurieta también subraya la importancia de invertir en la formación de talento calificado en áreas como la ciberseguridad y la gestión de datos: "El rápido avance de la tecnología no ha ido acompañado de una capacitación equivalente. Esto representa una oportunidad crucial para las empresas y universidades".

AMENAZAS EN UN ENTORNO MULTICLOUD

Ernesto Tachoires, director regional de desarrollo de negocios de ciberseguridad de Sonda, advierte que "los entornos multicloud —es decir, cuando una empresa utiliza servicios de computación en la nube de al menos dos proveedores distintos para gestionar y operar sus aplicaciones—, traen beneficios significativos, pero también amplían la superficie de ataque para los ciberdelincuentes". Entre las amenazas más comunes, menciona configuraciones erróneas, ataques a API y la problemática del Shadow IT, donde aplicaciones fuera del control corporativo introducen vulnerabilidades.

Tachoires también pone énfasis en el creciente riesgo de ataques a la cadena de suministro en entornos *cloud*. "Las dependencias de servicios externos y librerías de código abierto han incrementado la exposición a vulnerabilidades que pueden ser explotadas a gran escala", explica. Este tipo de ataques, combinados con la sofisticación de herramientas basadas en IA, requieren un enfoque integral de seguridad.

Para abordar estos riesgos, Tachoires recomienda adoptar estrategias como la implementación de controles de seguridad desde las primeras etapas de migración a la nube y el uso de tecnologías avanzadas como CNAPP (Cloud Native Application Protection Platform). Asimismo, enfatiza la importancia de la capacitación continua y la implementación de un modelo de responsabilidad compartida con los proveedores de nube.

También sugiere que las organizaciones evalúen de manera periódica su postura de seguridad mediante pruebas de penetración y simulaciones de incidentes. "La seguridad no es un producto, sino un proceso continuo que debe ajustarse a medida que evolucionan las amenazas", concluye.

COLABORACIÓN PÚBLICO-PRIVADA: UNA NECESIDAD URGENTE

Fernando Sánchez, gerente general de Fundación País Digital, resalta que "la colaboración entre los sectores público y privado es esencial para enfrentar las amenazas crecientes en la nube". Según el Global Cybersecurity Outlook 2025 del Foro Económico Mundial, los ataques basados en *ransomware* e IA continúan evolucionando, mientras que dispositivos IoT y cadenas de suministro también representan puntos críticos de vulnerabilidad.

En este contexto, Sánchez celebra la entrada en vigencia de la Ley Marco de Ciberseguridad en Chile, una legislación que, en su opinión, "impulsará a las organizaciones a fortalecer sus estrategias de seguridad y a capacitar a su personal, promoviendo una cultura de prevención y resiliencia".

El ejecutivo señala que esta colaboración no solo debe enfocarse en prevenir ataques, sino también en promover la innovación responsable: "Es fundamental que las organizaciones no solo se protejan, sino que también encuentren formas de utilizar la tecnología para impulsar cambios positivos en la sociedad".

Un ejemplo de esta colaboración es el desarrollo de iniciativas conjuntas entre gobiernos y empresas para compartir inteligencia sobre ciberamenazas. Este tipo de alianzas permite identificar patrones de ataque y responder de manera más eficaz a incidentes que podrían tener un impacto masivo.

EL PAPEL DE LA INTELIGENCIA ARTIFICIAL

Javier Ferraro, senior *cloud security engineer-tech* LAD en Oracle, destaca el papel transformador de la IA en la ciberseguridad: "La IA permite detectar y responder a amenazas en tiempo real, analizando patrones de comportamiento anómalos y automatizando tareas como la gestión de vulnerabilidades". Además, subraya que la adopción masiva de arquitecturas de confianza cero (Zero Trust) ha sido impulsada por la necesidad de reforzar los controles de acceso en entornos más distribuidos.

Ferraro también insta a las empresas a considerar la migración a la nube como una necesidad, no solo por los beneficios operativos, sino también por la oportunidad de mejorar significativamente su postura de seguridad. "Migrar a la nube con una estrategia bien definida permite a las organizaciones aprovechar herramientas de seguridad avanzadas que no estarían al alcance de muchas si no fuera por los proveedores de nube", sostiene.

En este sentido, destaca que la IA no solo ayuda a prevenir ataques, también permite a las organizaciones anticiparse a amenazas futuras mediante el análisis predictivo. Este enfoque proactivo, explica, es clave para mantenerse un paso adelante en un entorno de ciberseguridad que cambia rápidamente.

Ferraro enfatiza que sectores como la salud y las finanzas son particularmente vulnerables debido al alto valor de los datos que manejan. Por ello, la implementación de estrategias robustas, como la encriptación de datos y la autenticación multifactor, resulta fundamental para mitigar riesgos.

UN FUTURO PROMETEDOR Y DESAFIANTE

La nube sigue siendo un catalizador clave de la transformación digital, pero su implementación también requiere un enfoque riguroso en seguridad. Desde la adopción de estrategias de seguridad proactivas hasta la colaboración entre sectores, las organizaciones tienen la oportunidad de aprovechar al máximo esta tecnología mientras mitigan sus riesgos.

En palabras de Ángel Izurieta: "La nube no solo está revolucionando la manera en que las empresas operan, sino también cómo garantizan la seguridad de sus datos y operaciones. El desafío está en equilibrar la innovación con una protección robusta".

A medida que la nube se convierte en un pilar fundamental para la economía digital, la adaptación constante y el aprendizaje continuo serán esenciales para enfrentar los retos que trae consigo. Como explican los expertos, con estrategias bien definidas, colaboración público-privada y una mentalidad de innovación responsable, las empresas pueden asegurar un futuro donde la nube sea sinónimo de progreso y seguridad.

"La colaboración entre los sectores público y privado es esencial para enfrentar las amenazas crecientes en la nube".

FERNANDO SÁNCHEZ
Gerente general
Fundación País Digital.

"Migrar a la nube con una estrategia bien definida permite a las organizaciones aprovechar herramientas de seguridad avanzadas que no estarían al alcance de muchas".

JAVIER FERRARO
Senior cloud security engineer-tech
LAD de Oracle.

"La nube no solo está revolucionando la manera en que las empresas operan, sino también cómo garantizan la seguridad de sus datos y operaciones".

ÁNGEL IZURIETA
Country manager
de Google Cloud Chile.

"La seguridad no es un producto, sino un proceso continuo que debe ajustarse a medida que evolucionan las amenazas".

ERNESTO TACHOIRES
Director regional de desarrollo de negocios de ciberseguridad de Sonda.