Seguridad en la nube y el futuro

DOI: 10.29236/sistemas.n171a3

Javier Díaz Evans experto en ciberseguridad y líder en dirección aceptó la convocatoria para entrevistarlo alrededor de la seguridad en la nube y el futuro en este número de la revista.

"Existen personas muy importantes en mi desarrollo profesional, entre ellos César Tarazona, mi gran mentor, quien aportó en mi carrera el conocimiento técnico y la experiencia para evolucionar y desarrollarme en el frente de ciberseguridad y Julio Leonzo Álvarez quien me apoyó en el desarrollo de mis capacidades de liderazgo y dirección", señaló Javier Díaz Evans.

El entrevistado es ingeniero electrónico, especialista en Telemática de la Universidad de los Andes y eMBA de Inalde Business School. Cuenta con más de 20 años de experiencia en el campo de la ciberseguridad, ha desempeñado un papel clave en la evolución y expansión de A3SEC desde su fundación en 2012, como un spin-off de AlienVault y Teldat; A3SEC ha cre-

cido bajo su liderazgo para convertirse en una empresa líder en soluciones de ciberseguridad, operando en España, Colombia, Ecuador y México, con planes de expansión hacia Europa y Estados Unidos, agregó.

Javier Díaz Evans ha sido pionero en la adopción de una estrategia basada en la inteligencia de datos, la hiperautomatización y el uso de IA/ML, transformando la forma en que las organizaciones protegen sus activos digitales.

Antes de A3SEC, acumuló una vasta experiencia como proveedor y consultor de seguridad, así como CISO (Chief Information Security Officer) de un conglomerado financiero, lo que le ha permitido tener una visión integral y práctica de las necesidades del sector.

Revista Sistemas: *¿Es la computación confidencial el futuro de la seguridad en la computación en la nube?*

Javier Díaz Evans: Tradicionalmente, la protección de datos se ha centrado en el resguardo y la transmisión, pero la confidencialidad del procesamiento de datos solo se había abordado para elementos muy sensibles utilizando soluciones como los HSM (Módulos de Seguridad en Hardware) y los EPP (Pin Pad Cifrados). La computación confidencial promete extender esta protección al procesamiento de datos en entornos de nube, pero enfrenta varios retos significativos:

- Estándares y Regulaciones: La falta de normas unificadas y regulaciones claras puede dificultar la adopción generalizada.
- Rendimiento: Mantener un alto nivel de rendimiento mientras se garantiza la seguridad es un desafío técnico.

- Interoperabilidad: Es crucial asegurar que las soluciones de computación confidencial funcionen eficientemente en diferentes plataformas y con otros sistemas de seguridad.
- Adopción del Mercado: Convencer a las organizaciones del valor y la necesidad de invertir en estas tecnologías es un reto.
- Complejidad Técnica: Implementar y gestionar entornos de ejecución confiables (TEE) requiere conocimientos avanzados y recursos significativos.
- Ataques Sofisticados: Es necesario desarrollar métodos para protegerse contra ataques cada vez más sofisticados que buscan explotar vulnerabilidades en los TEE.

Aunque la computación confidencial tiene un gran potencial, el futuro podría ver la aparición de otras tecnologías emergentes que transformen este paradigma de la seguridad en la nube. La evolución constante en el ámbito de la seguridad cibernética significa que debemos estar preparados para adaptarnos a nuevas soluciones que puedan ofrecer aún más protección y eficiencia.

RS: *Si una organización quiere incorporar la computación confidencial en sus prácticas y despliegues actuales, ¿cuál sería la hoja de ruta a seguir?*

JDE: Para incorporar la tecnología de computación confidencial en una organización y garantizar que nos preparemos para enfrentar los desafíos y maximizar los beneficios es necesario seguir una hoja de ruta detallada, comparto algunas ideas:

1. Desarrollar Conocimientos y Capacidades:
- Fortalecer las competencias internas sobre el paradigma de la computación confidencial.
2. Evaluación Inicial:
- Realizar un análisis de las necesidades de negocio, inventario, flujos y clasificación de datos, así como de los riesgos actuales de ciberseguridad y privacidad.
3. Diseño de Arquitectura:
- Seleccionar los estándares y tecnologías más adecuadas, planificando la integración con las soluciones existentes y definiendo políticas y estándares específicos.
4. Prueba Piloto:
- Implementar una prueba piloto para evaluar la seguridad y el rendimiento, permitiendo realizar ajustes y optimizaciones necesarias antes del despliegue a gran escala.
5. Plan de Despliegue:
- Establecer un plan de migración gradual de la tecnología, con monitoreo constante y soporte continuo para asegurar una transición fluida.
6. Estrategia de Gobernanza:
- Desarrollar una estrategia de gobernanza que incluya evaluaciones periódicas de ciberseguridad, actualizaciones tecnoló-

gicas y la integración en procesos de gestión de fallos e incidentes.

7. Evaluación de Impacto:

- Medir y evaluar los resultados obtenidos con la nueva tecnología, generando retroalimentación continua para mejorar y ajustar la implementación según sea necesario.

RS: *¿Cuáles podrían ser los retos más importantes a tener en cuenta para una organización si quiere incorporar la computación confidencial en su infraestructura y aplicaciones?*

JDE: La respuesta fue planteada en la primera pregunta para validar si es el futuro de la computación en la nube, pero si analizamos los más importantes diría que son:

- Rendimiento.
- Interoperabilidad.
- Ataques Sofisticados.

RS: *¿Cómo encaja la computación confidencial con las actuales medidas de seguridad desplegadas en la nube como son XDR, SOAR, entre otras?*

JDE: La computación confidencial, al centrarse en el cifrado integral de los datos, plantea retos y oportunidades para los sistemas de seguridad en la nube.

Desafíos en Detección y Respuesta:

- Cifrado de Datos en Tránsito: Los sistemas de detección de intrusos (IDS) y su evolución NDR (Network Detection & Response) que analizan el tráfico de red pueden encontrar limitaciones al analizar datos cifrados, afectando su visibilidad y capacidad de detección de amenazas.
- Sistemas EDR: Podrían enfrentar dificultades para identificar ciertas tácticas y técnicas que implican acceso y procesamiento de datos cifrados, requiriendo una evolución en sus capacidades de detección.
- Integración y Evolución de Controles:

- XDR y SOAR: Estas soluciones, que combinan múltiples fuentes de datos y capacidades de respuesta automatizada, necesitarán adaptarse para gestionar y analizar datos en entornos de computación confidencial. Esto implica actualizar metodologías y procesos de ingeniería de detección para mantener y mejorar la eficacia en la identificación de amenazas, incluso con datos cifrados.

- Complementariedad:

- Analítica de Ciberseguridad: Herramientas de analítica avanzadas pueden complementar las capacidades de detección y respuesta de XDR y SOAR, asegurando que no se pierdan capacidades críticas para reducir el tiempo de exposición ante ataques.

En resumen, la computación confidencial exige una evolución en las herramientas de seguridad actua-

les para integrarse eficazmente, manteniendo y potenciando las capacidades de detección y respuesta.

RS: *¿Qué nuevos desarrollos se ven a futuro para la computación confidencial?*

JDE: La computación confidencial está avanzando con el desarrollo de procesadores que incorporan tecnologías para proteger la ejecución de código y datos. Estos procesadores permiten aislar la ejecución del sistema operativo y las aplicaciones, mejorando así la privacidad de datos.

Además, están surgiendo nuevos modelos criptográficos que facilitan realizar cálculos con datos cifrados sin necesidad de descifrarlos previamente. Esto no solo fortalece la privacidad, sino que también puede mejorar el rendimiento de las aplicaciones.

Otro avance importante es la computación distribuida confidencial, que permite a múltiples entidades colaborar en el cálculo de funciones sin revelar sus datos de entrada individuales. Este enfoque preserva la privacidad y la integridad de los datos entre los participantes.

Finalmente, se esperan desarrollos significativos en normativas y estándares, que jugarán un papel crucial en la regulación y adopción de estas tecnologías seguras a nivel global.