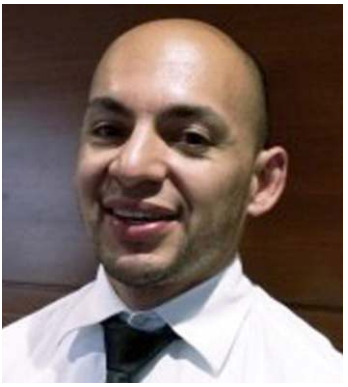
Computación confidencial

DOI: 10.29236/sistemas.n171a1

El reto de la seguridad y el control de los datos "en uso".



Jeimy J. Cano M.

Andrés R. Almanza J.

La dinámica de los datos tanto a nivel empresarial como global, implica reconocer los retos, los tratamientos y los flujos de información que determinan las diferentes ventajas competitivas de las naciones y los negocios. En este sentido, la protección de los datos en sus tres estados actuales: *en reposo* (almacenados en servidores y equipos de usuario final), *en movimiento* (a través de redes y conectores entre aplicaciones) y *en uso* (en la ejecución y procesamiento de las aplicaciones) se convierte en un escenario de acción conjunta entre organi-

zaciones y terceros de confianza para lograr un mayor aseguramiento de sus operaciones y por tanto, concretar la promesa de valor para sus clientes.

Una reciente encuesta latinoamericana realizada por la consultora internacional EY (2024) indica que los ejecutivos de las empresas de esta región consideran al menos las siguientes tecnologías como claves para su desarrollo en los próximos tres años: grandes datos & analítica, computación en la nube, inteligencia artificial y conectividad 5G.

En este escenario, el tratamiento de los datos a nivel de las aplicaciones se vuelve más sensible habida cuenta que, es en su explotación (la de los datos), donde se concreta el nuevo valor para los clientes, lo que implica un mayor procesamiento y uso por parte de las aplicaciones representadas en las nuevas iniciativas digitales generalmente desplegadas en la nube.

La computación confidencial tiene como objetivo "cifrar los datos en uso en la memoria principal del sistema sin comprometer el rendimiento. Lo anterior implica que los datos en memoria tienen dos aspectos claves:

- Cifrado de toda la memoria del sistema, y
- Cifrar la memoria individual de la máquina virtual (MV) y aislar la memoria de la MV del hipervisor (el hipervisor es un tipo de software informático, firmware o hardware que crea y ejecuta máquinas virtuales)" (Felk, 2023).

El reconocer que los datos "en uso" son el nuevo reto de las organizaciones modernas, ahora motivadas por una acelerada transformación digital y el desarrollo de nuevos ecosistemas digitales de negocio, implica actualizar el paradigma de seguridad y control vigente de las empresas que ha puesto el énfasis en los datos "en reposo" y en los datos "en tránsito". En este sentido, se advierten una serie de desafíos tanto para las organizaciones como para sus terceros de confianza para concretar y asegurar la confianza digital que los clientes demandan en un entorno cada vez más interconectado y dinámico como el actual. Algunos de los retos son: (CCC, 2021)

- Establecer un inventario de aplicaciones que requiere la implementación urgente de las características de la computación confidencial.
- Invertir en la formación de talento especializado que permita apalancar las nuevas iniciativas alrededor de la computación confidencial y cerrar la brecha que esto supone.
- Identificar los socios estratégicos en sus terceros de confianza para apalancar el aseguramiento de los datos extremo a extremo con el fin de aumentar la confiabilidad de la operación y el

aseguramiento de las exigencias normativas alrededor de los datos.
- Crear casos de negocio con los socios estratégicos para invertir de forma proactiva en el desarrollo de pruebas de concepto que muestren las oportunidades de la computación confidencial sobre sus aplicaciones críticas.
- Cuidar los elementos claves de la transición hacia un entorno de computación confidencial, lo que implica mantener entornos híbridos y mixtos en la operación, con una hoja de ruta clara y validada tanto por los objetivos de negocio como por los socios estratégicos.

En una organización centrada en la protección y defensa de los datos y la información, tanto de su dinámica empresarial como la de sus clientes, la computación confidencial se transforma en el estándar base de seguridad y control que asegura un adecuado procesamiento de los datos, cuidando no sólo la sensibilidad de la información que produce la compañía, sino el cumplimiento de la responsabilidad que implica el cuidado de la información que entregan los clientes al utilizar cada una de sus aplicaciones o iniciativas digitales.

Es por esto que esta edición de la revista *Sistemas*, de la Asociación Colombiana de Ingenieros de Sistemas −ACIS−, apunta a revisar, explorar y analizar los retos y oportunidades de la computación confidencial, con el fin de traer al escenario actual diferentes posturas sobre el tema, como insumo para plantear alternativas y opciones en un entorno de disrupción tecnológica acelerada. Con ese propósito fueron convocados profesionales especialistas, quienes desde su experiencia proponen reflexiones para seguirle la pista al desarrollo de las tendencias y prácticas vigentes en esta temática, capitalizando lecciones aprendidas, casos de estudio, repensando las dinámicas de los negocios y retos actuales, así mismo explorar el futuro que se avizora en el horizonte.

La ingeniera Sandra Rueda, profesora asociada del Departamento de Ingeniería de Sistemas y Computación de la Universidad de los Andes, columnista invitada, aborda algunas reflexiones sobre las tendencias y retos de la computación confidencial en la actualidad.

La entrevista efectuada al ingeniero Javier Evans, Director General Global firma A3SEC, revela aspectos prácticos de los retos de la computación confidencial y establece algunas orientaciones tanto para los profesionales en seguridad/ciberseguridad sobre este nuevo paradigma de protección datos en la nube que demanda repensar la vista de los diferentes estados de los datos y la infraestructura de hardware que se requiere para dar cuenta de las promesas de este nuevo avance en seguridad y control.

La investigación a cargo del ingeniero Andrés Almanza Junco, es el resultado del ejercicio continuado de la Asociación Colombiana de Ingenieros de Sistemas para tomarle el pulso a la evolución y transformación de las prácticas de seguridad/ciberseguridad en Colombia. Los resultados muestran entre otros aspectos como la confianza digital y la ciberresiliencia se convierten generadores de nuevos negocios, como elementos claves para cultivar las relaciones entre consumidores y quienes ofrecen los servicios, como una oportunidad para manejar y maniobrar en los ecosistemas digitales actuales.

El artículo desarrollado por el ingeniero Jeimy J. Cano M., se centrada en la conceptualización de la computación confidencial como nuevo paradigma de seguridad y control para la información “en uso”. Este hace una revisión básica de la temática, plantea algunas realidades (y una mentira) sobre la implementación de este nuevo paradigma y establece algunas conclusiones prácticas sobre sus retos e implicaciones tanto para las empresas como para los proveedores de servicios en la nube.

El foro de esta revista fue un espacio para compartir visiones desde diferentes ángulos la computación confidencial. Los ingenieros Diego Bueno de Oracle y Alonso Verdugo de Microsoft, desarrollaron un diálogo abierto y nutrido para contrastar y complementar sus posturas alrededor de los retos que implica la computación confidencial para las organizaciones modernas.

Ellos advierten sobre la necesidad de aumentar la visibilidad y conocimiento de esta nueva apuesta de transformación de la seguridad y control en la nube, el reto de establecer una seguridad extremo a extremo de las iniciativas digitales que actualmente despliegan las organizaciones y sobremanera, establecer planes de transición para concretar la promesa de valor de esta tecnología.

En resumen, se trata de un panorama renovado y provocador de nuevas transformaciones, retos y propuestas alrededor de la computación confidencial, que tensionan las certezas de los saberes y prácticas existentes de la seguridad en la nube y las realidades de las empresas en el tratamiento de sus datos con sus terceros de confianza. Su contenido invita a todos los profesionales, en las diferentes áreas del conocimiento, a explorar los nuevos retos y oportunidades en el uso y procesamiento de los datos y la información en un mundo digital y tecnológicamente modificado, sin perjuicio de las amenazas, fallas y vulnerabilidades propias de esta nueva propuesta de seguridad y control, donde tanto el negocio, la infraestructura, las aplicaciones y los datos plantean, revelan y reescriben nuevas incertidumbres y potencian el desarrollo de capacidades cibernéticas antes inexisten-

tes, de cara a los riesgos que permanecen ocultos en los retos de la transformación digital que avanza actualmente en las empresas.

Referencias

EY (2024). Desafíos y tendencias 2024 para las empresas de Latinoamérica. https://www.ey.com/es_co/insights/desafios-tendencias-2024-empresas-latinoamerica

Felk, Y. (2023). Confidential computing. En Mulder, V., Mermoud, A., Lenders, V. & Tellenbach, B. (editors). (2023). *Trends in Data Protection and Encryption Technologies*. Cham, Switzerland: Springer Nature Switzerland AG. 103-107.

Confidential Consulting Consortium – CCC (2021). Confidential Computing – The Next Frontier in Data Security. https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/Everest_Group_-_Confidential_Computing_-_The_Next_Frontier_in_Data_Security_-_2021-10-19.pdf

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*

***Andrés R. Almanza J., Ms.C, CISM**. Chief Growth Officer en CISOS.CLUB, Investigador en Ciberseguridad SegInfo y Liderazgo. | Executive Certificate in Cybersecurity Leadership & Strategy by FIU University | Certificado como ISO 27001 Lead Implementer and 27005 Lead Manager from PECB | CISM, ITILv3, LPI| Certificado como Coach Profesional Internacional, Master in Leadership and Organizational Development with Coaching, Executive Master's in Leadership Skills Developed in Harvard, & Coach Profesional avalado por International Coach Federation| Profesional en Ingeniería de Sistemas | especialista en seguridad en redes y máster en seguridad de la información. Docente del programa de maestría de la Universidad Externado de Colombia y de la Universidad de las Américas en Ecuador. Creador de la Comunidad CISOS.CLUB, CISOS-COL y CISOS-LATAM (Linkedin) y Miembro del comité editorial de la revista sistemas de ACIS.*