Computación confidencial

Cinco realidades (y una mentira) en el contexto organizacional.

DOI: 10.29236/sistemas.n171a6

Resumen
La transformación digital acelerada de las organizaciones demanda la incorporación de proveedores de servicios en la nube como apalancadores de las capacidades necesarias para concretar las iniciativas digitales claves para su promesa de valor. En este sentido, el tratamiento de la información en reposo (en los servidores), en tránsito (a través de las redes) y en uso (en el procesamiento de las aplicaciones) establecen retos particulares de seguridad y control que demandan una atención especial. La computación confidencial como nuevo paradigma de seguridad y control para la información en uso establece un nuevo referente para la seguridad en la nube donde ahora fluyen y se procesan los datos de los clientes como fundamento de los objetivos estratégicos de las compañías. Por tanto, este artículo hace una revisión básica de esta 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.

Palabras clave
Computación confidencial, riesgo cibernético, servicios en la nube, cifrado, entorno de ejecución confiable

Introducción

En la actualidad el tratamiento de la información tanto a nivel individual como organizacional representa no sólo un reto para las empresas, sino un mandato legal que implica fortalecer sus medidas tecnológicas, procedimentales y humanas para demostrar el compromiso y debido cuidado con este activo, sin perjuicio de los eventos adversos que tarde o temprano se van a materializar generando impactos negativos en la reputación de la compañía. En consecuencia, más allá de proteger la información frente a situaciones y riesgos conocidos, el ejercicio de defensa será el que marque la pauta para que tanto los ejecutivos corporativos como los profesionales de seguridad/ciberseguridad desarrollen una postura vigilante que se traduzca en hábitos automáticos que las personas apliquen en el desarrollo de sus actividades (Saydjari, 2018).

En este sentido, la información bien esté en reposo (guardado en servidores), en tránsito (transmitida por redes) o en uso (utilizado por aplicaciones y procesos) deberá contar con mecanismos de seguridad y control que permitan a los operadores adelantar su tratamiento de forma confiable y con la menor exposición, sin perjuicio de las acciones avanzadas o no previstas que un adversario pueda generar y concretar más allá de las medidas instaladas y disponibles para disuadir la acción de éstos últimos. En consecuencia, se requieren articular esfuerzos en estos tres momentos de la información para hacer más resistente a la organización a posibles brechas de datos (Kohnke et al., 2016).

A la fecha se cuentan con diferentes mecanismos de control para la información en reposo y en tránsito que se han venido utilizando con relativo éxito en las organizaciones. Temas como el cifrado de datos, el control de integridad, las soluciones de prevención de fugas de información, las listas de control de acceso y la implementación de esquemas administrativo de segregación de funciones se han configurado como la base fundamental de la custodia y aseguramiento de la información, que aún fuesen comprometidos, es posible contar con alguna evidencia o rastro que permita saber qué ocurrió con la información (Kohnke et al., 2016).

Sin perjuicio de lo anterior, la información en uso mantiene un margen de oportunidad donde es posible encontrar nuevas posibilidades para dejar un menor margen de acción para los atacantes. A la fecha los mecanismos de seguridad disponibles para la información en uso (aquella que se procesa o manipula activamente, reside en la memoria o en dispositivos) como son la autorización y autenticación de usuarios, gestión de permisos

de usuario y métodos seguros para compartir archivos, no consideran el entorno de ejecución de estas medidas lo que mantiene una ventana de exposición clave que puede ser aprovechada por los atacantes de forma silenciosa y posiblemente no detectable (ManageEngine, s.f).

Así las cosas, surge la computación confidencial (CC) como la nueva frontera de aseguramiento de la información en un entorno de procesamiento confiable, esto es, procesar datos en una zona protegida del procesador de un servidor, generalmente situado en la nube, manteniendo la confidencialidad de los datos cifrados en memoria hasta que la aplicación le indique al entorno de ejecución que los descifre para su procesamiento. Esta nueva realidad, poco conocida en la actualidad y disponible a través de muchos de los proveedores de servicios, representa una oportunidad para aterrizar las expectativas de las organizaciones respecto de su apuesta al hacer su transición a la computación en la nube (Mulligan et al., 2021).

Por tanto, este breve artículo presenta una revisión de esta propuesta de seguridad y control para la información en uso, ilustrando al menos cinco realidades a las cuales se van a enfrentar las organizaciones que se decidan por esta opción y una mentira, que pondrá a prueba los supuestos de los ejecutivos de seguridad y control, así como de los directivos respecto del tratamiento de la información ahora y en el futuro.

Evolución, fundamentos y riesgos de la computación confidencial

El *Confidential Computing Consortium* (CCC) define la computación confidencial (CC) como la protección de los datos en uso mediante la realización de procesamientos en un entorno de ejecución de confianza (EEC) (TEE – *Trusted Execution Environment* en inglés) basado en hardware y debidamente certificado (CCC, 2021). En este sentido, la CC más que un conjunto de arquitecturas que se basan en un ECC, es un nuevo paradigma de computación que cubre la seguridad en el hardware, la seguridad de los sistemas y la seguridad de los datos. Es una vista integrada de la protección de los datos en uso que tiene como objetivo que las aplicaciones se ejecuten con una mayor seguridad en un ECC.

Si bien el concepto no es nuevo, ha venido evolucionando desde finales de los 90s y durante la primera década del segundo milenio cuando se introduce la computación de confianza (*Trusted Computing*), y las funciones de seguridad se aíslan en coprocesadores criptográficos o chips de seguridad como TPM/TCM (*Trusted Platform Module* /*Trusted Cryptography Module*), el reto para ese momento era asegurar un procesamiento interno seguro que disuadiera a los adver-

sarios de llegar a funciones críticas del procesador, a pesar de contar con una ejecución de aplicaciones en plataformas posiblemente no confiables (Feng et al., 2024).

A mediados de la segunda década del nuevo milenio, se advierte la evolución de uno de los componentes centrales de la computación confidencial como lo es el ECC, para lo cual Intel introduce la tecnología hardware *Software Guard Extensions* (SGX), que podía construir "enclaves" seguros en espacios de procesos de usuario, esto es, segmentos aislados de ejecución dentro del entorno propio de un servidor. El código y los datos dentro de los enclaves eran inmunes a los ataques de software, y el cifrado de memoria podía evitar ciertos ataques físicos (Feng et al., 2024).

Finalizando el 2019 se consolida el concepto de computación confidencial, se acepta formalmente y comienza su expansión comercial. Se crea el CCC que vincula a proveedores de hardware como Intel, Arm y AMD, así como proveedores de servicios en la nube como Microsoft, Google, Huawei, Alibaba, Baidu y ByteDance, que toman el concepto de ECC tanto para software como para el hardware como paradigma fundamental para desarrollar una arquitectura de computación confiable que termine en entornos virtualizados seguros y resistentes a los ataques (Feng et al., 2024).

El objetivo de la computación confidencial es cifrar los datos en uso en la memoria principal del sistema sin comprometer el rendimiento. La protección de los datos en memoria presenta dos aspectos: (Felk, 2023)

- Cifrar toda la memoria del sistema.
- 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, firmware o hardware que crea y ejecuta máquinas virtuales).

En este contexto, la computación confidencial busca asegurar: (Sardar & Fetzer, 2023).

- Confidencialidad de los datos: Las entidades no autorizadas no pueden ver los datos mientras se utilizan en el ECC.
- Integridad de los datos: Las entidades no autorizadas no pueden añadir, eliminar o alterar datos mientras estén en uso dentro del ECC.
- Integridad del código: Las entidades no autorizadas no pueden añadir, eliminar o alterar el código que se ejecuta en el ECC.

Considerando diferentes aproximaciones de una arquitectura de confianza tecnológica colaborativa y las distintas hojas de ruta relacio-

nadas con el desarrollo de la computación confidencial, se detalla a continuación una vista básica de los componentes para la configuración de este nuevo paradigma de computación: (Feng et al., 2024)

- *Capa de hardware-firmware*, que proporciona la base de seguridad de hardware para toda la plataforma computación confidencial, proporcionando las primitivas de seguridad de hardware necesarias y el arranque de seguridad inicial del entorno.

- *Capa de software del sistema*, que gestiona la seguridad de los recursos de hardware de la plataforma de computación confidencial, así como el aislamiento y la transferencia segura entre los componentes de software.

- *Mecanismo de seguridad y capa de servicio*, que presenta un conjunto de mecanismos de seguridad y servicios de confianza para aplicaciones de computación confidencial, y ofrece una abstracción universal de la plataforma de computación confidencial para aplicaciones de alto nivel.

- *Capa de interfaz y aplicación*, que proporciona interfaces de programación unificadas y SDK (*Software Development Kit* – Paquetes de desarrollo de software) para el desarrollo de aplicaciones de computación confidencial.

Si bien este nuevo paradigma busca alcanzar un nuevo nivel de protección y aseguramiento para los datos en uso en tiempo de ejecución, no está exento de retos y riesgos de seguridad situados en el ECC. Un resumen de los riesgos a considerar en este nuevo entorno son: (Feng, 2024).

- Los ataques al sistema y al software incluyen principalmente ataques al kernel del sistema operativo y ataques a las llamadas al sistema. Los ataques al kernel incluyen principalmente ataques de escalada de privilegios y rootkits a nivel del kernel.

- Los ataques de canal lateral se deben principalmente a la gran cantidad de recursos del sistema compartidos entre el entorno normal y el ECC: memoria cache.

- El ataque de ejecución transitoria es un método de ataque que utiliza mecanismos de ejecución especulativa y de ejecución fuera de orden en las arquitecturas de CPU modernas para obtener información sensible:

  - Mecanismos de anticipación de bifurcaciones.
  - Mecanismos de ejecución fuera del orden.
  - Muestreo de datos de microarquitectura, que permite a los adversarios recopilar datos de recursos compartidos de microarquitectura de CPU, como cachés

de datos, búferes de almacenamiento, etc., filtrando así información confidencial a través de dominios de seguridad.

- Los ataques de inyección de fallos exponen información secreta al provocar fallos físicos o basados en software en los cálculos.

Cinco realidades (y una mentira) de la computación confidencial en una organización

Realidad 1. Se puede (y se debe) arreglar las cosas antes de que un incidente en la nube ocurra.

Prepararse de forma preventiva -antes de que se configure una brecha de seguridad- significa transformarse desde una posición pasiva, basada en riesgos conocidos a una de posición proactiva, que trabaja con los proveedores de servicios en la nube para configurar y desplegar un entorno de computación confiable ajustado a sus necesidades de seguridad y control. Los ejecutivos y los profesionales de ciberseguridad están facultados para centrarse en identificar nuevas iniciativas digitales que acompañen la promesa de valor, en lugar de sólo concentrarse en asegurar la protección de la información y asegurar el cumplimiento normativo (Cano, 2023).

Realidad 2. El liderazgo en ciberseguridad empresarial hará la diferencia en la implementación.

Las implementaciones exitosas de la computación confidencial no sólo serán impulsadas por la visión prospectiva del panorama de amenazas de la empresa, sino también, por cuestionar y retar el modelo de gestión del riesgo cibernético actual basado en certezas, y cambiar los modelos mentales y las estructuras organizacionales que subyacen tanto en los profesionales de las áreas de negocio, como en los ejecutivos de la compañía. La voluntad y el compromiso con la implementación del nuevo modelo a nivel directivo será un factor fundamental, sobre todo en un momento en el que la participación de las áreas de negocio en el proceso esté disminuyendo.

Realidad 3. No puede tomar atajos en el camino hacia un nuevo nivel de seguridad y control.

Es determinante que las empresas elaboren un plan de transformación y una narrativa convincentes de implementación de la computación en la nube al comienzo de este viaje, con una agenda de comunicación clara para sus diferentes grupos de interés (Reeves et al., 2024). En este sentido, tanto los ejecutivos como las áreas de negocio deberán asegurar victorias tempranas basada en historias de éxito con sus clientes, de tal forma que se fortalezca la confianza digital en las iniciativas digitales que se despliegen en la nube. De esta forma, en un ejercicio de colaboración, cooperación, coordinación y confianza

tanto los proveedores de servicios en la nube, la organización y los clientes, encuentren en esta nueva apuesta de seguridad y control las mejores razones para hacer la diferencia y hacerse más resistente a los ataques.

Realidad 4. La implementación es un ejercicio de transformación a largo plazo.

Lograr una implementación de la computación confidencial sostenible y un modelo operativo preparado para el futuro exige abordar las transformaciones a nivel de la cultura organizacional de seguridad de la información con una orientación a largo plazo, donde la información se transforme de ser un recurso más de la empresa y pase a ser un activo estratégico para la organización, y no centrarse simplemente en resolver los problemas de control de acceso tradicionales o procurar el aseguramiento de las buenas prácticas de seguridad y control vigentes. El reto es encontrar el equilibrio adecuado entre la creación de experiencias distintas para los clientes y el apetito de riesgo cibernético de la corporación.

Realidad 5. No se pueden inventar cosas sobre el desarrollo de la implementación.

Las implementaciones y despliegues de la computación confidencial requieren planeación y aseguramiento en al menos dos vías: de la empresa hacia los clientes y del proveedor de servicios en la nube hacia la empresa. Lo anterior exige la consecución simultánea de varios objetivos claves, tanto para el cliente como para la empresa, normalmente bajo una inmensa presión externa e interna. Por ello, las empresas no pueden inventar o incorporar elementos distintos de la planeación de estos proyectos sobre la marcha, so pena de comprometer la promesa de valor articulada en los proveedores y materializada en la experiencia del cliente.

Esto implica una gobernanza y un proceso claro para coordinar y asegurar los avances, comunicando y probando los resultados conforme se implementa los componentes de la computación confidencial.

Una mentira: la computación confidencial es especial y no se aplica a todas las empresas.

Cuando se trata de computación confidencial, nadie es especial. Las organizaciones que se deciden a transformar su modelo de seguridad y control en la nube, no tienen motivos para confiarse dada la evolución y sofisticación de los ataques cibernéticos. En este sentido, más que motivar un paradigma de protección se movilizan a uno de defensa que permite tanto a la organización como al proveedor de servicios en la nube configurar un entorno de computación más confiable y resiliente, que permite aumentar la eficiencia de las operaciones, la resistencia a los eventos adver-

sos y el aseguramiento de la cadena de suministro digital que cubra la información en reposo, en tránsito y en uso.

Conclusiones

La seguridad de la información ha avanzado a lo largo del tiempo en la protección de los datos en tránsito y en reposo. Sin embargo, asegurar la protección de los datos en uso sigue siendo un reto en múltiples dimensiones para los propietarios de los datos, la seguridad de los sistemas para los operadores de plataformas y la seguridad de los algoritmos para los procesadores de datos. En este sentido, la computación confidencial aparece como un nuevo paradigma de seguridad y control que enfrenta estos retos mediante el aislamiento de los sistemas a nivel de hardware y la protección colaborativa que implica tanto al hardware como al software.

No obstante lo anterior, al ser no sólo un reto de implementación de tecnología de información, es una apuesta de transformación de la cultura de la seguridad de la información y la apertura de un nuevo panorama de riesgos emergentes con los proveedores de servicios en la nube. Por tanto, implica entender ahora en detalle y profundidad cómo la organización se sitúa en una cadena de suministro digital, donde los diferentes participantes de un ecosistema digital buscan de forma conjunta hacerse más resistentes a los ataques y concretar mejores mecanismos de resiliencia cibernética frente a la inevitabilidad de la falla.

Ahora la gestión del riesgo cibernético orientada por tres elementos básicos: reducir las amenazas, reducir los impactos de un ataque exitoso y disminuir las vulnerabilidades inherentes propias de la organización, se convierte en un mandato base para acompañar el apetito de riesgo cibernético de las empresas, habida cuenta de las iniciativas digitales que las organizaciones comienzan a desplegar de forma acelerada para ganar nuevos posicionamientos en sus diferentes sectores de negocio. Esto implica, reconocer la información y los datos como activos estratégicos que la organización configura y custodia con el consentimiento de sus clientes para lograr las transformaciones que son necesarias en los diferentes grupos de interés.

La computación confidencial se configura como ese nuevo paradigma de la protección de la información en uso que busca disuadir los planes de los atacantes concentrados en los activos estratégicos de información, no para cambiar sus intenciones, sino para aumentar la incertidumbre en su modelo de riesgos dadas la condiciones y características de seguridad y control que este paradigma sugiere, ahora con aseguramiento del hardware y del software de forma conjunta a través de algoritmos de cifrado que hacen opaco el proce-

samiento de las aplicaciones en entornos de ejecución confiables.

El paradigma de la computación confidencial no busca crear seguridad por oscuridad, sino incorporar una nueva capa de protección y confianza para el procesamiento de las aplicaciones y el uso de los datos sensibles, de forma que a pesar de contar con un entorno hostil y agreste de operaciones cibernéticas adversas, las organizaciones se puedan concentrar en desarrollar propuestas digitales novedosas sabiendo que ahora la información en reposo, en tránsito y en uso adquiere un nivel de confiabilidad mayor: incorporar las prácticas y estándares previos para asegurar los controles de acceso tradicionales con una experiencia más confiable al procesar y tratar los datos de sus diferentes grupos de interés con los proveedores de servicios en la nube.

Referencias

Cano, J. (2023). Cyber risk assessment A conceptual framework for executives. *Proceedings 2023 18th Iberian Conference on Information Systems and Technologies (CISTI)*, Aveiro, Portugal. 1-7. doi: 10.23919/CISTI58278.2023.10211418

Confidential Computing consortium (CCC) (2021). Confidential Computing consortium: a technical analysis of confidential computing v1.2. https://confdentialcomputing.io/wp-content/uploads/sites/85/2022/11/CCC-A-Technical-Analysis-of-Confdential-Computing v1.2_updated_2022-11-02.pdf

Felk, Y. (2023). Confidential computing. En Mulder et al. (eds.) (2023) *Trends in Data Protection and Encryption Technologies*. Cham, Switzerland: Springer Nature Switzerland AG. 103-107. https://doi.org/10.1007/978-3-031-33386-6_19

Feng, D., Qin, Y., Feng, W., Shang, K. & Ma, H. (2024). Survey of research on confidential computing. *IET Communications*. 1-22. https://doi.org/10.1049/cmu2.12759

Kohnke, A., Shoemaker, D. & Sigles, K. (2016). *The complete guide to cybersecurity risk and controls*. Bocaraton, Florida. USA: CRC Press

ManageEngine (s.f.). Data in use. https://www.manageengine.com/data-security/what-is/data-in-use.html

Mulligan, D. P., Petri, G., Spinale, N., Stockwell, G. & Vincent, H. J. M. (2021). Confidential Computing—a brave new world. *2021 International Symposium on Secure and Private Execution Environment Design (SEED)*. 132-138, doi: 10.1109/SEED51797.2021.00025.

Reeves, M., Gruß, C., Ellmer, K., Job, A., Bouslov, G. & Catchlove, P. (2024). Five Truths (and One Lie) About Corporate Transformation. *BCG Research*. https://www.bcg.com/publications/2024/five-truths-and-a-lie-about-corporate-transformation

Sardar, M. U. & Fetzer, C. (2023). Confdential computing and related technologies: a critical review. *Cybersecurity*. *6*(10). 1-7. https://doi.org/10.1186/s42400-023-00144-1

Saydjari, O. (2018). *Engineering trustworthy systems: get cybersecurity design right the first time*. New York, USA.: McGraw Hill.

Jeimy J. Cano M., Ph.D, CFE, CICA. *Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, 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–.*