Computación confidencial: Eficiencia de la seguridad en la nube

DOI: 10.29236/sistemas.n171a5

La nube vs OnPremise.

A medida en que los líderes de la empresa confían más en el público y los servicios de nube híbrida, la privacidad de los datos en la nube es imperativa. El objetivo principal de la informática confidencial es brindar una mayor garantía a los líderes de que sus datos en la nube están protegidos y son confidenciales, también se trata de alentarlos a mover más de sus datos confidenciales y cargas de trabajo de computación a servicios de nube. Esto implica que la protección de los datos se da durante el procesamiento.

El control exclusivo de las claves de cifrado ofrece una mayor seguridad de los datos de un extremo a otro en la nube. El contenido del enclave (los datos que se procesan y las técnicas que se utilizan para procesarlos) son accesibles solo para el código de programación autorizado y son invisibles e incognosci-

bles para cualquier otra persona, incluido el proveedor de la nube.

Para tratar tales asuntos fueron invitados Diego Bueno, director del equipo de Ingeniería Cloud en Oracle, para la región denominada multicountry que comprende Ecuador, Colombia, Centroamérica y el Caribe, sin México. Y Alonso Verdugo Medina, chip medical officer de la vertical de salud para Latinoamérica en Microsoft.

En este sentido la idea es conversar sobre los retos, oportunidades y desafíos que esta tendencia de un futuro cercano puede ofrecerles a los servicios de negocios, en un ambiente con una densidad digital más compleja, unos datos que cada vez son más un impulsor del negocio, y un adversario cada vez más sofisticado, señalaron Jeimy J. Cano M. y Andrés R. Almanza J., moderadores del encuentro, quienes formularon la primera pregunta a los invitados:

¿Por qué la computación confidencial es el nuevo paradigma de seguridad y control para las empresas en la nube? ¿Cómo moverse a este nuevo escenario?

Diego Bueno
Ingeniería Cloud
Oracle
Uno de los mayores temores que normalmente representa no sólo para las empresas, sino para cualquier persona es tener la certeza sobre la seguridad de los datos en el momento de moverse hacia una computación en la nube y de ahí surge el concepto de computación confidencial, para que exista una seguridad de los datos en tránsito, servicio ofrecido por los proveedores de nube.

Hablando de una herramienta analítica en términos de seguridad, entra en juego la computación confidencial, muchos proveedores hoy en día lo ofrecen y AWS, Microsoft, GCP, e IBM, Oracle también ya lo tiene porque es una necesidad imperiosa para las empresas, sí, de qué manera señor proveedor de nube usted me garantiza a mí que durante el procesamiento de los datos esto realmente sí va a estar seguro y ni siquiera usted que me los está alojando, va a tener acceso a esa información, entonces entra el concepto de paradigma de seguridad en el sentido de tengo que confiar que ya no solamente el momento en que yo muevo mi data desde un punto origen hacia la nube, van a estar encriptados, sino que también cuando ya estén allá y los empiece a procesar, me ofrecen una capa adicional de seguridad y ahí viene todo el tema de contratos y bueno de más acuerdos que tienen los diferentes proveedores de nube con base también en regulaciones internacionales donde yo tengo que garantizarle al cliente que sus datos van a estar resguardados.

En tal sentido, podemos hablar de tres beneficios clave que me ofrece

la tecnología en la computación confidencial y es la seguridad mejorada de los datos. Otro aspecto es el relacionado con los estándares internacionales como el GDPR de la Unión Europea, uno de los más estrictos del mundo y por último el HIPAA sobre manejo de datos de salud.

Alonso Verdugo Medina
Chip Medical Officer
Microsoft Latinoamérica

Parte del negocio está en analizar el tráfico de la navegación web de los usuarios para entender sus patrones de comportamiento y hacer ofertas, proceso en el que entran en juego algunos aspectos de ética y de moral. En la actualidad no sólo se trata de saber cómo lo almacenamos o cómo lo transportamos de forma segura. Redondeo dos aspectos clave, la privacidad y la confidencialidad. Datos que sean confidenciales y no quiero que queden expuestos y luego los datos sensibles relacionados con la identificación de la persona, sus gustos y condiciones. En los últimos años la relevancia ha ido hacia el uso de datos que no puede ser empleado para segregar. Cuando aparecen los proveedores de nube nativos, o sea un Google o Amazon en donde el tráfico y la información personal es utilizada. Parte del negocio es conocer su tráfico para entender los patrones de comportamiento y hacer ofertas y luego pasarlo a un tercero. Ahí aparecen aspectos de ética y moral que son relevantes. Nosotros los humanos no usamos datos, usamos información, los algoritmos y mecanismos de inteligencia artificial.

Jeimy J. Cano M.
¿Por qué no se conoce tanto este nuevo paradigma en las empresas de Colombia? ¿Es un tema de difusión? ¿Es un tema de demanda? ¿Es un tema de costo?

Alonso Verdugo M.
Chip Medical Officer
Microsoft Latinoamérica
La falta de conocimiento es uno de los principales factores. Los ingenieros y responsables de tecnología en las empresas deben mantenerse actualizados no solo en las nuevas tendencias tecnológicas, sino también en las regulaciones pertinentes. Sin embargo, esto no siempre sucede.

Un ejemplo claro fue la adopción de la tecnología de Message Queues

o colas de mensajes, que facilita la integración de aplicaciones (MQ).

En mi experiencia, el primer gran cliente en adoptar esta tecnología fue el Banco Santander. Cuando la Superintendencia reconoció su potencial, esto incentivó su implementación, generando una ola de adopción en Colombia. Este caso ilustra cómo la difusión y la adopción de nuevas tecnologías pueden depender de la validación y el impulso inicial de entidades reconocidas.

Además, el entrenamiento y la capacitación son fundamentales. En Microsoft, he descubierto que existen muchas capacidades avanzadas, como la computación confiable. Sin embargo, un cliente que ya usa Azure debe no solo habilitar estas capacidades, sino también integrar estos procesos dentro de su organización. No se trata solo de activar una función, sino de gestionar la seguridad y ciberseguridad adecuadamente.

Otro aspecto crucial es la gestión de la información. Por ejemplo, muchas empresas desconocen que pueden utilizar las herramientas de etiquetado de información confidencial en Word o Excel para mejorar su seguridad. Microsoft ofrece alertas cuando se envía información sensible fuera de la compañía, pero estos controles requieren un nivel de conciencia y entrenamiento que impide la correcta implementación.

En última instancia, las barreras son las personas. La adopción de tecnologías como la inteligencia artificial mediante los asistentes como Copilot, en herramientas de desarrollo, (GitHub Copilot) depende no solo de la disponibilidad de la tecnología, sino también de un cambio cultural dentro de las organizaciones. Es crucial capacitarse y entender dónde y cómo estas tecnologías pueden ser aplicadas para aprovechar todo su potencial.

Estas son, en mi experiencia, las principales razones por las que el nuevo paradigma no es ampliamente conocido en las empresas de Colombia. Es un desafío de difusión, demanda, costo y, sobre todo, de educación y cultura organizacional.

Diego Bueno
Ingeniería Cloud
Oracle

Yo agregaría dos aspectos importantes a lo que mencionaba Alonso, uno es el tema de la difusión, lo cual definitivamente juega un papel significativo, no solo en lo relacionado con la computación confidencial, sino en diferentes tecnologías, puesto que lastimosamente eso va pegado al segundo factor y es la demanda de tecnologías avanzadas de seguridad. Recordemos que el año pasado aquí en Colombia hubo una situación fuerte en entidades gubernamentales que fue una noticia, en temas de seguridad. Eso fue un boom, fue terrible, ya que varias entidades se vieron afectadas,

entre esas el Ministerio de Defensa tuvo una afectación importante, entre otras entidades. Después de eso, fue que a nivel presidencial se sancionó una ley para temas de ciberseguridad y que cada entidad debía tener un protocolo y un plan asociado a eso, entonces como bien lo mencionaba hace un momento, se trabaja de manera muy reactiva, se trabaja en temas de seguridad en muchos campos no solo a nivel gubernamental, sino en diferentes empresas, entonces el hecho de que no se hace una difusión constante de nuevas tecnologías y como bien lo mencionó el Doctor Cano hace un momento, también hay muchas personas que no conocen sobre computación confidencial, aún cuando trabajan en el campo de la tecnología. Entonces sí, es muy común, que haya desconocimiento, pero vuelvo al punto anterior, también va muy asociado a la demanda, hasta que no se presenta una eventualidad no se toman las medidas y a consultar qué existe, para qué existe, más allá de un firewall o de un antivirus, sino que existen otros métodos de encriptación adicionales que me van a brindar esas capas de seguridad, entonces es totalmente un tema de difusión y de desconocimiento, a tal punto que hay empresas que ni siquiera saben que existen ya regulaciones en Colombia para el tema de manejo de datos en la nube que existe algo como la circular 005 emitida por el gobierno; que existe la Ley de Protección de Datos 1581 que el gobierno la sacó con base en el estándar GDPR, precisamente que mencionaba yo hace un momento es el estándar internacional más estricto en manejo de datos y que eso ya da unos puntos de partida para yo decir este tipo de datos yo si los puedo tener en la nube, o estos otros definitivamente no, pero eso todavía sigue siendo un mundo desconocido para muchas empresas, entonces eso hace que como bien lo mencionó el Doctor Cano, la computación confidencial es algo que se debe promover, es algo que yo como proveedor entrego, es algo que tengo que contarle al cliente o en general a la industria de tecnología, o en las universidades.

Jeimy J. Cano M.

¿Cómo plantear una transición de los esquemas tradicionales de seguridad y control en la nube a uno basado en computación confidencial? ¿Cuáles serían los pasos y qué cosas se deben tener en cuenta?

Diego Bueno

Comienzo mi respuesta haciendo un breve resumen sobre seis circulares importantes que existen en Colombia con base en el manejo de los datos, una es la circular 007 de 2018 que habla específicamente de los requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad luego en el 2019 sale la circular 005 que ya habla de reglas para el uso de servicios de computación en la nube, ahí fue cuando Colombia hizo como los primeros acercamientos a decir una realidad vamos a ponerlo en la ley y sale esta circular. Luego en el 2020, la circular 008 donde ya hubo una instrucción para el fortalecimiento de la Gestión de Riesgo Operacional de esos datos de lo que pasa a nivel financiero, si se llega a vulnerar de alguna manera los datos. Posteriormente en el 2020 también sale otra circular que fue la 033, en donde nuevamente y digamos que reforzando la 007 requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad, realmente esta 033 fue como una actualización. Por último, en el 2022, que es la más reciente, hace dos años, es emitida la circular 01 para recomendaciones de uso de servicios de la nube, cómo mitigar riesgos de seguridad digital, pero estas circulares, si usted va y se las menciona a muchas personas en empresas, no saben que esto existe y dice, no, no es que en Colombia todavía no hay un marco normativo para eso. Entonces, si hay unos primeros pasos y estas son seis seculares importantes que muchas empresas deberían conocer.

Ahora, respondiendo la pregunta con base en lo anterior, yo lo englobaría en seis pasos sencillos, uno, evaluación y planificación de lo que quiero hacer a nivel de computación confidencial, cuál es mi postura actual de seguridad, es decir, cómo estoy hoy en día y cuál es el caso de uso al que necesito llegar. Dos, compromiso y capacitación de las partes interesadas, entonces cuál es la postura que voy a tener a nivel de compañía para lo que quiero hacer, puesto que muchas veces esto es lo que hace fracasar los proyectos, lo que normalmente se llama el *Change Management*; yo puedo tener un proyecto súper exitoso, pero nadie me lo compró al interior, de tal manera que no se podrá ejecutar, por lo tanto, de qué manera realmente va a

haber una postura de seguridad en todas las áreas o al menos desde el director general hacia abajo y que sea un mensaje en cascada para que eso sea una realidad en la organización. Tres, selección de la tecnología requerida, puesto que las empresas deben optar por proveedores de nube que ofrezcan servicios robustos de computación confidencial y herramientas adicionales de seguridad, llámese cómo se llame dicho proveedor. Cuarto, implementación de un proyecto piloto, ya que este tipo de tecnologías siempre es recomendable probarlas, testear que si funciona más allá de la teoría y que hace lo que yo como cliente final requiero y en tecnología pasa mucho y son los *quick wins* o las victorias tempranas, a través de pruebas que me permitan a mí realmente demostrar que eso sí funciona que eso que yo quiero hacer sirve y que se aplica mi negocio a través de una prueba de concepto o una prueba piloto, pero que yo vea esta seguridad funcionando realmente con lo que necesito hacer. Quinto, integración y migración, ya que una vez seleccionado el proveedor, el siguiente paso es integrar la computación confidencial en los flujos de trabajo existentes, así como en mi ecosistema de aplicaciones, ya que esto a menudo implica reestructurar algunas de ellas, para aprovechar los enclaves seguros que me ofrece el proveedor. Por último, sexto, alineación de políticas de cumplimiento, cuál o cuáles van a ser esas políticas o procedimientos que yo como empresa voy a adoptar con base en la computación confidencial, que requiero de acuerdo con la industria o al propósito del negocio de mi compañía. En resumen, yo lo englobaría en esos seis pasos.

Jeimy J. Cano M.

¿Dónde no están conectados, dónde sí están conectados, dónde hay turnos va a haber una serie de cosas mixtas e híbridas cuando eso ocurre, entonces eso también va a ser un desafío de seguridad para la empresa como tal, ¿no?

Alonso Verdugo M.

Nosotros en Microsoft tenemos un marco de trabajo para la adopción de nuevas tecnologías disruptivas. (Innovación en la economía digital - Cloud Adoption Framework | Microsoft Learn). Mi experiencia me ha permitido observar que los centros de excelencia son un factor clave para adoptar rápidamente este tipo de tecnologías. (Información general sobre el Centro de excelencia (CoE) - Power Platform | Microsoft Learn).

Los centros de excelencia no son un concepto nuevo, han existido durante mucho tiempo. Son elementos indispensables para que las empresas adopten nuevas tecnologías, ya sea computación confiable u otras innovaciones. La evolución tecnológica actual es extremadamente rápida y disruptiva, por lo que estos centros deben incluir

tanto a personas del área de negocio como del área de tecnología, trabajando juntos en torno a la cadena de valor para aplicar las nuevas propuestas tecnológicas.

Dentro de estos equipos, lo primero es una evaluación inicial que incluye cuatro o cinco puntos clave. Se debe analizar los datos y procesos críticos que requieren seguridad. No todo necesariamente requiere el mismo nivel de seguridad, por lo que es crucial priorizar según la regulación y otros factores. Por ejemplo, la protección del capital intelectual de la empresa es fundamental, especialmente en industrias como la farmacéutica, donde se maneja información muy sensible.

Los ciberataques, actualmente, son una amenaza constante. Por ejemplo, hemos visto ataques a gran escala en Ucrania que Microsoft ha documentado, destacando la necesidad de proteger la información en entornos confiables, especialmente en sectores sensibles como energía, agua, transporte público y servicios esenciales.

La evaluación inicial permite identificar necesidades, analizar riesgos y priorizarlos. A partir de ahí, se define una estrategia, se desarrollan objetivos, y se crea un plan de proyecto. Es fundamental capacitar y concientizar al personal, ya que los humanos suelen ser el factor limitante en la seguridad. Luego se realiza una prueba de concepto o un MVP, seleccionando un área piloto para probar la tecnología, evaluar su impacto y ajustar según sea necesario.

El centro de excelencia juega un papel crucial en la implementación, escalado, integración, monitoreo y optimización de la nueva tecnología. Siguiendo principios similares a ITIL, se gestiona la operación y el mantenimiento, incluyendo acuerdos de servicio, manejo de requerimientos y actualizaciones.

En Microsoft, facilitamos cursos sobre computación confiable y otros temas, proporcionando ejemplos prácticos y procesos de certificación para ayudar a las empresas en la adopción y capacitación. (Introducción a la computación confidencial de Azure | Microsoft Learn).

En Latinoamérica hemos visto casos donde la banca ha liderado en la adopción de estas tecnologías, protegiendo información sensible y controlando intentos de acceso no autorizado. Por ejemplo, en Europa, una aseguradora ha implementado un esquema de salud con información gestionada de manera segura, cumpliendo con diversas regulaciones nacionales y permitiendo una gestión eficaz de pacientes con enfermedades crónicas.

Estos ejemplos demuestran que la seguridad de la información es crítica y que la adopción de nuevas tecnologías requiere un enfoque

integral, desde la gestión de datos en la nube hasta el uso seguro de dispositivos personales.

Jeimy J. Cano M.
Diego, puede contarnos algún caso también en algún sector de América Latina.

Diego Bueno
Ingeniería Cloud
Oracle
Mencionaré cuatro casos de éxito, independientemente del proveedor, sobre computación confidencial; en el caso de Colombia, tenemos al Banco de Bogotá, esta compañía aplicó computación confidencial para mejorar la seguridad y entre los datos personales de sus clientes sí que volvió exitoso este proyecto, ya que le ofrecen a sus clientes una capa adicional que permite reducir temas de riesgos de fraude y ciberataques, eso va a repercutir necesariamente en la confianza del cliente y que este diga, o sea, yo como banco, publico datos y digo este año le apostamos a que la tasa de fraude baje o que baje el número de ciberataques, o no tuve ninguno de ellos. Bueno, pues es un banco bastante seguro, creo que vale la pena meter mi información allá, ¿No? Y pues esto muy alineado, con el cumplimiento normativo, por ende, podemos decir esos tres aspectos volvieron exitoso ese proyecto en Banco de Bogotá. En Argentina hay otro caso y muy de la mano con lo que mencionaba Alonso previamente, el Hospital Alemán también hizo una adopción de soluciones de computación y confidencial y es el hecho de ellos poder hacer análisis de los datos médicos sin riesgo de la privacidad de los pacientes, puesto que yo no estoy buscando si Diego está enfermo, si Alonso está enfermo, lo que quiero ver son patologías, patrones, de qué manera yo identifico que está enfermedad tuvo cierta evolución o cierto comportamiento en el tiempo, independientemente del paciente que la tuvo; entonces, qué hace exitoso este tipo de proyectos, la privacidad de los pacientes que me permite a mí hacer una investigación colaborativa con demás médicos probablemente de otras instituciones independientemente del paciente que tiene la enfermedad y eso necesariamente me permite a mí como hospital generar un avance en salud. En Brasil también en temas de Turismo existe un caso, de una empresa que se llama *cereza experience*, que digamos ellos son turismo y crédito, quiénes también para el procesamiento de sus datos, aplicaron computación confidencial. Otros dos casos a mencionar son banco de Crédito del Perú y Banco de Chile Banco, este último básicamente es el banco más grande de ese país, en donde nuevamente muy similar al caso de Banco de Bogotá, usaron esta tecnología para detección de fraudes, transparencia y confianza hacia sus usuarios y nuevamente el tema normativo que yo como empresa prestadora de servicios financieros pueda garantizarle a mis clientes,

que estoy cumpliendo con las leyes de mi país en el caso de Brasil se llama la LGPD que es la Ley General de Protección de Datos y demás estándares que yo tenga en cada país. Por tanto, yo puedo englobar tres factores claves para decir cómo puedo medir que la computación confidencial sea exitosa, uno, cumplimiento normativo; dos, un tema de mejora o aumento de la confianza de mi cliente; y tres, a través de esa innovación tecnológica que hago con la computación confidencial, cómo creo algo más colaborativo, como en el caso de la salud, por ejemplo, sin ver afectada la identidad de mis pacientes, sin importar su enfermedad.

Jeimy J. Cano M.
Interesantes los casos que se tienen en varias industrias, donde muchas personas pueden estar de alguna manera experimentando los efectos positivos de esta nueva tecnología instalada, sin percatarse que están en un ambiente de computación confiable (*Trusted Computing Environment*), con un mayor nivel de aseguramiento y confianza en el procesamiento de sus datos particularmente en la nube.

Jeimy J. Cano M.
¿Cuál es el futuro de la computación confidencial? ¿Qué pueden esperar las empresas en el mediano plazo (3-5 años)?

Diego Bueno
En mi opinión, es algo que promete mejorar significativamente, puesto que los temas de privacidad y seguridad de los datos siguen preocupando en diversas industrias, sobre todo ahora por el boom que hay de la inteligencia artificial, sí, y ahí vienen dos grandes preocupaciones y son, ¿Qué tanta información puede acceder la inteligencia artificial? ¿Qué cantidad de motores de búsqueda por debajo son los que están realmente trabajando y voy a decirlo así, perdón, el término machacando los datos cierto, pero a qué nivel van a llegar y qué tan vulnerable puede estar la información en ese proceso? Aquí el problema es que existe una línea muy delgada para entrar en temas éticos, que es otro de los dilemas en temas de Inteligencia Artificial, dicho lo anterior, básicamente el futuro de la de la computación confidencial puede estar asociado a qué tan acelerada va a ser la adopción y la estandarización de esto en varias industrias, eso va a ser algo determinante para establecer si va a ser una tecnología que va a durar en el tiempo y que a su vez se vuelva más accesible, que se difunda de manera más masiva, con mejores soluciones a nivel de *hardware* y *software*, que proveedores como como Intel y AMD, ofrezcan mejores soluciones, no solo a nivel de máquinas virtuales sino a nivel de desarrollo también, que los SDKs tenga incorporada esta tecnología de manera embebida, ya que los software también son algo que en el día a día se usan tremendamente en todas las industrias y muchas cosas se hacen a través de APIs y cada vez

existen más APIs en diferentes lenguajes, pero yo tengo que también pensar en que tan vulnerable va a estar mi información y simplemente no consumir un servicio, sino de qué manera no va a ser vulnerada dicha data; qué sectores realmente lo van a aprovechar, ya hablamos aquí del sector salud, asimismo es clave para el sector financiero, pero muy seguramente las agencias gubernamentales también se van a montar en ese bus, porque todos los usuarios de un país, usamos muchas entidades gubernamentales, pero muchas veces no sabemos qué está pasando y vuelvo al comentario que hice hace un rato, qué pasa cuando existen esos ataques de seguridad y las primeras que caen son las agencias gubernamentales, uno como usuario piensa, ¿Cuál es la confianza que tengo en el gobierno? Es decir, qué estamos haciendo con los datos, definitivamente el tema regulatorio es algo clave que tiene que ir de la mano con la computación confidencial, lo cual me obliga a mí como proveedor y como usuario, a que entre más estándares haya y entre más la normativa cambie conforme la tecnología avanza, así mismo me debo adaptar a esto. Cierro con el tema de la inteligencia artificial, puesto que esto sigue avanzando muy rápido, pero las primeras conversaciones sobre la confidencialidad y el alcance de esto, se están teniendo en Europa, sobre qué tanto alcance vamos a permitirle a la inteligencia artificial para que esto no se descontrole, entonces, a medida que la computación confidencial tome mucha más fuerza y se vuelva un *MUST*, se va a masificar y evolucionar más rápido en el tiempo.

Jeimy J. Cano M.

Ahora bien, el tema de costos para desplegar las características de la computación confidencial. ¿Son características que se activan de productos ya existentes o se deben instalar nuevos productos? ¿Cómo sería la visión del tema?

Diego Bueno

Yo lo veo desde los puntos de vista uno como lo mencionó Alonso y es nuevamente desconocimiento incluso a muchas empresas les pasa y con todos los proveedores de nube, eso pasa con todos, que este ya ofrecer características de seguridad asociadas que no generan ni una factura adicional, ni un consumo de créditos, ni algo extra en el costo, pero el cliente no lo sabe o el usuario no lo sabe y no lo utiliza. Sí, ahí digamos que también el reto para nosotros como proveedores de nube, es cambiar esa mentalidad del usuario y enseñarle sobre esas funcionalidades o características, para ello hacer workshops de seguridad, hacer talleres de trabajo sobre el funcionamiento de dichas herramientas o por medio de un evento masivo, así como también realizar Assessment de seguridad, para validar el estado actual a nivel de seguridad de su ambiente o qué otras cosas puedes activar como cliente, no necesariamente pagan-

do más. Segundo punto, a medida que esta tecnología avance como pasa con todo cuando se masifica su costo baja, automáticamente eso hace que su costo vaya empezando a ser más asequible para las personas.

Jeimy J. Cano M.
Diego, puede contarnos algún caso en algún sector de América Latina.

y nuevamente vuelvo a los ejemplos de acciones de hardware propiamente dichas para temas de computación confidencial, pero si ellos empiezan a ver qué, pues hay una mayor demanda de esto la ley básica de la microeconomía no a mayor demanda baja la oferta y al revés a mayor oferta, baja la demanda. Eso hace que los costos pues empiecen a equipararse y a hacer mucho más accesibles para las personas.

Alonso Verdugo M.
El futuro de la computación confidencial es prometedor y hay varios aspectos clave que las empresas pueden esperar en el mediano plazo (3-5 años). En primer lugar, veremos una mayor estandarización en los conceptos y una adopción más amplia de estas tecnologías. La colaboración entre los desarrolladores de hardware y software está abriendo nuevas fronteras, impulsando la evolución de la computación confidencial.

Un ejemplo de adopción temprana es el caso de una pequeña empresa en 2021 que utilizó entornos seguros para proteger información sensible, demostrando que no es necesario ser una gran corporación para beneficiarse de estas tecnologías. Además, la demanda por transparencia en el manejo de datos está creciendo. Los clientes y gobiernos están exigiendo saber dónde están sus datos, cómo se usan y qué medidas se toman para protegerlos.

La conciencia sobre la ciberseguridad ha aumentado. Hace unos años, no éramos tan conscientes de quién manejaba nuestra información. Hoy en día, estamos más alertas. Un ejemplo claro es la inversión en seguridad digital por empresas como Telefónica, que, a pesar de invertir millones, deben asegurarse de que los usuarios también adopten prácticas seguras. (Chema Alonso: “Lo verdaderamente peligroso es dejar solos a los niños en Internet con el ordenador en su habitación, sin saber qué hacen y con quién” - Telefónica (telefonica.com)).

En cuanto a la adopción de la computación confidencial, existen mitos que aún deben ser desmentidos.

Muchas empresas aún des-confían de la nube, pensando que exponen sus datos, cuando en realidad, un servicio de nube hiperescala puede ofrecer mayor seguridad que un centro de datos local mal gestionado.

Para startups y empresas que buscan internacionalizar sus soluciones, especialmente en sectores como la gestión de pacientes diabéticos o hipertensos, cumplir con los estándares de seguridad y privacidad es esencial. Esto no solo protege la información, sino que también abre puertas en términos de comercialización y expansión internacional.

Las empresas pueden esperar un aumento en la adopción de tecnologías de computación confidencial, mayor concientización sobre ciberseguridad, y un entorno regulatorio más exigente. Es crucial que las empresas comprendan estas tecnologías y las integren en su cadena de valor para proteger su capital intelectual y ofrecer transparencia a sus usuarios finales.

Jeimy J. Cano M.
En esta conversación encontrar, que incluso dentro del personal de los mismos proveedores de tecnología, la computación confidencial no se conozca, evidencia una oportunidad para detallarlo en profundidad y validar sus ventajas y limitaciones en las organizaciones en Colombia. Lo anterior nos confirma que es necesario abrir un espacio de reflexión y diálogo alrededor del tema en el gremio de tecnologías de información para avanzar en una postura de seguridad y control que ahora no sólo dispone controles para los datos en reposo y en tránsito, sino que pone igualmente el énfasis a los datos cuando están en uso, particularmente en la ejecución de las aplicaciones en entornos locales y de terceros.

Jeimy J. Cano M.
Para cerrar nuestra sesión agradezco una perspectiva resumen de cada uno sobre lo conversado alrededor de la computación confidencial.

Diego Bueno
Bien, yo creo que queda y de nuevo, no solamente por el hecho de trabajar en Oracle sino por estar en la industria de tecnología, en la cual llevo un poco más de 12 años, y es que a la final uno también debe tener una responsabilidad social de hablar de este tipo de temas con la gente en espacios sociales, no necesariamente en el trabajo, pero ayudar en ese proceso de difusión y que se conozca y que sea una preocupación para el común de las personas, otra vez, y a veces yo también doy algunas charlas de temas de inteligencia artificial y hoy en día el activo más valioso que tiene cualquier empresa son los datos, la información, ese es el activo más importante que tienen las compañías, sin embargo, no todos saben el nivel de madurez que tienen de sus datos, ni la capacidad de explotarlos y cómo eso me ayuda a mí y a mi negocio a mejorar, cómo mi marca mejora su Market share, como puedo atraer más clientes, así las cosas, yo me llevo de esta conversación, la responsabilidad de hablar un poco más de este tema en términos generales, claramente

empezando por mi equipo de trabajo, a quienes les dije que debíamos conocer mucho más de esto y promoverlo con los clientes.

También me gusta mucho que ustedes como promotores de la revista se preocupen por estos temas, porque eso hace que seguramente mucha gente cuando lo vea independientemente que sea Diego y Alonso los que hablen, se interesen por el tema y digan oiga, esto es una necesidad imperiosa en mí industria y tengo que ejecutarlo sin duda.

Alonso Verdugo M.
El futuro de la computación confidencial es prometedor y hay varios aspectos clave que las empresas pueden esperar en el mediano plazo (3-5 años). En primer lugar, veremos una mayor estandarización en los conceptos y una adopción más amplia de estas tecnologías.

La colaboración entre los desarrolladores de hardware y software está abriendo nuevas fronteras, impulsando la evolución de la computación confidencial.

Un ejemplo de adopción temprana es el caso de una pequeña empresa en 2021 que utilizó entornos seguros para proteger información sensible, demostrando que no es necesario ser una gran corporación para beneficiarse de estas tecnologías. Además, la demanda por transparencia en el manejo de datos está creciendo. Los clientes y gobiernos están exigiendo saber dónde están sus datos, cómo se usan y qué medidas se toman para protegerlos.

La conciencia sobre la ciberseguridad ha aumentado. Hace unos años, no éramos tan conscientes de quién manejaba nuestra información. Hoy en día, estamos más alertas. Un ejemplo claro es la inversión en seguridad digital por empresas como Telefónica, que, a pesar de invertir millones, deben asegurarse de que los usuarios también adopten prácticas seguras. (Chema Alonso: “Lo verdaderamente peligroso es dejar solos a los niños en Internet con el ordenador en su habitación, sin saber qué hacen y con quién” - Telefónica (telefonica.com)).

En cuanto a la adopción de la computación confidencial, existen mitos que aún deben ser desmentidos. Muchas empresas aún desconfían de la nube, pensando que exponen sus datos, cuando en realidad, un servicio de nube hiperescala puede ofrecer mayor seguridad que un centro de datos local mal gestionado.

Para startups y empresas que buscan internacionalizar sus soluciones, especialmente en sectores como la gestión de pacientes diabéticos o hipertensos, cumplir con los estándares de seguridad y privacidad es esencial. Esto no solo protege la información, sino que también abre puertas en términos de

comercialización y expansión internacional.

Las empresas pueden esperar un aumento en la adopción de tecnologías de computación confidencial, mayor concientización sobre ciberseguridad, y un entorno regulatorio más exigente. Es crucial que las empresas comprendan estas tecnologías y las integren en su cadena de valor para proteger su capital intelectual y ofrecer transparencia a sus usuarios finales.