Estrategia multinube

DOI: 10.29236/sistemas.n166a6

Consideraciones y retos para las organizaciones modernas.

Resumen
La inestabilidad global y los cambios acelerados por cuenta de las tensiones internacionales generan retos en las empresas en torno a las estrategias digitales previstas para continuar su proceso de transformación digital y la conquista de sus clientes. En este sentido, la multinube aparece como una postura de interés para las organizaciones, en la medida en que les permite no sólo crecer y desplegar rápidamente sus nuevos productos y servicios, sino encontrar un punto de apalancamiento financiero (costo-efectivo) para asegurar su desempeño operacional. Desde esa perspectiva, este artículo hace una síntesis de los modelos propios de la computación en la nube y su esquema de responsabilidades, para situar la estrategia multinube y motivar reflexiones documentadas, de cara a los riesgos que las compañías deben considerar para posicionarse en el contexto digital.

Palabras claves
Multinube, Ciberseguridad, Estrategia digital, Transformación digital, Riesgo cibernético

Introducción

Los recientes reportes internacionales advierten sobre un mundo fragmentado, inestable y de múltiples crisis simultáneas, que crean un escenario complejo para las organizaciones y sus estrategias de negocio. No se ha terminado el proceso de recuperación y manejo del endeudamiento, tanto de las empresas como de los Estados por cuenta de la pandemia, cuando ya se asoma en el horizonte un panorama de recesión económica, tensiones geopolíticas y debilitamiento de la globalización, mostrando síntomas de desacoplamiento de las estructuras de mercado, de las cadenas de suministro y el debilitamiento de las alianzas internacionales que generan inciertos y volatilidades que comprometen la lectura estratégica de las empresas actuales (Colomina et al., 2022).

En este sentido, las inversiones que se han venido realizando por cuenta de una acelerada transformación digital se encuentran en medio de esta nueva encrucijada, lo que obliga a repensar y ajustar los presupuestos de tecnología, las nuevas iniciativas digitales y, muy especialmente, a evaluar el apetito de riesgo actual de la compañía en un contexto que implica mayor atención a las variables geopolíticas y macroeconómicas que afectan la promesa de valor de la empresa. Lo anterior, necesariamente exige al sector empresarial revisar opciones para optimizar sus costos y potencializar sus capacidades para mantener la operación en el mediano y largo plazo (Marsh – Microsoft, 2019).

En consecuencia, la computación en la nube se revela como una opción atractiva y costo-efectiva para los propósitos de optimización de las operaciones, aseguramiento de la infraestructura tecnológica, como una forma de entregar a un tercero especializado el funcionamiento y actualización de las iniciativas digitales que la compañía tiene previstas. En razón a lo anterior, el manejo de los costos de esta alternativa, de pagar por aquello que se usa o se consume de acuerdo con las necesidades específicas de la empresa, establece un marco de trabajo básico para las organizaciones que en la actualidad buscan mantener el “momentum” de la transformación digital y acelerar el despliegue de proyectos que consoliden nuevas experiencias en sus clientes (Woerner et al., 2022).

Si bien para 2025, habrá más de 100 zettabytes de datos almacenados en la nube -para ponerlo en perspectiva, un zettabyte es un billón de terabytes (o un billón de gigabytes) (Sumina, 2022)-, es necesario establecer el mejor modelo de despliegue y operación bien en infraestructuras públicas (compartidas con muchos clientes) o privadas (dedicadas para un solo clien-

te), para concretar no sólo las condiciones económicas de base de esta opción, sino reconocer y avanzar en los retos de un modelo como del otro (o su combinación) para efectos de articular una estrategia corporativa ajustada con la capacidad de riesgo y los desafíos estratégicos de la empresa.

En consecuencia, este artículo busca detallar cómo la estrategia multinube se configura en una opción atractiva para las organizaciones y sus retos actuales, como una forma de expandirse hacia otros mercados, construir nuevos productos/servicios y ganar flexibilidad en su modelo de costos, frente a un escenario de alta volatilidad y cambios, en el que los datos de las personas estarán en el centro de su estrategia y serán parte integral del ejercicio de confianza digital construido en la experiencia misma del cliente.

Computación en la nube. Modelo de responsabilidades

La computación en la nube no es una tendencia nueva para las organizaciones; en el contexto de la pandemia se aceleró su apropiación en las empresas, habida cuenta de la necesidad de operar desde casa y en diferentes espacios disponibles, haciendo que las opciones denominadas "*on premise*" (adquisiciones locales instaladas en los centros de datos) quedaran rezagadas y comprometidas frente al reto de un trabajo remoto y con exigencias de ancho de banda, almacenamiento, seguridad y continuidad, distintos a los que tradicionalmente había tenido la organización.

En este escenario, la estrategia en la nube cambia el modelo de responsabilidades tradicional de la gestión y administración de la tecnología de información, incorporando a un tercero de confianza para que sea el nuevo responsable por mantener la operación con la orientación y guía del ejecutivo de tecnología de la organización, y bajo unos parámetros contractuales y jurídicos distintos, que demandan una lectura cuidadosa de condiciones y un uso controlado de recursos según las necesidades y expectativas de la empresa y sus clientes, en donde la responsabilidad de los datos y su acceso siempre queda en manos de aquel que contrata el servicio.

En el modelo de infraestructura como servicio (*Infrastructure as a Service* – IaaS) la responsabilidad del proveedor está situada desde la configuración técnica de las redes, pasando por el almacenamiento, los servidores, la virtualización y hasta el sistema operativo. De aquí en adelante, lo correspondiente al entorno de ejecución y gestión de API (*Application Program Interfase*) (*middleware*), los elementos concretos de la ejecución de las aplicaciones (*runtime*), las aplicaciones y los datos quedan en manos de la empresa que contrata el servicio (IBM, 2020). El modelo

IaaS es una manera de delegar en un tercero la obsolescencia tecnológica y los costos de mantenimiento propios de la infraestructura.

En el modelo de plataforma como servicio (*Platform as a Service* – PaaS) la responsabilidad del proveedor cubre todo lo señalado para IaaS más los temas del *middleware* y *runtime*, queda en manos del contratante las aplicaciones y los datos. En este modelo, las organizaciones buscan asegurar un despliegue homogéneo de las aplicaciones e iniciativas que desarrolle, para lo cual el proveedor deber mantener un entorno de ejecución ajustado a las necesidades de la organización, siguiendo el plan de proyectos claves que articulen la promesa de valor de la empresa (IBM, 2020). Esto exige declarar al proveedor como aliado estratégico de la compañía.

En el modelo de software como servicio (*Software as a Service* – SaaS), la responsabilidad de proveedor no sólo cubre lo establecido para el modelo PaaS, adicionalmente incluye las aplicaciones, lo que implica un control casi total del manejo y gestión de la infraestructura, entorno de ejecución y programas aplicativos, que demandan una responsabilidad de aseguramiento, continuidad, gestión y seguridad para que el contratante pueda establecer cuáles datos se van a capturar, en qué condiciones de seguridad y control, y cómo se van a usar para los efectos de la estrategia de la empresa (IBM, 2020). En este modelo, el contratante pierde visibilidad de los detalles de la implementación y control sobre posibles vulnerabilidades de las aplicaciones.

Nubes privadas, nubes públicas y nubes híbridas. Apuestas corporativas contemporáneas

La computación en la nube como el nuevo "*commodity*" tecnológico de las empresas juega un papel fundamental en la estrategia digital de las organizaciones actuales. Desde este ejercicio de pago por consumo o uso, las compañías encuentran las capacidades claves necesarias para articular proyectos estratégicos y las distintas experiencias que quieren situar en la retina y expectativas de sus clientes.

Por tanto, se habilitan una serie de opciones para adquirir dichas capacidades que van desde compartir con múltiples clientes un espacio, mantener un espacio privado para el desarrollo de sus iniciativas o tener una combinación de éstas.

Una *nube pública* de acuerdo con la definición de la empresa Red Hat es:

> … un conjunto de recursos virtuales desarrollado a partir de un sistema de hardware que pertenece a una empresa externa encargada también de gestionarlo. La nube se pone a disposición de varios clientes a través de una interfaz de auto-

servicio de manera automática. Es una forma sencilla de adaptar la capacidad de las cargas de trabajo que sufren variaciones inesperadas en la demanda. (RedHat, 2022)

Dentro de sus características se encuentran: (Ausum, 2019)

- Bajo costo: sólo se paga por los servicios que se usan, durante el tiempo establecido. Los costos asociados con el hardware, su administración y mantenimiento, le corresponden al proveedor de los servicios.
- Escalabilidad virtualmente ilimitada: se cuenta con acceso a recursos casi ilimitados en función de las necesidades del cliente. Detrás de estos servicios se encuentran grandes proveedores domo Google, Amazon, Oracle o Microsoft.
- Fiabilidad y estabilidad: al contar con una amplia red de servidores y altos niveles de disponibilidad de grandes jugadores como los mencionados previamente se asegura la prestación del servicio de forma fiable y continua.
- En una nube pública se tiene menos control del sistema, limitando su capacidad para detectar y abordar nuevos riesgos y vulnerabilidades.

Las *nubes privadas* indica la firma Red Hat:

> El conjunto de las tecnologías forma una nube que será privada si proviene de sistemas exclusivos para las personas que los utilizan, quienes se encargan también de gestionarlos. (RedHat, 2022)

Dentro de sus características se destacan: (Ausum, 2019)

- Flexibilidad y personalización: se adapta a las condiciones y necesidades específicas de la organización.
- Seguridad y privacidad: los recursos asignados son exclusivos, por lo que la organización puede establecer y asegurar los datos a su manera bien sean sensibles o no.
- Escalabilidad y costos: hay menos escalabilidad. Los costos de adquisición, gestión y mantenimiento son más elevados.
- Talento humano especializado: se demanda la contratación de talento humano especializado para atender la infraestructura contratada y el aseguramiento de la misma.

Finalmente, las *nubes híbridas* se definen como:

> Una solución de nube que es una combinación entre la nube pública y la privada. Se trata de un entorno de computación que combina características de ambas nubes, permitiendo que los datos y las aplicaciones puedan ser compartidos entre la infraestructura privada y la nube pública. (Ausum, 2019)

Dentro de las características de la nube híbrida se cuentan: (Ausum, 2019)

- Control y seguridad: los datos menos sensibles pueden procesarse en la nube pública a menor costo, mientras la información confidencial permanece protegida en una infraestructura de nube privada.
- Flexibilidad y escalabilidad: los recursos de la nube, prácticamente ilimitados, están disponibles para la organización cuando esta los necesite.
- Costos ajustados: mantener una infraestructura local económica y acceder a las capacidades de la nube pública cuando sea necesario y bajo demanda, pagando solo por los servicios utilizados.
- Complejidad de la administración y gestión: la gestión por parte del contratante es compleja dados los diferentes acuerdos y contratos que se deben administrar, así como las condiciones y exigencias para cada uno de los proveedores involucrados.

Cualquiera de las opciones que la organización tome deberá obedecer a una decisión informada, esto es, consciente de los retos, riesgos y oportunidades en cada uno de los modelos de consumo y uso planteados, teniendo claro que las condiciones contractuales y alcances de cada proveedor deberán ser revisados y analizados detalladamente para efectos de la claridad de posibles situaciones no contempladas y cómo se deberá proceder para proteger a la compañía y los datos de sus clientes.

Estrategia multinube. Un habilitador de la transformación digital

La nube está influyendo en tendencias clave que conducen a casos de uso emergentes que resuelven retos empresariales y tecnológicos únicos. En este sentido, las organizaciones han tomado la ruta de contar con estrategias multinube para concretar lo mejor de ambos mundos (nube híbrida) y motivar impactos tanto a nivel negocio como a nivel tecnológico que apalanquen las estrategias digitales de las empresas.

Los impactos a nivel de negocio se pueden establecer en cuatro elementos fundamentales: (Tang, 2019)

- Crecimiento del negocio: para los cual la incorporación de capacidades analíticas de datos e información se convierte en factor fundamental para la toma de decisiones y actualización de estrategias (casi) en tiempo real para posicionar un producto o servicio.
- Riesgos y regulaciones: uso de algoritmos de cálculo de riesgo de liquidez, monitoreo de las negociaciones y configuración de reportes de solvencia, permiten conocer el estado de la empresa y su nivel de cumplimiento frente a normativas internacionales.

- Reducción de costos: simplificar la infraestructura tecnológica y sus mantenimientos, archivo y almacenamiento de correos electrónicos y voz, analíticas de comportamiento de los clientes.
- Mejora de las operaciones: realizar pagos en tiempo real, implementación de contratos inteligentes, trazabilidad del flujo de pagos e información.

Los impactos a nivel tecnológico se pueden detallar como se presenta a continuación: (Tang, 2019)

- Almacenamiento: disponibilidad para guardar y asegurar datos según la capacidad planeada (incluidos posibles aumentos de datos no planeados).
- Contenedores, API y microservicios: un acceso más rápido y sencillo a los datos de la empresa.
- Gestión de datos maestros: proporcionar una visión del cliente en todos canales e identificar oportunidades de ventas cruzadas.
- Reportes y analítica: obtener información en tiempo real sobre los clientes y elaborar informes tácticos y estratégicos para soportar las estrategias del negocio.

Si bien estos impactos tanto de negocio como tecnológicos son relevantes para la estrategia multinube, es necesario reconocer los riesgos inherentes de esta opción, comoquiera que, en el ejercicio de alineación y coordinación de múltiples proveedores para crear las capacidades necesarias que transformen el negocio, múltiples interacciones son necesarias las cuales crean nuevos puntos ciegos que terminan siendo aprovechados por los adversarios para crear inestabilidad, incierto y caos (Akinrolabu et al., 2018).

De acuerdo con una reciente investigación de Forrester Research (2022), existen cinco grandes riesgos que las compañías deben mantener en el radar cuando toman la decisión de concretar una estrategia multinube. Estos riesgos deben ser revisados y actualizados de forma periódica dada la dinámica inherente de este tipo de estrategias y la evolución permanente de los atacantes para concretar acciones no autorizadas. Los riesgos claves son:

- Robo de datos – generalmente por inadecuadas configuraciones de acceso.
- Ransomware – por lo general provocados por estafas o engaños en las personas.
- Ataques de ataques de ingeniería social – basados en la distracción y el engaño.
- Revelación de contraseñas /Fuga de secretos – generalmente por descuidos de clientes o empleados y/o operaciones de espionaje patrocinadas.
- Ataques a software de terceros y proveedores de servicios en la nube – casi siempre asociados

con intereses corporativos estratégicos y/o pivotes para llegar a otras empresas.

Así las cosas, la estrategia multinube será una opción viable para las empresas y sus necesidades de transformación digital, en la medida en que se entienda que es una decisión estratégica de la compañía frente a su plan de negocios digital de mediano y largo plazo, y no como un proyecto del área de tecnología para apalancar la estructura de costos de la organización (Durg & Podder, 2019).

De otra parte, la estrategia multinube es un ejercicio de apetito de riesgo corporativo que reconoce el riesgo inherente a su despliegue, para lo cual deberá diseñar y simular escenarios de falla sistémica, es decir, de propagación de los efectos tanto en sus proveedores, como en las aplicaciones y estrategias de negocio articuladas. Esto es, preparar y motivar un marco de trabajo de resiliencia organizacional ajustado a las dimensiones y retos de la empresa que vaya más allá de los estándares y buenas prácticas actuales, que pueda responder a amenazas imprevisibles e inesperadas en el ciberespacio (Cano, 2021).

La estrategia multinube demanda conceptualizar, entender y gobernar un ecosistema digital de negocio con sus partes e interrelaciones, con el fin de situar cómo sus diferentes interacciones le dan forma a las expectativas y estrategias digitales de la organización. En este sentido, debe mantener en foco y una postura vigilante sobre los datos, la arquitectura, las comunicaciones con sus diferentes grupos de interés, las tecnologías emergentes, los terceros de confianza, la ciberseguridad, las operaciones de tecnología de información y las regulaciones. Esto es, desarrollar un pensamiento ecosistémico que reconoce cómo los diferentes participantes afectan a los otros y cómo entre todos es posible construir una postura resistente y resiliente frente a la inevitabilidad de la falla (Zukis et al., 2022)

Reflexiones finales

Hasta la fecha, las estrategias multinube han sido de naturaleza reactiva, respondiendo al aumento de las cargas de trabajo y las funcionalidades propias de las iniciativas digitales. Sin embargo, a medida que aumenta la complejidad de los sistemas, es necesario que las empresas redefinan su estrategia de nube y establezcan mejores alianzas con sus terceros de confianza de cara a facilitar y profundizar la transformación digital de las empresas (Durg & Podder, 2019).

Las estrategias multinube de próxima generación deben ser más inteligentes y proactivas, esto es, fortalecidas con inteligencia artificial, analítica de datos y capacidades prospectivas, con el fin de ajustarse rápidamente a las demandas de sus clientes.

En este sentido, las organizaciones deben atender con claridad su plan estratégico corporativo y sus estrategias digitales para encontrar la mejor relación costo-beneficio en los contratos multinube, que le permitan tener mayor flexibilidad y capacidad de crecimiento de cara a las exigencias de nuevas experiencias de sus clientes, y a un aumento de conectividad y de aplicaciones en manos de las personas quienes estarán atentos a evaluar, adoptar, desechar o ignorar las iniciativas digitales de las empresas.

Una estrategia multinube deberá crear una cadena de confianza entre sus diferentes participantes con el fin de construir en su interior una mayor confiabilidad en la configuración, aseguramiento y despliegue de los diferentes esquemas disponibles para el uso y operación de la infraestructura tecnológica disponible, así como las medidas y consideraciones de seguridad y control que hagan más resistente y resiliente esta infraestructura frente a la inevitabilidad de la falla y a los efectos de las tensiones geopolíticas y cibernéticas globales, que pueden terminar comprometiendo las expectativas de posicionamiento estratégico de las empresas (Yeluri & Castro-León, 2014).

Finalmente, la estrategia multinube deberá mantener en foco al menos siete aspectos claves para concretar su promesa de valor empresarial y asegurar los retos propios de la transformación digital de las organizaciones: (Kime, 2022)

- *Experiencia del usuario* - Agilidad, portabilidad y confianza en las interacciones del cliente con la iniciativa digital.
- *Seguridad/ciberseguridad* - Segregación de accesos, validación de conexiones y aseguramiento de canales.
- *Monitorización y actualización de activos* - Descubrir, identificar, inventariar y evaluar continuamente las exposiciones de los activos de la empresa y su relación con los terceros de confianza.
- *Inteligencia y cacería de amenazas* - Evaluación proactiva de las intenciones y capacidades de los adversarios en el mundo físico y el ciberespacio.
- *Servicio de Acceso Seguro de Borde* (*Secure Access Service Edge*) - Marco único que permite habilitar y gestionar los requisitos de acceso a datos y aplicaciones en la nube.
- *Ecosistema digital* - Conjunto de infraestructura, servicios, aplicaciones y usuarios que interactúan entre sí para crear valor a los clientes.
- *Gestión del gasto en la nube* – Evaluación financiera y técnica permanente de cara al apetito de riesgo, la estrategia digital y las capacidades requeridas para desplegar las iniciativas digitales previstas.

Referencias

Akinrolabu, O., New, S. & Martin, A. (2018). Cyber Supply Chain Risks in Cloud Computing - Bridging the Risk Assessment Gap. Open Journal of Cloud Computing (OJCC). 5. 1-19. https://www.researchgate.net/publication/321881757_Cyber_Supply_Chain_Risks_in_Cloud_Computing_-_Bridging_the_Risk_Assessment_Gap

Ausum (2019). Pública, privada o ambas: ¿qué es la nube híbrida? https://ausum.cloud/es/publica-privada-o-ambas-que-es-la-nube-hibrida/

Cano, J. (2021). Resiliencia cibernética. El arte y la ciencia de desviarse (y equivocarse) para encontrar el camino en el contexto digital. Global Strategy. Global Strategy Report No. 39. https://global-strategy.org/resiliencia-cibernetica-el-arte-y-la-ciencia-de-desviarse-y-equivocarse-para-encontrar-el-camino-en-el-contexto-digital/

Colomina et al. (2022). El mundo en 2023: diez temas que marcarán la agenda internacional. CIDOB Notes Internationals. No. 238. https://bit.ly/3YHt7uK

Durg, K. & Podder, S. (2019). Navigating the interoperability challenge in multi-cloud environments. Accenture. https://www.accenture.com/us-en/blogs/cloud-computing/kishore-durg-cloud-interoperability-challenges

Forrester (2022). Unlocking Multicloud's Operational Potential. Forrester Research. https://www.datocms-assets.com/2885/1659554932-unlocking-multiclouds-operational-potential-forrester-hashicorp.pdf

IBM (2020). Securing your journey to hybrid multicloud. Protecting workloads to enable business innovation and growth. IBM Security. https://www.ibm.com/security/digital-assets/hybrid-multicloud-ebook/pdfs/Secure_Hybrid_Cloud_EB.pdf

Kime, B. (2022). The Future of Hybrid Work and Cybersecurity Risks. Security Boulevard. https://securityboulevard.com/2022/09/the-future-of-hybrid-work-and-cybersecurity-risks

Marsh – Microsoft (2019). Global Cyber Risk Perception Survey 2019. https://www.microsoft.com/en-us/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

RedHat (2022). ¿Qué es la nube pública? https://www.redhat.com/es/topics/cloud-computing/what-is-public-cloud

Sumina, V. (2022). 26 Cloud Computing Statistics, Facts & Trends for 2023. Cloudwards. https://www.cloudwards.net/cloud-computing-statistics/

Tang, M. (2019). Cloud computing. More than just a CIO conversation. Deloitte. https://www.deloitte.com/content/dam/assets-shared/legacy/docs/perspectives/2022/gx-cloud-banking-2030-fsi.pdf

Woerner, S., Weill, P. & Sebastian, I. (2022). Future ready. The four pathways to capturing digital value. Boston, MA. USA: Harvard Business Review Press

Yeluri, R. & Castro-León, E. (2014). Building the infrastructure for cloud security. A solutions view. New York, USA: Apress

Zukis, B., Ferrillo, P. & Veltos, C. (2022). The great reboot. Succeding in a complex digital world under attack from systemic risk. Second edition. USA: DDN Press.

***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–.*