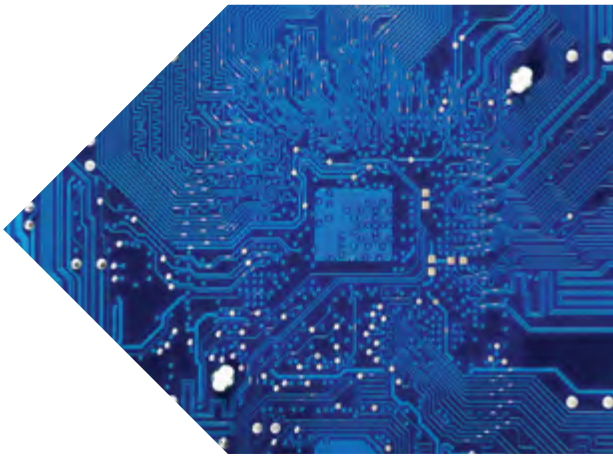
MOORE Colombia

TI

RIESGOS EN LA NUBE Y ASPECTOS RELEVANTES PARA SU GESTIÓN



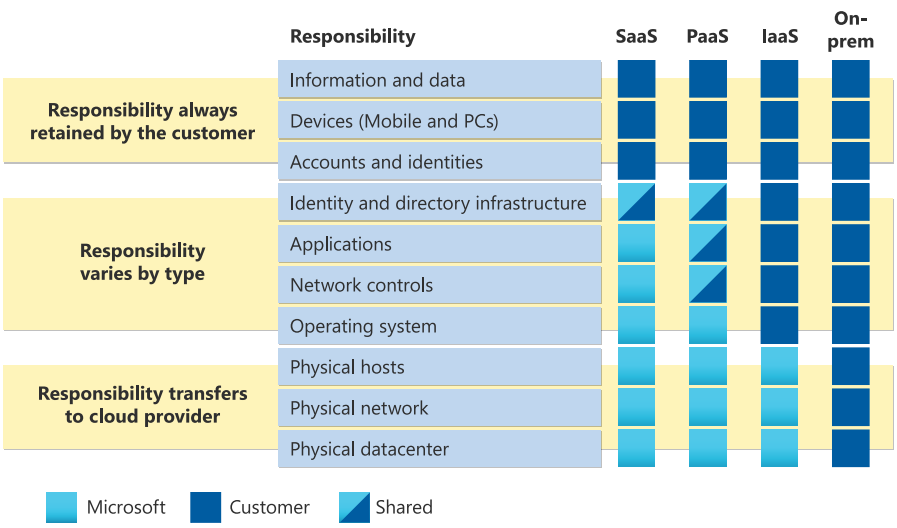
Cuando evaluamos los servicios en nube desde la perspectiva de negocio, podemos encontrar como elementos mínimos característicos la reducción de costos en la gestión operativa de los sistemas y/o plataformas, el nivel de escalabilidad de los recursos, la disponibilidad a la información y flexibilidad en los tiempos. Cada uno de estos elementos, aportan un alto valor a la rentabilidad y evolución de las compañías; y aunque como toda tecnología, existen desventajas por la dependencia con terceros que podrían dificultar la gestión de problemas, entre otros, la adopción de servicios en nube se ha convertido en una solución lógica y viable que, empezando por posicionarnos en el escenario de la transformación digital, abre las puertas a nuevas posibilidades de aprovechamiento de recursos. En Colombia, las compañías han adoptado cambios significativos, pospandemia y nuevamente el uso de servicios en nube resalta.

De acuerdo con lo indicado por la CELAC - Comunidad de Estados Latinoamericanos y Caribeños, en su publicación “Digital technologies for a new future” del 2021:

- “Los servicios en la nube se han vuelto dominantes como impulsores de la transformación digital. La nube proporciona recursos de tecnología de la información flexibles que crean las condiciones para modelos de negocio transformados y provisión de servicios, procesos de marketing ágiles y fácil experimentación con nuevos servicios sin necesidad de nuevos recursos de tecnología de la información, además de ofrecer una mayor ciberseguridad. La modalidad más utilizada es el software como servicio, con soluciones como correo electrónico, videoconferencia, aplicaciones de oficina, gestión de relaciones con clientes, planificación de recursos, automatización de flujos de trabajo y seguridad. Además, permite el uso de herramientas de apoyo al comercio electrónico, como chatbots y mensajería, que amplían los canales de comunicación con los clientes”.
- De acuerdo con las estadísticas, “en 2019, la utilización de software como servicio constituyó casi el 50 % del mercado de la nube en América Latina y el Caribe, seguidos de la utilización de la infraestructura como servicio, con un 46%, y la utilización de las plataformas como servicio, con un 4,3 % (GlobalData, 2020). La región representa el 8 % del tráfico global en la nube, y se espera que este tráfico crezca un 22 % en promedio por año hasta 2023”.
- Para el año 2020, del total de 27 países de América Latina y el Caribe, Colombia es uno de los 16 que contaba con una Agenda Digital en proceso de implementación, lo que impulsa eventualmente la adopción de servicios en la nube.

Es claro que la nube llegó para quedarse y apoyarnos en el proceso de evolución corporativa, pero lo que no es tan claro aún es la apropiación de las compañías en la gestión del riesgo implícito que viene asociado con la adopción de la tecnología y la mejora continua. Esto se refiere al diseño de controles que permitan asegurar, no solo, la calidad del servicio del proveedor y el cumplimiento de los elementos contractuales, sino el adecuado dimensionamiento de los riesgos relacionados con el servicio y la implementación y funcionamiento de controles para su mitigación.

La adopción de servicios en nube define un esquema de responsabilidad compartida entre el Consumidor (Cliente) y el Proveedor para su gestión operativa, podemos tomar como referencia el modelo definido por Microsoft Azure según se muestra en la imagen extraída de su sitio web – cada proveedor define su modelo. Este esquema establece hasta dónde llega la responsabilidad del Proveedor y dónde empieza la del Consumidor en la operatividad del servicio.



Ubicación: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Pero esto no es todo, sin que importe la modalidad del servicio de nube adoptado, el dueño de los datos siempre será el Consumidor, por lo que no es posible tercerizar la gestión del riesgo de la seguridad de la información y la responsabilidad en el cumplimiento de elementos regulatorios internos o externos (según aplique por el sector económico de operación); y en el caso específico de Colombia la responsabilidad de la gestión del Control Interno de TI.

La correcta gestión de un servicio de nube debe enfocarse en (a) la administración del contrato y acuerdo de nivel de servicio, y (b) la administración del riesgo del servicio, este último basado en un análisis que, como mínimo, incluya lo siguiente:

- Relevancia y valoración del impacto del servicio desde los puntos de vista financiero y operacional.
- Evaluación del servicio frente al Análisis de Impacto al Negocio (BIA).
- Relevancia del servicio en el cumplimiento de normas / regulaciones externas que apliquen a la organización, tales como Ley 1581 – Privacidad de Datos, Circular 007 – Ciberseguridad (para entidades vigiladas por la Superintendencia Financiera), Estándares del PCAOB (para compañías que cotizan en la bolsa de Nueva York).
- Relevancia del servicio en el cumplimiento de normas corporativas locales / globales.
- Relevancia del servicio para la evaluación del Control Interno realizada por el Revisor Fiscal.
- Relevancia del servicio para sistemas establecidos y certificados como ISO 27001 – Seguridad de la Información.

La consideración de estos elementos permite dimensionar los riesgos asociados al servicio de nube, de manera que puedan identificarse dentro de la organización los actores interesados, para definir los controles adecuados de gestión.

Dependerá del resultado del análisis sobre el riesgo del servicio si un reporte de aseguramiento (ISAE 3402 o similar) será indispensable para conocer la gestión del Control Interno de los proveedores y el modelo de riesgos y controles de los servicios que ellos prestan; o bien sea posible desarrollar procedimientos periódicos de control, o trabajar con una combinación de los anteriores; en todo caso, la organización estará cumpliendo su objetivo de ir a la nube, al tiempo que gestiona el riesgo y fortalece su control interno.

Con lo anterior, es importante que las organizaciones realicen ejercicios de autoevaluación con los que puedan identificar si la forma en como gestionan a sus proveedores y servicios en nube tiene debilidades que denotan riesgos no administrados o simplemente oportunidades de mejora continua.

Adriana Piñango – Gerente Senior de Consultoría
Email: apinango@moore-colombia.co
Location: Bogota, CO

Camilo Escobar – Supervisor de Consultoría
Email: cescobar@moore-colombia.co
Location: Bogota, CO

MOORE Colombia

www.moore-colombia.co