¿Innovar moviéndose a la nube es seguro para la organización?

mexis aggity

Una pregunta muy frecuente con los tomadores de decisiones ya que están planeando mover su infraestructura tecnológica a la nube para poder ser más ágiles e innovar.

La innovación quizá es la primera razón por la cual se empieza a hablar de la nube como una opción para poder dejar atrás la infraestructura en sitio de las organizaciones y buscar esa agilidad. Innovar forma parte de la transformación digital y que se vio acelerada por el cambio de la antigua normalidad a esta nueva normalidad.

Hay muchas definiciones de innovación, entre las que más me han llamado la atención se encuentran: "innovación es convertir una idea en una solución que añade valor desde la perspectiva del cliente", "innovación es la aplicación de ideas que son novedosas y útiles", "innovación es acerca de seguir siendo relevantes"; incluso Barak Obama, el ahora expresidente de los Estados Unidos mencionó que "la innovación es la creación de algo que mejora la forma en que vivimos".

La nube ha demostrado ser una estrategia que ayuda a las empresas a capitalizar nuevas oportunidades y diferenciarse para las organizaciones, incluso permitiendo acelerar procesos que antes no era posible.

Es el impulsor directo de la innovación de una nueva sociedad de la información, una sociedad que cada vez requiere de más inmediatez y disponibilidad con elementos de confiabilidad y tecnología.

¿Cuándo íbamos a pensar que estaría al alcance de un clic una infraestructura completa? Recuerdo que hace años para incrementar la infraestructura era necesario hablar al proveedor para que tomara un pedido y que enviara un mes después los equipos para poder configurarlos. Esos tiempos quedaron atrás, uno puede tener una serie de servidores en cuestión de minutos. En otros casos, la misma infraestructura se modifica según los requerimientos que se van presentando.

La principal razón por la cual una organización se mueve a la nube tiene que ver con reducción de costo, desde los esquemas de pago por uso, la flexibilidad que permite hacer cambios sin impactar a largo plazo a la empresa y finalmente poder cambiar de gasto de capital a gasto operativo (CAPEX vs OPEX).

Pero no siempre hay que ver la parte económica al inicio. La nube, como todo, trae muchas ventajas, pero también algunos riesgos.

Es posible implementar los conceptos básicos de ciberseguridad: Confidencialidad, Integridad y Disponibilidad en los diferentes servicios de la nube que se van a implementar. Complementa los planes de continuidad de negocio, se puede convertir en nuestro centro de datos alterno, parte del plan de recuperación de desastres y mucho más.

Pero… siempre hay un, pero. La nube en muchos de los casos no tiene elementos de ciberseguridad por defecto o activados. También en otros casos se tendrá que cerciorar que estén bien configurados.

Ha habido muchos casos donde a un administrador de base de datos se le olvidó colocar una contraseña a una base de datos permitiendo que se tenga acceso desde Internet. Algo que incluso ha llegado a que las autoridades de protección de datos personales multen a la empresa relacionada con esto.

La flexibilidad de la nube puede generar falta de control y falta de visibilidad.

Administradores que implementan sin una estrategia pueden estar generando una telaraña de infraestructura que posteriormente será más complicada integrar y asegurar.

La opción por uso sin un límite puede generar un gasto no controlado o hasta que ciertos recursos sean usados indiscriminadamente.

Simplemente por irse a la nube no se tiene ciberseguridad. Se tienen que hacer varias acciones para poder asegurar la infraestructura, una estrategia y complementarla con los análisis de riesgo y pruebas que normalmente se harían a cualquier infraestructura.

Entonces, no es momento que limite o bloquee el proyecto de migración a la nube, tampoco la transformación digital de la organización hacia la nube. Mejor busque al estratega y pregunte cómo se incorporará la ciberseguridad en este proyecto o migración. Trate de que la ciberseguridad esté presente desde la creación de la idea, desde que se empieza a innovar y no al finalizar el proyecto para validar que no hay riesgos.

Al final, un piloto siempre revisa de forma anticipada si un avión está en capacidad de volar; nunca he visto un piloto iniciar carrera de despegue y en el aire revisar si tiene combustible y aceite. Siempre lo hará cuando esté a ras de suelo. Igual debe ser la ciberseguridad.

Autor: Andres Velazquez
Fuente de información: www.forbes.com.mx