UTN FRCU
UNIVERSIDAD TECNOLÓGICA NACIONAL
Facultad Regional Concepción del Uruguay

2013 CoNaIISI
UTN FRC INGENIERÍA EN SISTEMAS DE INFORMACIÓN

Cloud Computing:
Aspectos relevantes sobre la seguridad.

Biondi, María Juliana - Eckerdt, Mariano Ignacio - Medina, Osvaldo Nicolás
Monetta, Agustín Ignacio - Róttoli, Giovanni Daián.

Administración de Recursos, 4º Año Ingeniería en Sistemas de Información.

Abstract

Empleando la búsqueda blibliográfica, se han comparado las opiniones extraidas de tres papers, obteniendo los lineamientos generales que concuerdan y difieren entre ellos sobre los aspectos más relevantes de la seguridad de los servicios virtualizados. También se tratan aquellos que surgen del establecimiento de la relación entre el servidor de servicios y el cliente.
Este trabajo sirve para ampliar la visión del lector sobre la problemática y comprenda los nuevos desafíos que genera esta tecnología.

Resultados

Los autores estudiados coinciden en cuáles son los riesgos que trae consigo la virtualización de documentación importante para los clientes del servicio: cumplimiento normativo, localización de datos, aislamiento de datos, recuperación ante desastres, viabilidad a largo plazo, entre otros.
Algunas empresas podrían rechazar completamente esta tecnología debido a los riesgos en la seguridad de sus datos que esto implica. Sin embargo, si se aplicaran todas las políticas de seguridad tales que garantizaran que los servicios en la nube tienen el mismo o superior nivel de seguridad que los sistemas on-promise, esto podría provocar una sobrecarga de datos aumentando la latencia del sistema, siendo así la performance un desafío más.
Ristov y otros, critican la falta de especificidad de la norma ISO27001:2005, debido a que esta define requerimientos mínimos sin tener en cuenta el tamaño tipo o naturaleza de la organización que lo aplica.
Además, estos autores coinciden en sugerir que el proveedor de servicio en la nube debería cubrir características de seguridad tales como Data Privacy Regulation and Standards Compliance, la cual no solo se refiere al cumplimiento de los estándares actuales como ISO27001, sino también aquellas regulaciones que el cliente requiera para mantener la privacidad sus datos en el sistema; Multi-tenant environment, permitir el acceso múltiple al sistema por lo cual debería, además, el servidor clasificar a las usuarios en categorías y establecer medidas en consecuencia, para asegurar un uso confiable de la nube respecto de los demás usuarios.
Un ítem fundamental a considerar es el manejo de los datos, en cuanto a la protección brindada por el servidor respecto a los demás clientes que utilizan la misma cloud pública (Isolation o Aislamiento), y protocolos de actuación establecidos frente a un ataque externo. Observar e identificar esos otros clientes que utilizan dicho servidor actualmente, y prestar especial atención a la situación financiera y legal del proveedor del servicio, verificando si se cumple con las normativas vigentes.
El más completo de los papers elejidos fue “Cloud Computing Security in Business Information Sistems”, ya que destaca más aspectos e incluye principios para sus soluciones, tales como: “Loss of Control”, “Data Location”, “Heteroheneity, Complexity, Interoperability” y “Data Proteccion”, entre otros ya mencionados.
En este, además, se destaca la relevancia de la relación entre el proveedor y el cliente, los cuales deben llegar a un acuerdo que satisfaga las necesidades del cliente y el proveedor sea capaz de cumplir.
Esto no es siempre posible, por ejemplo, si el proveedor solo dispusiera de servidores en Estados Unidos y se requiere que la información sea almacenada fuera de este país. Sin enbargo, en este caso, el cliente podría determinar que cierta información sea tratada por su sistema on-promise y cierta otra por su proveedor, así disminuyendo la carga en su sistema y manteniendo el control sobre aquella información considerada crítia para la empresa, ya sea porque no puede faltar o porque debe quedar limitado, por razones legales o de negocio, al exlusivo conocimiento interno.
Una buena posibilidad, sería otorgar tratamiento diferencial según qué tipo de información sea, y los requerimeintos de seguridad de la misma. Así, Security-as-a-service se aplicaría solo en los casos necesarios, manteniendo el rendimiento del resto del sistema.

Conclusión

La computación en la nueve no siempre plantea problemas de seguridad desconocidos, sino que genera nueva dificultades para resolverlos.
Uno de los mayores desafíos es lograr una norma única que asegure un nivel de seguridad mínimo comparable al de los sistemas tradicionales dentro de las empresas.
La Security-as-a-service podría ser una buena solución para lograr ello, aplicandolo solo para aquellos clientes que lo requieran y así mantener el resto de los recursos disponibles. Sin embargo, esta es una problemática general que preocupa la gran parte de las empresas, por lo cual se debería desarrollar técnicas que mejoren la seguridad general de la nube.