Valoración final y conclusiones del mundo Cloud

Author : j.carazo.colina

Categories : Auditoría, Certificación y Calidad de Sistemas Informáticos, General

Date : 1 diciembre, 2018

En este quinto y último post, mencionaré brevemente cuáles han sido los puntos más importantes de los últimos 4 posts, continuaré con la explicación de algunas de las cuestiones que me deje en el tintero y finalmente haré una valoración de todo el trabajo realizado y que me ha supuesto la realización de este trabajo.

En primer lugar, debo decir que el mundo del Cloud Computing es tan amplio que la mayor dificultad que he tenido para la redacción de estos Posts ha sido el poder filtrar y mostrar aquella información más relevante. Dicho esto, considero que si bien es cierto que en el tercer y cuarto post hable de los riesgos y controles respectivamente, hubo algunas cuestiones que no trate respecto a la mitigación de riesgos.

Antes de definir algunas técnicas de mitigación, conviene repasar algunos de los riesgos más comunes en Cloud computing [1], como son la pérdida de propiedad intelectual, la confianza y

la calidad de los acuerdos firmados con el tercer y seguramente el más importante de todos, la protección de los datos.

En este sentido, según se detalla en la presentación elaborada por Protiviti y publicada en KnowledgeLeader [2], una vez se identifican las áreas de riesgos, se deben implementar controles con un claro objetivo: la mitigación de los riesgos estos riesgos.

Por ejemplo, en el caso de la propiedad intelectual, se propone la instauración de controles de monitorización, un diseño seguro y encriptado de la propia arquitectura y una gestión adecuada de las políticas de copias de seguridad. Las empresas, dependen en gran medida de uno de los activos más valiosos: el conocimiento que poseen y la información que respalda a dicho conocimiento. Por lo tanto, en el caso de tener dicho conocimiento almacenado en un tercero, es realmente importante asegurarse de que se estén implementadas unas buenas políticas de seguridad.

Por otro lado, se menciona como uno de los puntos clave el implantar políticas de control de acceso efectivas y un sistema de autenticación seguro para tener acceso al CSP. Como ya he mencionado anteriormente, el punto central es la protección de los datos y por ende, la forma de mitigar posibles problemas y brechas de seguridad viene por tener sistemas que sean seguros por defecto y por diseño. Para hacer estas dos características efectivas, es necesario definir de antemano la segregación de roles y funciones y después implantar estas políticas.

Por último, con el fin de llevar a cabo controles más exhaustivos es igual de importante la tenencia de unas gestión de logs adecuada. Los logs, son el mejor sistema para comprobar y revisar el funcionamiento de los sistemas alojados en la nube. Por lo tanto, es necesario que estos logs sean accesibles en todo momento y que mediante una gestión segura se asegure su integridad.

Una vez explicado este breve apartado sobre la mitigación de los riesgos, me gustaría concluir esta serie de Posts con unas valoraciones generales.

Considero que el Cloud Computing es el futuro y debido a sus grandísimos potenciales todas las empresas que cuenten con recursos suficientes adoptarán de una forma u otra la tecnología Cloud. No obstante, antes de adoptar la tecnología es necesario estudiar el sistema que mejor se adapta a las necesidades de cada empresa. No hablo solo de la parte IT sino también a aquellas cuestiones que he enfatizado como son los acuerdos contractuales o el derecho a la realización de auditorías independientes (el estándar SAS 70 entre otros) [3].

Por otra parte, desde mi punto de vista las empresas deben seguir una regla de oro básica: aplica al menos los mismos criterios de seguridad a los sistemas que tienes en la nube, respecto a los sistemas propios. El hecho de externalizar los recursos no implica una externalización de responsabilidades.

Finalmente, creo que esta serie de Posts me ha permitido enriquecer mis conocimientos sobre este campo en particular, y también considero que la parte de auditar estos sistemas en la nube, no difiere mucho a una auditoría IT de los sistemas tradicionales. No obstante, aunque la

metodología pueda parecer similar, el impacto que pueden tener estos riesgos y radicalmente diferente.

[1] "Risks in Cloud Based Services: A Primer | KnowledgeLeader." https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/gurisksincloudbasedservicesaprimerguide. Se consultó el 1 diciembre 2018.

[2] "Cloud Computing Training Guide | KnowledgeLeader." https://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/GUCloudComputingTrainingGuide. Se consultó el 1 diciembre 2018.

[3] "SAS 70 Service Organization Auditing Standards, Public Accounting ...." http://sas70.com/. Se consultó el 1 diciembre 2018.