4. Valoración de Servicios Cloud

4.1.2 Beneficios y Riesgos de los Servicios en Cloud (II).

Ya hemos visto los beneficios y riesgos o barreras que en general presentan los servicios en modo cloud, el informe de INTECO-CERT sobre riesgos y amenazas en cloud computing, hace un análisis de éstos según la titularidad de la infraestructura o el tipo de servicios, viendo que estos beneficios o barreras pueden destacar de manera especial como pasamos a comprobar:
Titularidad pública y acceso al público en general. En este caso cabe destacar la facilidad de la escalabilidad, la eficiencia del pago por uso y el ahorro en tiempo y costes. Como contrapartida tenemos que la infraestructura se comparte con más organizaciones desconociendo qué otros clientes confluyen en la infraestructura, además de tener un menor control en los mecanismos de seguridad.

Titularidad **privada**. Nos permite adoptar políticas internas propias, favorece el trabajo colaborativo entre sedes distribuidas, pero, por el contrario tendremos que afrontar un elevado coste de inversión material, dependiendo de la limitación que presente la infraestructura creada y presentará un ROI a más largo plazo. En el caso de abordar la infraestructura de forma privada con otra u otras organizaciones, reduciremos los costes y mejoraremos el ROI, a cambio tendremos que consensuar la seguridad y los procedimientos de explotación con las otras organizaciones.

A menudo se utiliza tanto las de titularidad pública como privada en aras de asegurar aspectos como la portabilidad de datos o de aplicaciones, en este caso las ventajas y barreras será un compendio de las de cada caso.

Pero ateniéndonos no a la titularidad de la infraestructura, sino al **tipo de servicio** que nos ofrece, software, plataforma o infraestructura, cabe destacar los siguientes beneficios y riesgos o barreras.

SaaS. Son servicios llave en mano que reducen los costes hard y soft y de operación y mantenimiento, pero la seguridad la controla el proveedor limitándonos a elegir preferencias o privilegios según qué usuario.

PaaS. En este caso nos olvidamos de la gestión de la compra y mantenimiento, así como de la gestión de las instalaciones físicas, pero tendremos un control parcial en las aplicaciones y en la configuración del entorno. La seguridad se establecerá según acuerdo proveedor-usuario de la plataforma contratada.
IaaS Nos evitamos la compra en sí de los recursos, sólo consideramos recursos u objetos virtuales a los que se accede por un interfaz de usuario, definiendo el entorno y la gestión de la

seguridad por parte del usuario que contrata la infraestructura.

Como vemos siempre hay factores de riesgos, pero no debe ser un hándicap determinante, pues a menudo estos factores pueden transformarse en oportunidades. Tomemos el que a menudo se expone como factor de riesgo más determinante, el de la seguridad.

LA SEGURIDAD COMO ELEMENTO DIFERENCIADOR

La seguridad constituye una prioridad para muchos clientes en nube. Los clientes toman las decisiones relativas a la adquisición basándose en el renombre del proveedor en cuanto a confidencialidad, integridad y resistencia a los fallos, así como en los servicios de seguridad ofrecidos por el proveedor, todavía más que en los entornos tradicionales.

Éste es un motivo de peso para que los proveedores en nube mejoren sus prácticas de seguridad y generen competencia en este aspecto, por lo que el factor de riesgo de la seguridad cada vez es menor si tenemos en cuenta las buenas ofertas que hay en el mercado.

Referencias:

- Cloud Computing. Benefits, risks and recommendations for information security. Págs. 17-20