RUBRICA
CLOUD COMPUTING

Una nuvola…di incertezza
Costi nascosti e rischi del Cloud Computing

INDICE

INTRODUZIONE

Una delle *disruptive technology* più discusse negli ultimi anni nel mondo dell'IT è sicuramente il **Cloud Computing**, definito da Gartner come *"una modalità secondo la quale funzionalità IT scalabili e flessibili vengono erogate sotto forma di servizi ai clienti, utilizzando le tecnologie Internet".*

La "Nuvola" sta acquisendo un crescente successo[1], soprattutto tra le piccole e medie imprese e nella Pubblica Amministrazione che sempre più di frequente migrano verso soluzioni sviluppate, raggruppate e confezionate come **offerte di servizi in outsourcing** per le quali il Service Provider usa una o più tecnologie di Cloud Computing all'interno dell'architettura complessiva della soluzione.
Questi servizi possono essere forniti direttamente da un Cloud Provider o attraverso un aggregatore di servizi per la fornitura di **soluzioni di business/IT pre-ingegnerizzate** e configurabili in **tempi brevi** e **con costi ridotti**.

In entrambi i casi il modello di esercizio al quale si fa riferimento è quello del Public Cloud, nel quale i servizi sono resi disponibili al pubblico su Internet, diverso dal modello del Private Cloud, costituito da una rete o un data center proprietari, gestiti dalla stessa azienda che se ne serve, che utilizzano tecnologie di Cloud Computing come la virtualizzazione.

Sebbene tali servizi siano in piena evoluzione e tutt'altro che consolidati, sono attualmente classificati in **tre categorie**:

- **SaaS-Software as a Service**:na rivisitazione dell'approccio ASP (Application Service Provider), con il quale l'Outsourcer mette a disposizione dei propri client dei servizi applicativi (ERP, CRM, Office, Desktop,…) fruibili attraverso interfacce web;
- **Paas-Platform as a Service**:un ambiente completo di infrastrutture, sistemi operativi, librerie, middleware, etc., messo a disposizione in tempi brevi e a costi ridotti rispetto a soluzioni ad hoc, per la progettazione, lo sviluppo, il testing, il rilascio e l'hosting di applicazioni specifiche;
- **aaS-Infrastructure as a Service**: risorse elaborative e di rete disponibili on-demand attraverso tecnologie di virtualizzazione;tipicamente: capacità elaborativa, RAM, spazio di archiviazione, software di base, banda di accesso. Tutti gli spazi e i servizi di manutenzione e aggiornamento sono normalmente inclusi ed erogati in modo del tutto trasparente.

Il NIST[2] ha dato una definizione oggi ampiamente condivisa che fuga ogni dubbio rispetto alle caratteristiche di cui un servizio dovrebbe essere dotato per poter rientrare nella **categoria Cloud [1]**:

- **On demand self-service**: il cliente può usufruire dei servizi in base alle sue esigenze, in autonomia, senza il bisogno di interagire fisicamente con il service provider;

1 Il crescente interesse delle aziende verso soluzioni IT di Public Cloud è confermato da un'analisi di Gartner, che ha stimato, per il quinquennio 2011-2016, una spesa complessiva di 112 Miliardi di Dollari per SaaS, PaaS, IaaS [2][3]

2 NIST = National Institute of Standards and Technology è l'agenzia del governo degli Stati Uniti d'America che si occupa della gestione delle tecnologie.

- **Broad Network Access**: i servizi sono erogati agli utenti attraverso la rete e sono accessibili da qualsiasi piattaforma del cliente (smartphones, tablets, laptops e postazioni di lavoro tradizionali);
- **Resource Pooling**: le risorse IT del provider sono raggruppate per servire più clienti, in un modello in cui risorse sia fisiche che virtuali (capacità elaborativa, storage, memoria, banda di accesso) vengono assegnate dinamicamente ai consumatori sulla base delle loro richieste;
- **Rapid elasticity**: i servizi offerti hanno un'elevata scalabilità, per poter rapidamente adattarsi alle richieste dei clienti. Per il cliente le risorse da utilizzare spesso appaiono illimitate e possono essere messe a disposizione quando ne ha bisogno e in qualsiasi quantità;
- **Measured service**: i sistemi Cloud controllano ed ottimizzano l'utilizzo delle risorse in automatico, garantendo trasparenza sull'utilizzo dei servizi sia ai providers che ai consumatori.

La virtualizzazione, quindi, non basta!

Il diffondersi di servizi in outsourcing basati sul Cloud in sostituzione dei tradizionali servizi sta portando, ovviamente, ad un **cambiamento delle dinamiche di mercato** in termini di **processo di fornitura**, struttura degli **accordi** e **modello di delivery**.
Per i **servizi IT tradizionali,** basati su un modello di delivery 1 a 1 (1 provider e 1 consumer), la fornitura prevedeva più customizzazioni e quindi gli accordi richiedevano lunghi periodi di negoziazione, erano complessi e includevano condizioni poco flessibili (ad esempio legate al trasferimento fisico di persone e asset).
Nel **nuovo scenario Cloud**, in cui il modello di delivery è 1 a molti (1 provider, più consumers), invece, vengono proposte soluzioni fortemente virtualizzate e standardizzate, con accordi standard e pronti alla firma, più semplici, più flessibili e ottimizzati per essere efficienti.
In tale contesto, il **Cloud** ha, quindi, tutte le carte in regola per rappresentare un **acceleratore per il business della piccola e media impresa e della Pubblica Amministrazione**, grazie alla possibilità che offre di implementare servizi condivisi, garantendo la **protezione dei dati**, risparmiando sui costi ed incrementandone l'**efficienza**, facendo leva anche sulla **standardizzazione delle tecnologie e dei processi**, nonché riducendo l'ammortamento dei costi lungo l'intero ciclo di vita dei sistemi informatici, **senza investimenti iniziali** elevati e valorizzando quanto già presente.

Come qualsiasi innovazione, però, ha dei "**difetti di gioventù**" che determinano **costi e rischi non immediatamente evidenti**, che devono essere giustamente soppesati perché non diventino un freno nel contesto specifico del cliente. È evidente, quindi, la necessità di effettuare delle **analisi preliminari** volte ad individuare tali rischi e costi nascosti, molto spesso dovuti a **carenze strutturali dei contratti** e ad un'immaturità delle dinamiche di contracting tra i Cloud service providers e i clienti.

In questo articolo cercheremo di **indirizzare** alcune delle **problematiche più critiche** da tenere in considerazione, gestire e conteggiare prima di migrare verso il Cloud.

Costi nascosti e rischi del Cloud

Quando si valuta la possibilità di implementare una soluzione Cloud bisogna stare attenti a non farsi ingannare da basse tariffe mensili e tenere conto, prima della stipula del contratto, di alcuni fattori al fine di **evitare una costante crescita dei costi durante il ciclo di vita del servizio** e per **mitigare il rischio** legato al passaggio alla nuova soluzione Cloud. È opportuno, quindi, effettuare un'**analisi costi/benefici**, individuando le problematiche più critiche che si manifestano nella migrazione verso il Cloud.
In altre parole, il Cloud fa risparmiare e permette di tenere sotto controllo i costi a patto che si comprendano con precisione le esigenze,comprando servizi con la giusta cognizione di causa.

Questa consapevolezza comincia a farsi strada nel mondo dell'IT, come dimostrato dai tanti studi effettuati su come calcolare i costi del Cloud e dalla nascita di aziende specializzate in questa attività. Particolare attenzione deve essere focalizzata sul fatto che il **modello** di contracting tra Cloud Service Provider e Cliente è ancora **poco maturo e consolidato** le condizioni dei contratti Cloud, spesso standardizzate, **favoriscono il provider** e non sono accettabili per i clienti perché non rispettano i requisiti di compliance, rischio e pricing.

Il grado di impegno garantito dai Cloud Service Providers è spesso **più basso di quello di molti contratti per Servizi IT tradizionali**; capita spesso, infatti, che alcune clausolecritiche per la qualità del servizio (riguardanti ad esempio, i livelli di servizio sulle performance e sull'up-time della soluzione) vengano dettagliate rimandando a link esterni al contratto e, quindi, possano cambiare a discrezione del fornitore, spesso senza alcuna notifica preventiva.

Molti contratti Cloud sono stipulati sotto forma di abbonamento o con la formula "pay as you go", ed offrono in questo modo **limitate garanzie sul rinnovo** e sul fatto che le condizioni rimangano le stesse o migliorino.
Molti **contratti** Cloud sono **standardizzati** in linea con la natura "industrializzata" del servizio che forniscono e questo, per quanto possa sembrare un vantaggio, limita la possibilità di customizzare la soluzione sulla base delle esigenze del cliente.

Di seguito vengono analizzate alcune delle **problematiche più critiche che tipicamente si manifestano negli accordi tra Cloud Service Provider e Cliente**, per poi fornire indicazioni su **possibili soluzioni**:

- ***Costi per i servizi pilota***: la maggior parte dei Cloud Providers offre ai potenziali clienti dei periodi di prova gratuita o ad un prezzo molto basso; le aziende che si apprestano ad acquistare un servizio Cloud devono quindi valutare la presenza di tali condizioni nei contratti e, qualora manchino, cercare di negoziare per ottenere un servizio pilota, al termine del quale valutare se acquistare il servizio Cloud, rinegoziare i termini del contratto in virtù delle esigenze emerse o rinunciare;

- ***Costi di set-up***: in alcuni casi i Cloud Providers richiedono esborsi extra per il set-up della soluzione o per servizi aggiuntivi quali, ad esempio, l'installazione dei database e/o del software, le configurazioni preliminari, la pianificazione dell'importazione dei dati, la conversione dei dati. Tali richieste sono molto spesso ingiustificate perché in un modello Cloud il software dovrebbe già essere installato sulle piattaforme del provider e il caricamento dei dati dovrebbe essere parte del servizio [4]. Le aziende clienti, quindi, pur dovendo tenere conto di inevitabili costi di set-up della soluzione, da pagare, eventualmente, anche a terze parti esterne, devono assicurarsi che almeno tali

servizi siano inclusi nell'offerta;

- ***Costi di customizzazione e di integrazione***: soprattutto per le soluzioni SaaS (ERP, CRM, Office, Desktop,…) esistono necessità di customizzazione che solo in parte possono essere soddisfatte dal Cloud Provider. Molto spesso si ricorre quindi ad applicazioni di terze parti, che richiedono costi per le licenze aggiuntive e che, tra l'altro, non sempre sono integrabili in real-time con la soluzione Cloud; per ragioni di performance, infatti, la quantità di dati trasferibili in real-time dalle applicazioni esterne è limitata in corrispondenza dei picchi di utilizzo del servizio o è soggetta a tariffazione extra. Nella valutazione del servizio Cloud, bisogna quindi considerare cosa esso includa e cosa no, valutando il tutto rispetto ad una soluzione "inhouse", sicuramente più facilmente customizzabile (considerare, ad esempio, eventuali costi aggiuntivi per CR e richieste di intervento che con soluzioni "in-house" sarebbero gratis);

- ***Costi di formazione***: uno dei vantaggi dei modelli Cloud è quello di non avere bisogno di staff di supporto "in-house". D'altra parte, soprattutto per le soluzioni SaaS (ERP, CRM, Office, Desktop,…) i service providers richiedono che i clienti paghino la formazione sulle applicazioni Cloud, almeno per un gruppo ristretto di utenti. Le aziende dovranno, quindi, evitare di accettare clausole in cui la formazione viene fornita con una tariffa ricorrente per tutti gli anni di durata del contratto e richiedere invece di usufruire (e quindi pagare) della formazione solo sulla base delle reali necessità;

- ***Costi aggiuntivi per lo storage***: molto spesso, soprattutto per le applicazioni SaaS, ci sono restrizioni sulla capacità di storage: alcuni providers hanno limitazioni specifiche per utente, altri, invece, garantiscono maggiore flessibilità imponendo un limite massimo per tutti gli utenti; tutti però richiedono premi considerevoli per richieste di spazio aggiuntivo. Le soglie variano molto da fornitore a fornitore (ad esempio per servizi di CRM Cloud la capacità di storage varia in un range che va da 20 MB a 1 GB per utente, per l'e-mail il limite tipico è di 25 GB per mailbox [4]). Per tale motivo le aziende dovrebbero costantemente monitorare l'utilizzo di storage per poter valutare l'eventuale passaggio ad un nuovo fornitore con diverse limitazioni di storage. Inoltre, visto che i dischi fisici hanno un rapido decremento nel prezzo, è consigliabile legare i prezzi pagati per lo storage al costo corrente dello spazio su disco fisico;

- ***Costi di Manutenzione e Supporto***: tutti i Cloud providers forniscono aggiornamenti, miglioramenti e supporto; alcuni includono tali servizi nelle tariffe base, altri li forniscono aggiungendo una percentuale alle stesse. In primis, quindi, le aziende devono assicurarsi che tali servizi siano garantiti come parte della tariffa mensile e che non siano invece offerti a discrezione del fornitore. Inoltre, devono assicurarsi che alcuni indicatori di performance legati al supporto come, ad esempio, il tempo di risposta, il "time to repair" o il numero di contatti consentiti siano chiaramente specificati nel contratto; molto spesso infatti, tali specifiche sono dettagliate rimandando a link esterni al contratto, potendo quindi cambiare a discrezione del fornitore: Per quanto sia garantito che le condizioni on-line non possano cambiare nell'arco della durata del contratto, questo pone il cliente in una condizione di vulnerabilità al momento del rinnovo del contratto. Nella maggior parte dei casi, comunque, il supporto incluso nelle tariffe base non è sufficiente; ad esempio non è consentito

il supporto telefonico, oppure i tempi di risposta sono nell'arco di uno o due giorni, invece che nell'arco di ore; per questo motivo le aziende sono costrette a ricorrere a servizi premium che implicano il pagamento di tariffe aggiuntive che vanno dal 10% al 37,5% delle tariffe base [4]. Le aziende devono quindi chiarire quali diritti siano inclusi nel supporto base e quali siano invece "premium", specificandolo nel contratto. Bisogna fare in modo, inoltre, che gli SLA relativi ai tempi di risposta siano documentati in maniera chiara; se da un lato, infatti, il tempo di risposta garantito in caso di sistema fuori servizio è di circa un'ora, esso aumenta a qualche giorno in caso di problemi di entità minore. Prevedere quindi delle penali economiche per il mancato rispetto degli SLA è una buona pratica da adottare per premunirsi rispetto ad eventuali inefficienze del service provide;

- ***Garanzia di up-time del servizio***: nonostante l'alto livello di criticità di business di alcune applicazioni Cloud (si pensi a soluzioni di CRM o di ERP), in molti contratti mancano del tutto garanzie sui livelli di servizio riguardanti le performance e il tempo di funzionamento (up-time) della soluzione, che sono esplicitate, al più, in link esterni al contratto, potendo pertanto cambiare anch'essi a discrezione del fornitore. In altri casi, invece, alcuni Cloud Providers che calcolano il tempo di non funzionamento (down-time), specificano nel contratto che esso non include il down-time delle WAN, di Internet o delle LAN o dovuto a guasti di terze parti.
  In generale, quindi, è consigliabile stabilire i livelli di servizio relativi alle performance della soluzione Cloud e assicurarsi che siano documentati nel contratto, possibilmente con delle penali a carico del provider se gli standard di performance non sono garantiti;

- ***Penali per gli SLA ed eccezioni***: è importante negoziare penali di tipo economico a carico del provider per il mancato rispetto degli SLA; molti contratti limitano le penali, portando così il cliente, nei casi in cui il servizio non sia rimasto in funzione per un mese intero, a pagare comunque il 50% della tariffa mensile, quando invece, nei tradizionali contratti di outsourcing tale percentuale oscilla tra il 10% e il 20% [5]. Le aziende devono inoltre prestare molta attenzione alle eccezioni al diritto di applicare penali: molti Cloud Providers, ad esempio, conteggiano il tempo di non funzionamento (down-time) solo dopo un certo tempo in cui l'applicazione non funziona (tipicamente dai 5 ai 15 min [5]); bisogna quindi fare in modo che il calcolo del down-time inizi esattamente all'effettivo inizio del down-time. In aggiunta, molto spesso i providers non considerano le interruzioni programmate del servizio nel computo del down-time; è opportuno invece che i clienti richiedano un tempo di notifica delle interruzioni programmate di almeno 24 ore;

- ***Sicurezza, Privacy dei dati e Compliance normativa:*** i temi di Sicurezza, Privacy dei dati e Compliance normativa sono troppo ampi per essere trattati in questo articolo; ci limitiamo a dire che spesso molti contratti Cloud stabiliscono che il cliente è responsabile della sicurezza, della protezione dei dati e della conformità alle leggi locali rappresentando un rischio importante per le aziende, che viene tipicamente mitigato con soluzioni di crittografia dei dati, gestione di audit logs off-line, back-up dei dati. La sicurezza, in particolare, non può essere gestita esclusivamente attraverso meccanismi contrattuali: i clienti dovrebbero accertarsi che le procedure di sicurezza del service provider siano almeno allo stesso livello di quelle applicate in azienda, soprattutto se

la stessa ricade sotto la regolamentazione sulla privacy della Industry di appartenenza o del Paese in cui ha sede;

- ***Business Continuity e Disaster Recovery***: i contratti Cloud raramente contengono disposizioni sul Disaster Recovery ostabiliscono degli obiettivi per il tempo di ripristino quantificati in termini economici; solo in alcuni casi di providers SaaS ciò avviene. In alcuni casi di soluzioni IaaS, inoltre, il service provider non si assume la responsabilità del back-up dei dati del cliente [5]. Tutto ciò sposta i rischi della perdita dei dati tutta sul cliente che, pertanto, dovrà analizzarli considerando l'impatto e la probabilità degli stessi, quantificarli economicamente e pianificare possibili contromisure;

- **Sospensione e interruzione permanente del servizio**: alcuni contratti Cloud stabiliscono che il servizio possa essere interrotto dal Provider se il pagamento è in ritardo di più di 30 giorni. Questo conferisce al provider molto potere di negoziazione nel caso di dispute sul pagamento; bisogna quindi specificare che dispute sui pagamenti giustificate non portano all'interruzione automatica del servizio. Inoltre molti contratti Cloud consentono al provider di interrompere definitivamente l'accordo con il cliente con un preavviso scritto di soli 30 giorni che, in particolare per le soluzioni SaaS e PaaS, non permette di trovare una soluzione alternativa verso la quale migrare il servizio; in tali casi sarebbe opportuno negoziare con il provider un preavviso di almeno 6 mesi per l'interruzione del rapporto a meno di rotture contrattuali;

- ***Responsabilità***: in ambito Cloud sono molto frequenti le perdite di dati del cliente e in molti casi il risarcimento riconosciuto al cliente ammonta ad una cifra massima veramente irrisoria, pari alla somma delle tariffe pagate negli ultimi 12 mesi. È opportuno, quindi, cercare di negoziare condizioni migliori, puntando sul fatto che i providers sono coperti da assicurazioni.

Conclusioni:

Le **problematiche descritte** evidenziano alcuni **difetti strutturali degli attuali contratti Cloud**, **suggerendo** alle aziende che si apprestano ad implementare una soluzione Cloud di **negoziare clausole aggiuntive** con il Cloud Service Provider, oltre che effettuare una dettagliata analisi dei rischi.
D'altra parte, i Cloud Service Providers dovrebbero **correggere questi difetti strutturali** per far sì che i contratti standard siano accettati così come sono ed ottenere, in tal modo, i vantaggi delle economie di scala che ne derivano. Quanto più grande è il contratto in termini di valore, più facile è ottenere delle modifiche alle clausole; in ogni caso, i cambiamenti rispetto allo standard potrebbero essi stessi far crescere sia i costi che i rischi per i clienti.

Le aziende dovrebbero quindi rivedere i loro business-case durante il processo di negoziazione e, **se le condizioni non sono sufficientemente negoziabili**, essere pronte a **rompere l'accordo**. Le aziende devono capire cosa può essere negoziato in base alla valutazione degli elementi di rischio e cosa non dovrebbe essere oggetto di negoziazione.

Nel tempo, la combinazione delle esigenze dei clienti e della volontà dei provider di **abbreviare i cicli di vendita e il numero di customizzazioni**, porterà ad un **maggiore equilibrio tra domanda ed offerta**.

I temi esposti devono essere considerati uno **spunto per ulteriori analisi** più circostanziate e finalizzate a comprendere meglio:

- le **reali esigenze** di acquisto;

- la **maturità** delle soluzioni Cloud disponibili;
- gli aspetti legati al **controllo** e ai **requisiti normativi**;
- i **costi** e i **benefici** associati al modello Cloud che l'azienda sta per scegliere.

Tali analisi risultano fondamentali per comprendere se l'azienda che si appresta ad implementare la soluzione Cloud, sta facendo la scelta giusta e la sta facendo nella maniera corretta, in un **contesto complesso** caratterizzato da una **varietà di servizi e modelli di delivery**, offerti da una **varietà di fornitori**, ognuno con soluzioni diverse e diversi modelli di pricing.

Fonti:

[1] Special Publication 800-145 "The NIST definition of Cloud Computing" - Peter Mell, Timothy Grance - NIST - Settembre 2011
[2] Forecast: "Public Cloud Services, Worldwide and Regions, Industry Sectors, 2009-2014" - Gartner - Giugno 2010
[3] Forecast Analysis: "Software as a Service, Worldwide, 2009-2014, Update" - Gartner - Novembre 2010
[4] IT Procurement Best Practice: "Seven ways to reduce hidden upfront costs of Cloud Contracts" - Alexa Bona, Frank Ridder - Gartner - Febbraio 2011
[5] IT Procurement Best Practice: "Nine contractual terms to reduce risk in Cloud Contracts" - Alexa Bona, Frank Ridder - Gartner - Marzo 2011