

“Cloud computing
per le imprese”

- Premessa pag. 3
- Tipologie di cloud pag. 4
- Utilità per le imprese pag. 5-8
- Vantaggi percepiti pag. 9
- Consigli per il corretto utilizzo del cloud pag. 10 – 12
- Fonti pag. 13

Il cosiddetto “cloud computing” (nuvola informatica), può essere inteso come l’archiviazione, l’elaborazione e l’uso di dati su computer remoti e il relativo accesso via Internet.

In altre parole gli utenti hanno a disposizione una potenza di elaborazione quasi illimitata, non sono tenuti ad investire grandi capitali per soddisfare le proprie esigenze e possono accedere ai loro dati ovunque sia disponibile una connessione Internet.

Grazie all’uso della nuvola informatica, anche le imprese più piccole possono accedere a mercati sempre più grandi, mentre i governi possono rendere i propri servizi più interessanti contenendo i costi.



Private Cloud

La “nuvola privata” è una infrastruttura informatica (rete di computer collegati per offrire servizi) per lo più dedicata alle esigenze di una singola organizzazione, ubicata nei suoi locali o affidata in gestione ad un terzo (nella tradizionale forma dell’hosting dei server), nei confronti del quale il titolare dei dati può esercitare un controllo puntuale. Le “nuvole private” possono essere paragonate ai tradizionali “data center” nei quali, però, sono usati degli accorgimenti tecnologici che permettono di ottimizzare l’utilizzo delle risorse disponibili e di potenziarle agevolmente in caso di necessità.



Public Cloud

Nel caso della “nuvola pubblica”, l’infrastruttura è di proprietà di un fornitore specializzato nell’erogazione di servizi che mette a disposizione di utenti, aziende o amministrazioni i propri sistemi attraverso la condivisione e l’erogazione via Internet di applicazioni informatiche, di capacità elaborativa e di “stoccaggio” dati. La fruizione di tali servizi avviene tramite la rete Internet e implica il trasferimento dei soli dati o anche dell’attività di elaborazione presso i sistemi del fornitore del servizio, il quale assume un ruolo importante in ordine all’efficacia delle misure adottate per garantire la protezione delle informazioni che gli sono state affidate.

Con il cloud pubblico l’utente insieme ai dati, infatti, cede una parte importante del controllo esercitabile su di essi.



Altre “nuvole”

Esistono altri tipi di nuvole con caratteristiche miste, quali i cloud ibridi (hybrid cloud) - caratterizzati da soluzioni che prevedono l’utilizzo di servizi erogati da infrastrutture private.



Riduzione del costo dell'IT







Condivisione delle informazioni e mobilità del personale





Sicurezza del sistema ICT

Il **Cloud computing** consente alle imprese di:

-  ridurre il numero dei server in house,
-  standardizzare e raggruppare le risorse
-  automatizzare molte delle attività di manutenzione attualmente eseguite manualmente.
-  abbattere contemporaneamente le spese di manutenzione delle apparecchiature, quelle per le licenze e l'aggiornamento dei software, per l'immagazzinamento dei dati, per la sicurezza e per l'energia.

La riduzione del costo IT è tanto maggiore:

-  quanto maggiore è l'**incidenza del costo dell'IT relativamente al budget di impresa**
-  quanto più elevata è la **variabilità della produzione nel tempo.**



Secondo il **Cloud Industry Forum** (2011) le soluzioni Cloud sono molto più economiche rispetto alle implementazioni informatiche tradizionali, per la maggiore agilità che essi forniscono alle imprese (Cowen, 2011). L'agilità è misurata dalla capacità di un'architettura ICT flessibile offerta ad un'impresa di operare in modi nuovi e adottare pratiche di lavoro innovative.



In un'economia basata sui servizi ad alto valore aggiunto, la **mobilità del personale** e la **condivisione delle informazioni** non è più soltanto un vantaggio competitivo ma una precondizione per entrare nei mercati più profittevoli.



Il cloud facilita l'**accesso ai dati** e ai programmi in remoto, sempre e da qualunque computer connesso a internet, compresi smartphone e tablet.



Permette di installare più velocemente nuove funzionalità e di integrarle con quelle già esistenti ed erogate via cloud; questo permette di **ridurre i tempi** di programmazione e gestione.

Il fallimento o guasto di una parte del sistema non ha alcun impatto sulla disponibilità delle informazioni e non si traduce in tempi di inattività percepibili.

La resilienza delle imprese si basa su:



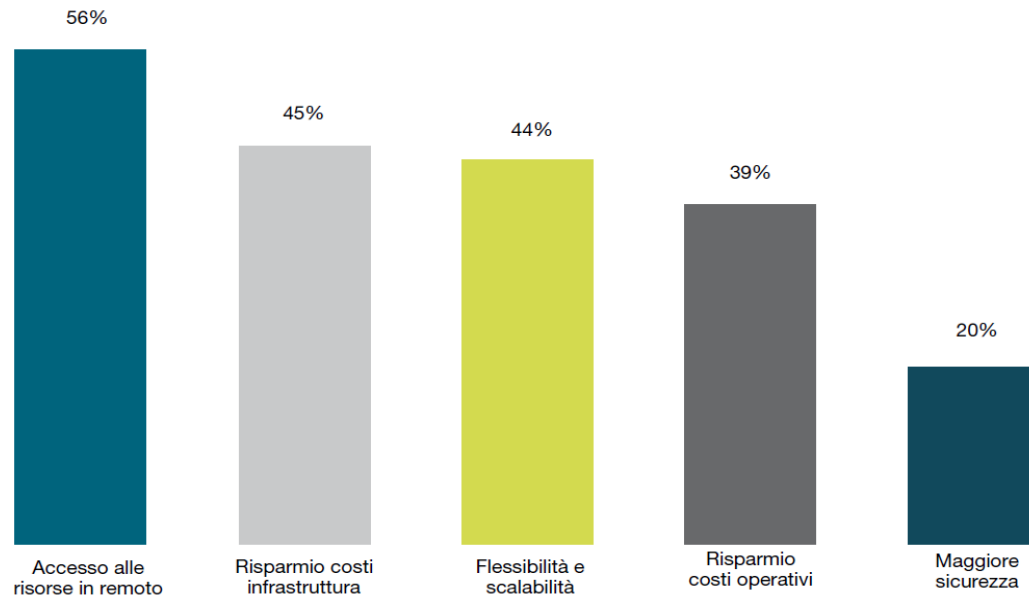
Disaster recovery per i sistemi di IT;



Business continuity per i processi aziendali, le risorse umane e le infrastrutture;

I vantaggi percepiti dalle PMI

Il sondaggio condotto nel 2013 dal blog Enterthecloud.it mostra i vantaggi percepiti da chi* utilizza già sistemi di cloud computing.



Numero rispondenti = 1.000

*Il sondaggio è stato erogato via e-mail ad un bacino di sviluppatori, system administrator, webdesigner, CIO e CTO che lavorano come liberi professionisti, startupper o dipendenti di imprese operanti su tutto il territorio nazionale. Ai target è stato sottoposto un questionario di 15 domande. La raccolta dei dati è avvenuta il 16 gennaio 2013. Le risposte sono state acquisite attraverso la piattaforma Polldaddy e successivamente analizzate. Il campione preso in considerazione per l'analisi dei dati è di 1.000 professionisti IT che hanno correttamente compilato i questionari. La distribuzione geografica dei rispondenti è così suddivisa: Nord (42%), Centro (33%), Sud e Isole (25%).



Ponderare prioritariamente rischi e benefici dei servizi offerti: è opportuno che l'utente verifichi la quantità e la tipologia di dati che intende *esternalizzare*. Tale analisi valutativa dovrà evidenziare l'opportunità o meno di ricorrere a servizi *cloud* (*limitandone l'uso ad esempio a determinati tipi di dati*), nonché l'impatto sull'utente in termini economici e organizzativi, l'indisponibilità, pur se parziale o per periodi limitati, dei dati *esternalizzati* o, peggio, la loro perdita o cancellazione.



Effettuare una verifica in ordine all'affidabilità del fornitore: In funzione della tipologia di servizio che necessitano, oltre che della criticità dei dati, è opportuno che valutino la stabilità societaria del fornitore, le referenze, le garanzie offerte in ordine alla confidenzialità dei dati e alle misure adottate per garantire la continuità operativa a fronte di eventuali e imprevisi malfunzionamenti.



Privilegiare i servizi che favoriscono la portabilità dei dati: E' consigliabile ricorrere a servizi di cloud computing nelle modalità SaaS, PaaS o IaaS in un'ottica lungimirante, vale a dire privilegiando servizi basati su formati e standard aperti, che facilitino la transizione da un sistema cloud ad un altro, anche se gestiti da fornitori diversi.



Assicurarsi la disponibilità dei dati in caso di necessità: Nell'utilizzo dei servizi di cloud computing, in assenza di stringenti vincoli sulla qualità formalizzati attraverso il contratto con il fornitore, si raccomanda di mantenere una copia di quei dati (anche se non personali) dalla cui perdita o indisponibilità potrebbero conseguire danni economici, per l'immagine o in generale relativi alla missione e alle finalità perseguite dall'utente.



Selezionare i dati da inserire nella cloud: Alcune informazioni che si intende inserire per loro intrinseca natura, possono esigere particolari misure di sicurezza. In tali casi, poiché dal relativo inserimento nella *cloud* consegue comunque una attenuazione, seppur parziale, della capacità di controllo esercitabile dall'utente, ed una esposizione di tali informazioni a rischi non sempre prevedibili di potenziale perdita o di accesso non consentito, l'utente medesimo dovrebbe valutare con responsabile attenzione se ricorrere al servizio di cloud computing oppure mantenere in house il trattamento di tali tipi di dati.



Non perdere di vista i dati: E' sempre opportuno che l'utente valuti accuratamente il tipo di servizio offerto anche verificando se i dati rimarranno nella disponibilità fisica dell'operatore proponente, oppure se questi svolga un ruolo di intermediario, ovvero offra un servizio progettato sulla base delle tecnologie messe a disposizione da un operatore terzo.



Informarsi su dove risiederanno, concretamente, i dati: Sapere in quale Stato risiedono fisicamente i server sui quali vengono allocati i dati, è determinante per stabilire la giurisdizione e la legge applicabile nel caso di controversie tra l'utente e il fornitore del servizio. La presenza fisica dei server in uno Stato comporterà per l'autorità giudiziaria nazionale, infatti, la possibilità di dare esecuzione ad ordini di esibizione, di accesso o di sequestro, ove sussistano i presupposti giuridici in base al singolo ordinamento nazionale.



Attenzione alle clausole contrattuali: Una corretta e oculata gestione contrattuale può supportare sia l'utente, sia il fornitore nella definizione delle modalità operative e dei parametri di valutazione del servizio, oltre a individuare i parametri di sicurezza necessari per la tipologia di attività gestita.



Verificare le politiche di persistenza dei dati legate alla loro conservazione: In fase di acquisizione del servizio *cloud* è opportuno approfondire le politiche adottate dal fornitore, che si dovrebbero poter evincere dal contratto, relative ai tempi di persistenza dei dati nella nuvola. Da una parte l'utente dovrebbe accertare il termine ultimo, successivo alla scadenza del contratto, oltre il quale il fornitore cancella definitivamente i dati che gli sono stati affidati. Dall'altra, il fornitore dovrà presentare adeguate garanzie, assicurando che i dati non saranno conservati oltre i suddetti termini o comunque al di fuori di quanto esplicitamente stabilito con l'utente stesso.



Esigere e adottare opportune cautele per tutelare la confidenzialità dei dati: si raccomanda di privilegiare i fornitori che utilizzano a tal fine tecniche di trasmissione sicure, tramite connessioni cifrate (specie quando i dati trattati sono informazioni personali o comunque dati che devono restare riservati), coadiuvate da meccanismi di identificazione dei soggetti autorizzati all'accesso, la cui complessità sia commisurata alla criticità dei dati stessi.



Garante per la protezione dei dati personali



Unione Europea



Commissione Europea: Comunicazione al parlamento europeo (27.9.2012)



“The TechInsights Report 2013: Cloud Succeeds. Now What?”



Astrid – ResPublica



Cloudpeople.it