
Guida al Cloud
Nella Nuvola
la Stella Cometa
per il Manager
seeweb
HIGH QUALITY HOSTING

Marco Rodolfo Alessandro Bozzetti
Sintesi 2012

Marco Rodolfo Alessandro Bozzetti, laureato in ingegneria elettronica al Politecnico di Milano, è amministratore unico di Malabo Srl, società di consulenza sull'ICT (si veda www.malaboadvisoring.it), ed ideatore e curatore di OAI, Osservatorio Attacchi Informatici in Italia, e di EAC, Enterprise Architecture Conference.
Marco ha operato con responsabilità crescenti presso primarie imprese di produzione, quali Olivetti ed Italtel, e di consulenza, quali Arthur Andersen Management Consultant, oltre ad essere stato il primo responsabile dei sistemi informativi a livello "corporate" dell'intero Gruppo ENI.
Fu uno dei primi a livello mondiale ad occuparsi di internetworking, operando attivamente anche presso vari Enti di standardizzazione internazionali e partecipando a progetti di ricerca sia nazionali che europei. Ha maturato significative esperienze nella definizione di strategie sia per la domanda che per l'offerta, nello sviluppo di architetture dei sistemi informatici, nella gestione e nel governo dell'ICT, nella sicurezza ICT, nell'innovazione tramite l'ICT, nella riorganizzazione di strutture e processi, nella gestione della compliance. Tra i risultati delle sue attività particolarmente rilevanti furono per Olivetti l'ideazione e l'implementazione di ONE, Olivetti Network Environment, per l'intero Gruppo ENI dell'enterprise architecture MICEA, per SMAU e per le principali Fiere europee di EITO, European IT Observatory.
È stato Presidente e VicePresidente di FidaInform, di SicurForum in FTI e del ClubTI di Milano, oltre che componente del Consiglio del Terziario Innovativo di Assolombarda.
È attualmente nel Consiglio Direttivo di AIPSI e di FIDAInform, socio fondatore e componente del Comitato Scientifico dell'FTI, socio del ClubTI di Milano, di AIPSI, di itSMF e di Prospera.
È certificato ITIL v3.
Ha pubblicato articoli e libri sull'evoluzione tecnologica, la sicurezza, gli scenari e gli impatti dell'ICT.
Appassionato di alpinismo e sci, pratica anche jogging, vela, sub e golf.

Indice

1. Introduzione

Il presente Rapporto è orientato ai responsabili decisionali nelle Aziende e nelle Pubbliche Amministrazioni, di qualsiasi settore e dimensione, con l'obiettivo di fornire uno strumento veloce e semplice di ausilio per comprendere il fenomeno "cloud computing" e per decidere correttamente in merito nell'ambito della propria Azienda o Ente.
Sul fenomeno cloud molto si è scritto e molto si scrive, tutti i grandi attori del mondo informatico e delle telecomunicazioni offrono servizi in cloud accompagnate da imponenti campagne promozionali, spesso multimediali, tutte molto competitive anche in termini di prezzi: pur in toni e declinazioni diverse, chiaramente emerge che il cloud sta impattando profondamente lo scenario ICT che pur è sempre in continua evoluzione da ormai più di cinquant'anni.
Qualsiasi organizzazione, pubblica o privata, deve essere più efficiente, più efficace, più competitiva, più agile e veloce nel rispondere ai sempre più veloci cambiamenti dei mercati, delle attività, del business. In questo contesto l'informatica, tecnologia abilitante al supporto di tutti i processi e di tutte le attività, diviene una risorsa essenziale e critica: ed il cloud computing porta un modello dirompente, rispetto anche al recente passato, che consente di allineare i costi ed i tempi informatici a quelli richiesti/imposti dall'Azienda/Ente.
Il cloud non è la panacea ad ogni problema, e deve essere adottato contestualizzandolo alle specifiche esigenze e realtà di chi intende usarlo. I decisori, sia livello sistema informativo che al vertice, devono capire che cosa è, quali sono i suoi pro ed i suoi contro, come approcciarlo e contestualizzarlo per avere successo. In tale ottica è articolato il presente Rapporto: nel Capitolo 2 è illustrato, con un taglio più manageriale che tecnico, che cosa è il cloud e quali sono i suoi aspetti tecnici, organizzativi, economici; nel Capitolo 3 si approfondisce a chi, quando e come conviene adottare una soluzione cloud, nel Cap4 si evidenziano i principali attori dell'offerta in Italia; nel Capitolo 5 sono presentati alcuni significativi casi di successo in diversi settori, sia pubblici che privati; nel Capitolo 6 sono descritte linee guida per scegliere e gestire il cloud, frutto anche dell'esperienza in campo dell'autore; il Capitolo 7 chiude il Rapporto con considerazioni sugli aspetti legali, sempre di taglio pratico e manageriale.

2. Che cosa è il cloud computing

La crescente disponibilità di larga banda, unita ad altri fattori innovativi nella continua evoluzione tecnologica, dalla riduzione dei consumi energetici alle moderne tecniche di virtualizzazione, ha ridato vigore a varie forme di terziarizzazione delle risorse informatiche e di telecomunicazione (nel seguito indicate con l'acronimo ICT, Information and Communication Technology), molte delle quali erogate e viste come un servizio, e per questo denominate con il termine finale di "***as a service***", fruibile e pagabile in funzione del consumo, indicato spesso con il termine "***pay per use***".
Il termine di "servizio"sottintende che la risorsa ICT sia erogata e misurata attraverso opportuni indicatori, chiamati in inglese ***KPI***, Key Performance Indicator, concordati a livello contrattuale nell'ambito di clausole sui livelli di servizio richiesti, i così detti Service Level Agreement (***SLA***).

Tipici esempi di KPI includono il tempo di utilizzo di una risorsa, la memoria e le capacità elaborative utilizzate, il tempo di risposta, ecc.
Si è quindi "specializzata" la terziarizzazione di singole risorse ICT erogabili come un servizio (sintetizzabile nell'acronimo XaaS), dalle infrastrutture (reti server, storage, stampanti, ecc.) alle applicazioni, denominando ciascuno come Infrasctructure-Platform-Software as a Service (IaaS, PaaS, SaaS) e/o più in particolare Data storage as a Service (DaaS), Data Base as a Service, Printer as a Service, Network as a Service, Security as a Service, Cloud Identity as a Service (IDaaS) e così via.
Nella stessa logica e con un forte supporto informatico, alcuni fornitori erogano "as a service" anche l'intero processo, denominandolo Business Process as a Service (BPaaS).
La fornitura di tali servizi in maniera più o meno distribuita ***ma attraverso Internet,*** la "nuvola", ha portato alla diffusione del termine ***cloud computing***, grazie anche alle robuste iniezioni promozionali e di marketing di tutti i principali attori dell'offerta.
Come verrà approfondito più avanti, il cloud computing presuppone l'uso della "nuvola" oltre che della scalabilità e della virtualizzazione delle risorse ICT sui sistemi del fornitore (ormai spesso chiamato anche in italiano con il termine inglese di "provider").
Ai termini di cloud computing e di XaaS si affiancano e continuano ad esistere e ad essere usati termini quali "housing", "hosting", ASP, Application Service Provider, ISP, Internet Service Provider. Rientra in tale ambito anche la terziarizzazione della gestione dei servizi ICT, in inglese ***managed services***, che tipicamente è suddivisa nella gestione dei vari componenti: network, server, storage, application, security, posti di lavoro e sistemi mobili, dal PC "lap-top" al tablet e allo smartphone.
Il concetto di acquisire un determinato servizio, pagando per il suo utilizzo, non è affatto nuovo, e da sempre questa è la logica di utilizzo, ad esempio, di mezzi di connessione e comunicazione in rete, dalla telefonia alla trasmissione dati.
Anche la fornitura di applicazioni con accesso telematico ha origini antiche: basti pensare ai servizi tipo Mark III e Geis (venivano chiamati "infoservices") attivi fin dagli anni '60.
La differenza rispetto ad oggi è che allora:

- i collegamenti erano molto lenti, via modem su circuiti dedicati o commutati che al massimo raggiungevano i 9,6 Kbps all'utente finale;
- I processori e le memorie per l'archiviazione erano costose e con capacità limitate.

Oggi le capacità elaborative e di "storage" sono ordini di grandezza superiori rispetto a soli pochi anni fa ed assai meno costose, e, soprattutto, sono sempre più diffusi dispositivi mobili assai potenti (laptop, PDA, smartphone) e la disponibilità di banda trasmissiva abbastanza "larga", dai 2 M bps (bit per secondo) in su, sia wired con xSDL (4-20 Mbps) che wireless (54 Mps): con la fibra ottica si arriva a velocità fino a vari Giga bps. La continua crescita di capacità elaborativa e di memorizzazione si basa sulla miniaturizzazione dei componenti, ora a livello di 20 nanometri, sulla densità di informazione archiviabile per centimetro quadrato, sulle moderne architetture dei componenti e dei circuiti integrati (ad esempio con le CPU "quadcore"); tutte queste tecnologie hanno seguito più o meno la Legge di Moore, raddoppiando densità e capacità ogni 18 mesi circa. Pur con un diverso tasso incrementale,anche le tecnologie di comunicazione continuano ad ampliare la banda disponibile.

Ma la differenza con il passato non è solo tecnologica: alla continua innovazione tecnica si affianca, seppur più lentamente, un cambio di mentalità e di cultura sia per l'utente finale sia per i responsabili dell'ICT, che si sta estrinsecando con un maggior orientamento, anche organizzativo, alla logica di servizio per l'ICT, con la sua sistematica misurazione grazie ai sistemi di monitoraggio, alle SLA, e alla loro terziarizzazione/cloudizzazione.
Il termine cloud computing non ha un'univoca e consolidata definizione, come d'altro canto non le hanno e non le avevano gran parte dei vecchi termini citati sopra, dato il loro uso molto commerciale. Per avere un punto di riferimento che aiuti a meglio comprendere che cosa si intende per cloud e XaaS, nel prossimo paragrafo si fornisce una delle più accreditate definizioni, commentandola.

2.1 La definizione di cloud computing del Nist

Lo statunitense Nist, National Institute of Standards and Technology, ha pubblicato la sua definizione a gennaio 2011 come Special Publication 800-145 - Draft. Tale definizione (nel seguito in corsivo la traduzione dall'inglese) è schematizzata nella fig. 2-1; essa include la maggior parte delle caratteristiche

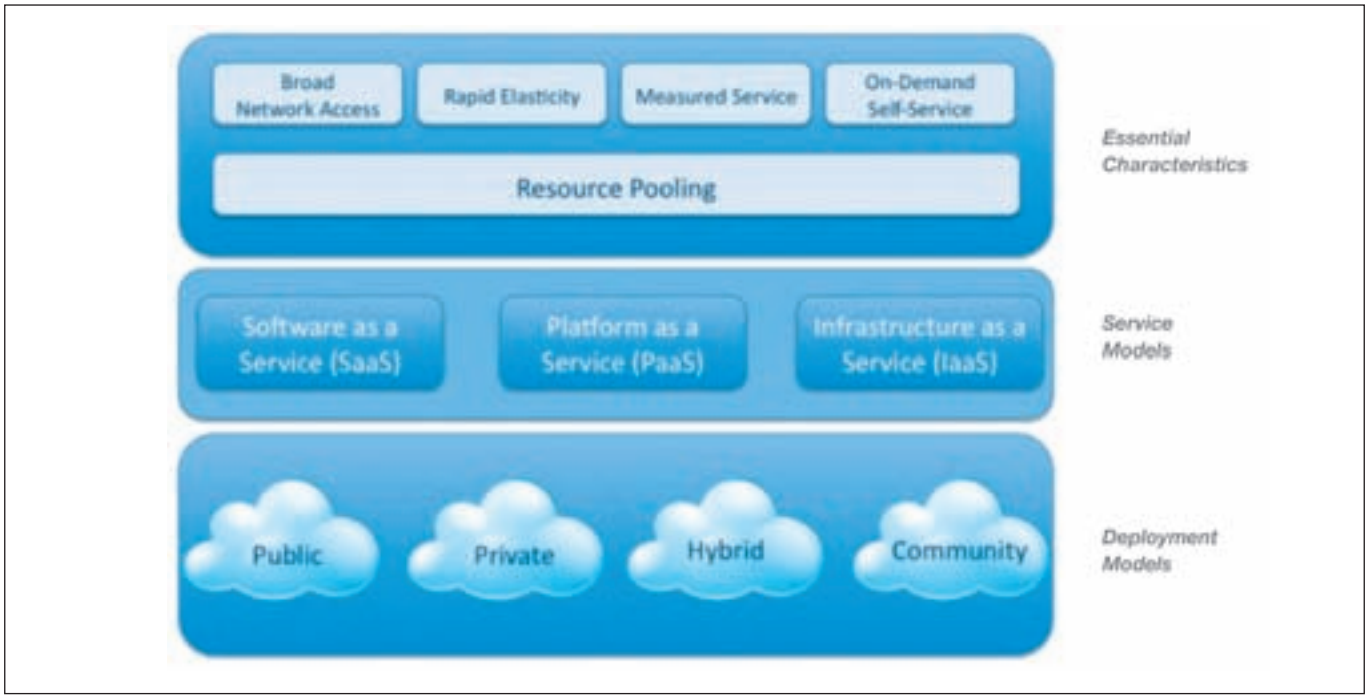


Fig. 2-1 Schema visuale della definizione di cloud computing del Nist (Fonte: Nist)

delle soluzioni proposte dai maggiori fornitori sul mercato, e definisce il Cloud Computing come "*un modello per consentire ovunque (ubiquitous) un accesso su richiesta (on-demand) economicamente conveniente ad un insieme condivisibile di risorse computazionali configurabili (ad esempio: reti, server, storage, applicazioni e servizi) che possano rapidamente essere erogati e rilasciabili da parte di un fornitore con un minimo sforzo per la gestione o l'interazione*".
Questo modello promuove la disponibilità ed è costituito da 5 caratteristiche essenziali, da 3 modelli di servizio e da 4 modelli di distribuzione.

Le caratteristiche essenziali:

- ***Self-service a richiesta*** *(on-demand self-service). Un consumatore deve poter automaticamente e unilateralmente acquisire le necessarie capacità computanzionali, quali il tempo elaborativo su server e lo storge di rete, in maniera automatica e senza dover interagire con il personale (human interaction) del fornitore dei servizi.*
- ***Ampio accesso alla rete****. Le capacità sono disponibili attraverso la rete ed accessibili tramite meccanismi standard che consentono il loro utilizzo da dispositivi-piattaforme client eterogenee di tipo "thin" o "thick"[1] (per esempio cellulari, laptop e PDA).*
- ***Pool di risorse*** *(resource pooling). Le risorse computazionali del fornitore sono raggruppate in un insieme (pool) per poter servire una molteplicità di consumatori usando un modello "multi-tenant"[2], con differenti risorse fisiche e virtuali dinamicamente assegnate e riassegnate secondo le richieste dei consumatori (on-demand). Tale contesto è permeato dalla indipendenza della locazione: in generale il cliente non ha il controllo e la conoscenza dell'esatta locazione delle risorse fornite, ma può essere in grado di specificarla ad un livello di astrazione più elevato (ad esempio di paese,di regione, di data center). Esempi di risorse includono storage, elaboratori, memorie, larghezza di banda e macchine virtuali.*
- ***Rapida elasticità*** *(rapid elasticity). Le capacità richieste possono essere rese disponibili rapidamente e in maniera elastica, ossia adattabile dinamicamente al carico di lavoro, in alcuni casi automaticamente per scalare rapidamente su sistemi distribuiti (scale out), e rapidamente rilasciarle per velocemente ricentralizzarsi (scale in). Al consumatore-cliente le capacità disponibili devono spesso apparire illimitate e possono essere acquistate in qualsiasi momento nelle quantità desiderate.*

---

1 Con il termine thin, magro, si intende un PC con limitate capacità di elaborazione e di storage in locale, che per espletare la maggior parte delle operazioni deve collegarsi in rete tipicamente via browser; spesso è chiamato netPC. Con il termine thick, grasso, si intende il tradizionale PC con elevate capacità di elaborazione e di storage interne, dotato di numerosi software applicativi che può operare sia in rete che non (off line).

2 Si veda § 2.2

- ***Servizi misurati*** *(measured service). I sistemi cloud automaticamente controllano e ottimizzano l'uso delle risorse facendo leva su capacità di misurazione[3] a un livello di astrazione appropriato per il tipo di servizio richiesto (per esempio: storage, processing, larghezza di banda e contabilizzazione degli utenti attivi). L'uso delle risorse può essere monitorato, controllato, riportato per fornire trasparenza sia per il fornitore sia per il consumatore del servizio utilizzato.*

I modelli di servizio:

- ***Cloud Software as a Service (SaaS)****. Le capacità rese al consumatore di utilizzare le applicazioni del fornitore operanti su una infrastruttura cloud. Le applicazioni sono accessibili da diversi dispositivi "client" tramite una interfaccia "thin client" come un web browser (ad esempio per una posta elettronica basata sul web). Il consumatore non gestisce o controlla la sottostante infrastruttura cloud che include reti, server, sistemi operativi, storage, o anche applicazioni individuali, con la possibile eccezione di un limitato gruppo di impostazioni di configurazione per applicazioni specifiche di un certo utente.*
- ***Cloud Platform as a Service (PaaS****). Le capacità rese al consumatore di distribuire sull'infrastruttura cloud applicazioni create dallo stesso consumatore o acquisite, realizzate tramite linguaggi di programmazione e strumenti supportati dal fornitore dell'infrastruttura. Il consumatore non gestisce o controlla la sottostante infrastruttura cloud, che include, server, reti, sistemi operativi, storage, ma ha il controllo sulle applicazioni distribuite e, se possibile, sulle configurazioni dell'ambiente che le ospita.*
- ***Cloud Infrastructure as a Service (IaaS)****. Le capacità rese al consumatore di acquisire risorse computazionali, storage, reti, ed altre fondamentali risorse elaborative dove il consumatore è in grado di installare e attivare software di qualsiasi tipo, che può includere sistemi operativi e applicazioni. Il consumatore non gestisce o controlla la sottostante infrastruttura cloud, ma ha il controllo dei sistemi operativi, dello storage, delle applicazioni installate, e,se possibile, un limitato controllo di alcuni componenti della rete (ad esempio i firewall degli host).*

I modelli di installazione:

- ***Cloud privata****. L' infrastruttura cloud è utilizzata esclusivamente da un'organizzazione. Può essere gestita direttamente dall'organizzazione oppure da uno o più provider specializzati, ed esistere nella sede ("on premise") oppure fuori sede ("off premise").*
- ***Cloud di comunità****. L'infrastruttura cloud è condivisa da più organizzazioni e supporta una comunità di utenti-consumatori che hanno gli stessi interessi (per esempio: la missione, i requisiti di*

[3] Tipicamente tramite un modello di business a consumo (pay per use).

sicurezza, le policy, le considerazioni sulla conformità). Essa può essere gestita dalle organizzazioni o da terzi e può esistere in forma "on premise" o "off premise".

- ***Cloud pubblica**. L'infrastruttura cloud è messa a disposizione del pubblico o di un settore industriale di grandi dimensioni ed è di proprietà di un'organizzazione che vende i servizi cloud.*
- ***Cloud ibrida.** L'infrastruttura cloud è una composizione di due o più modelli di distribuzione (cloud privata, di comunità, pubblica), che rimangono entità uniche ma che sono integrate da tecnologie standard o proprietarie che consentono di effettuare la portabilità delle applicazioni e dei dati (per esempio il cloud bursting, una tecnica per il bilanciamento del carico tra cloud).*

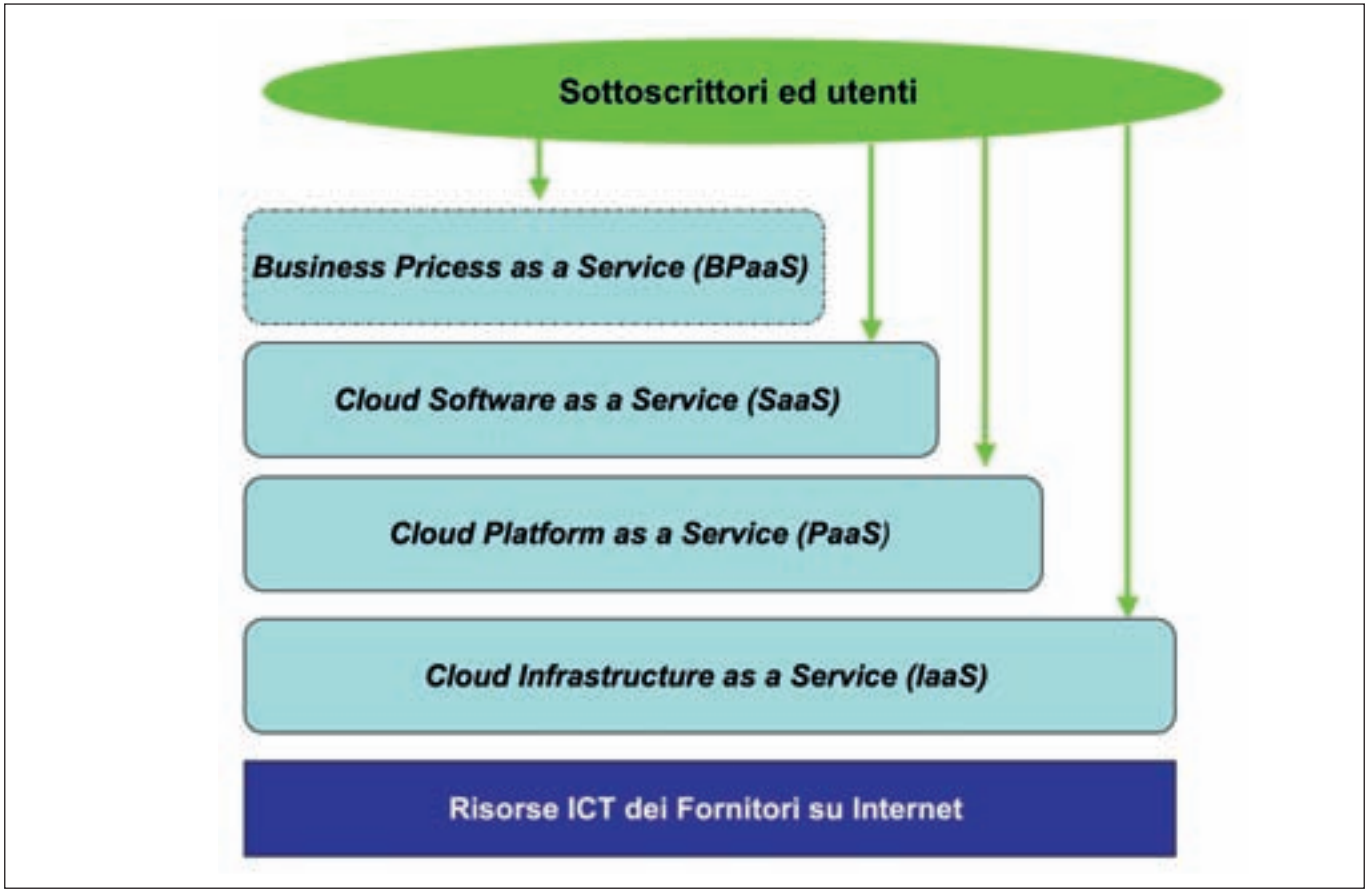


Fig. 2-2 Schema della struttura gerarchico architetturale degli XaaS

Questa definizione del Nist è "una" definizione, non "la" definizione standard e universalmente accettata. E in effetti sui modelli di servizio considera solo i servizi strettamente legati all'ICT, e non la classe di servizi BPaaS, Business Process as a Service, che si posiziona logicamente al di sopra di SaaS (si veda fig. 2-2).

Tipiche declinazioni di XaaS come DaaS o DBaaS, per Data Base e Storage as a Service, oppure Printer as a Service, Network as a Service e così via sono tutte appartenenti alle infrastrutture, e quindi sottoclassi di IaaS.
Tra i modelli di installazione ed erogazione universalmente condivisi, pubblico, privato ed ibrido, NIST ha recentemente inserito anche il cloud di comunità, per evidenziare il ruolo ormai determinante dei social network, che altri considerano come sottoclassi di cloud pubblici o ibridi.
Il termine ibrido, sia nella definizione del NIST sia in tutte le altre, fa riferimento ad un uso misto di cloud privato e di cloud pubblico.
Ma il termine " ibrido " è spesso usato anche per indicare l'uso di cloud applicativo ed infrastrutturale insieme con il Data Center preesistente gestito internamente "on premise". Un esempio di tale uso, assai diffuso, è presentato in §2.2.1.
Un approfondimento sulle caratteristiche dei diversi modelli di installazione, che costituiscono attualmente argomento di acceso dibattito, è riportata in §2.3.

2.2 Gli aspetti tecnici chiave per il cloud

Come già introdotto nei paragrafi precedenti, il cloud computing si basa (o si dovrebbe basare) su moderne tecnologie e logiche architetturali che includono il ritorno alla centralizzazione dei server, l'aumento di capacità elaborativa dei sistemi e dello storage, la riduzione dei consumi energetici per i sistemi, la crescente disponibilità ed aumento della banda nella connessione dei sistemi, l'ampia adozione della SOA, Service Oriented Architecture, e della virtualizzazione, l'adozione di architetture ad alta affidabilità il miglioramento e la più ampia adozione di sistemi di controllo, monitoraggio e misurazione.

2.2.1 Interoperabilità

L'interoperabilità tra ambienti, piattaforme ed applicazioni diverse nel cloud computing e con le soluzioni on premise e/o coi sistemi di altri fornitori comporta la necessità di adottare standard internazionali consolidati, quali Internet con la sua pila di protocolli ed il suo schema di indirizzamento, e i *Web Services* della *SOA*[4].

[4] Per un approfondimento sulle architetture SOA si rimanda al volume dell'autore Marco Bozzetti: "SOA – Il Libro Bianco sull'evoluzione delle Enterprise Architecture", pubblicato da Soiel International agli inizi del 2010.

Il modello SOA costituisce il *framework* di riferimento consolidato ed universalmente accettato per l'interoperabilità tra qualsiasi programma software, indipendentemente dal linguaggio con cui è stato programmato e dall'ambiente nel quale opera. Nella logica di orientamento ai servizi le singole applicazioni non devono essere più intese come la soluzione di problemi specifici e a sé stanti, ma devono essere di fatto parte integrante e integrata di un processo di business.
Nell'ambito Cloud le logiche SOA sono opportune, ma possono essere forniti servizi che non corrispondono a tale frame work standard. Si è infatti diffusa, anche per la sua semplicità e facilità implementativa, l'interfacciamento tra servizi sulla base dei principi architetturali REST[5].

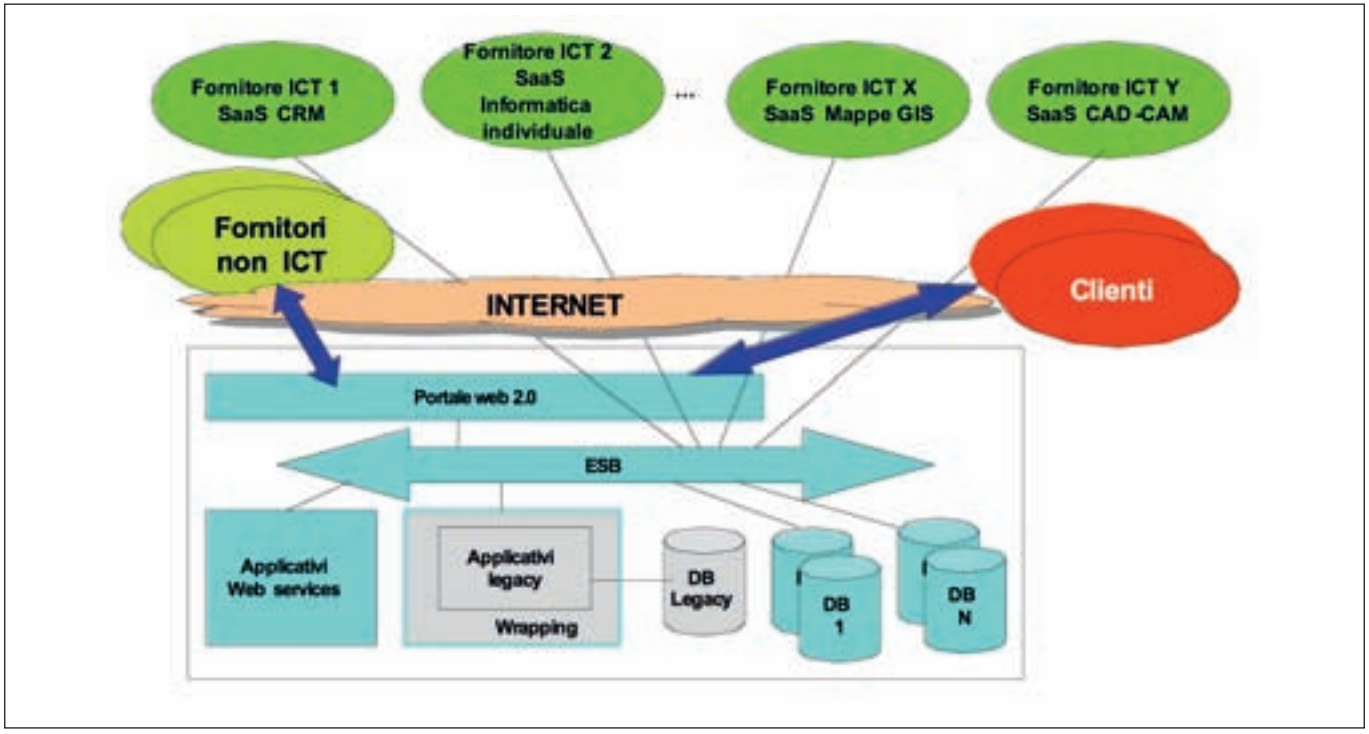


Fig. 2-3 Un esempio semplificato d'uso di "Cloud computing" integrato all'ambiente on premise.

[5] REST, REpresentational State Transfer, è un insieme non standardizzato di principi architetturali ed implementativi software per ambienti ipertestuali distribuiti come i siti web. Esso specifica come le risorse distribuite devono essere definite e indirizzate avendo come base il protocollo HTTP. E' un approccio più semplice e facile rispetto all'ambiente standard SOA per creare web service, ma di contro non standard e quindi con diverse soluzioni in funzione dei vari fornitori-implementatori.

I principali attori dell'offerta forniscono "web services" con protocolli SOA e REST disponibili nell'ambito dei loro ambienti di sviluppo: per il cloud particolarmente significativi sono Amazon AWS, una collezione di web services alla base di Amazon EC2, Elastic Compute Cloud, e di Amazon S3, Simple Storage Service, oltre a CloudStack, open source, per realizzare piattaforme per cloud.

La fig. 2-3 mostra un semplice esempio d'uso di un "cloud computing" integrato con l'ambiente "on premise". Tramite un portale, tipicamente un web 2.0, delle applicazioni SOA locali (in azzurro in figura) con i loro data base (DB 1 .... N in azzurro) interoperano con applicazioni non SOA locali, e relativi data base (in grigio in figura), "wrappati" ed interfacciati tutti ad un ESB[6]; il sistema locale nel suo complesso, via Internet, utilizza applicativi di terzi "on demand", che nella figura, in verde, sono come esempio un CRM, Cad-Cam, mappe per la geo-referenziazione e strumenti di informatica individuale. L'esempio cerca di far capire, almeno intuitivamente, come un'Azienda/Ente possa integrare, via SOA e SaaS, applicativi gestiti direttamente nel proprio sistema informativo con applicativi in SaaS.

2.2.2 Virtualizzazione

La tecnologia alla base del cloud per garantire la condivisione di risorse e la rapida elasticità è la "virtualizzazione". Per ***virtualizzazione*** si intende la creazione di una versione virtuale di una risorsa normalmente fornita fisicamente. Qualunque risorsa hardware o software può essere virtualizzata: server, memoria, spazio disco, sottosistemi, sistemi operativi, programmi applicativi ed anche reti di comunicazione.
Un tipico esempio di virtualizzazione è la divisione di un disco fisso in partizioni logiche.
Esistono varie tecniche e logiche di virtualizzazione, quelle più avanzate permettono la ridefinizione dinamica tanto delle caratteristiche della risorsa virtuale, tanto della sua mappatura sulle risorse reali. Questo consente la riconfigurazione e la migrazione "live" delle risorse ICT coinvolte.
Come per la terziarizzazione, anche il concetto di virtualizzazione non è affatto nuovo, ed affonda le sue radici nelle "macchine virtuali" realizzate sui main frame già dagli anni '60 e '70 del secolo scorso.
Nell'ambito della virtualizzazione si usano logiche "multi-tenant" o "multi-istanze". Il termine ***multi-tenant*** indica che una singola istanza del software, normalmente il sistema operativo o l'applicativo sull'infrastruttura del fornitore, è acceduta ed usata da più clienti contemporaneamente.
Questa logica architetturale si contrappone a quella "***multi-istanza***" dove istanze separate di software (o anche di hardware) vengono attivate per ciascun differente cliente del provider.
Entrambe queste logiche possono essere e sono usate per fornire soluzioni cloud, ma la "multi-tenant" richiede che il software sia progettato ed implementato ad hoc per partizionare virtualmente sia i dati che le configurazioni.

[6] Enterprise Service Bus

Sempre nell'ambito della virtualizzazione per il cloud è crescente l'interesse per quella dei posti di lavoro, indicata generalmente con l'acronimo **DVI**[7], Virtual Desktop Infrastructure (o Interface), che consente di creare su una macchina virtuale centralizzata un ambiente di posti di lavoro, ciascuno con uno specifico sistema operativo e applicativi di informatica individuale, ed indipendenti dalle caratteristiche hardware e software del dispositivo in uso presso l'utente finale. La logica VDI si basa sia sulla virtualizzazione dei sistemi sia sul modello "client-server".
Rispetto al tradizionale modello d'uso, nel quale ogni PC opera in maniera completamente autonoma con il proprio sistema operativo, con le proprie periferiche e stampanti, la virtualizzazione dei dispostivi d'utente fornisce numerosi vantaggi e qualche svantaggio.
L'utilizzo di soluzioni VDI consente una miglior gestione dei posti di lavoro, che viene centralizzata e che facilita quindi i sistematici aggiornamenti del software, l'effettuazione dei back-up, l'eventuale crittazione delle informazioni critiche e riservate, il controllo dei programmi usabili e delle licenze, la possibilità di accedere al proprio dispositivo virtuale da ogni luogo anche se non si ha il proprio dispositivo fisico, la possibilità di usare il proprio dispositivo fisico rispettando le norme dell'azienda/ente. E' l'importante tema della "**consumerizzazione**" e del " **BYOD**, Bring Your Own Device": la possibilità di utilizzare i propri personali dispositivi terminali d'utente, dai lap top ai tablet ed agli smartphone, sia in ambito domestico che professionale, ma garantendo i livelli di sicurezza richiesti dall'azienda/ente; la consumerizzazione inoltre velocizza l'attivazione di nuovi posti di lavoro (provisioning) e di nuovi applicativi, la gestione dei diritti d'accesso e della sicurezza informatica, l'allocazione dinamica dello storage per ogni posto di lavoro virtuale, e, non da ultimo, allunga e potenzia il ciclo di vita dei dispostivi fisici d'utente. Complessivamente garantisce una maggior integrità dei dati trattati ed il poter usare o dispositivi terminali "leggeri" quali i più recenti lap top e i così detti KVM switch[8], oppure vecchi PC ormai obsoleti come "stand alone" che collegandosi possono emulare virtualmente il PC più avanzato.
Gli svantaggi principali includono la necessità di avere una buona connettività, come per ogni servizio in cloud, e talune difficoltà nel gestire specifiche periferiche e stampanti.

Concettualmente le logiche VDI costituiscono l'evoluzione delle tradizionali soluzioni per la gestione dei PC e dei terminali, dai terminal server ai terminal services ed al remote desktop. Attualmente tutti i principali attori dell'offerta a livello mondiale propongono loro soluzioni di VDI, in particolare Citrix, Dell, HP, IBM, Microsoft, Oracle, Red Hat, VMware. Anche i produttori di hardware e di chip hanno realizzato soluzioni per la virtualizzazione di terminali, da Intel ad AMD e Ncompunting.

---

7 Il termine è stato introdotto da VMware, viene talvolta usato anche come "Virtual Desktop Interface", ed è ora largamente usato come riferimento ad ogni soluzione di virtualizzazione dei posti di lavoro

8 I KVM (Keyboard Video, Mouse) switch sono dispositivi intelligenti che interfacciano un monitor, una tastiera, un mouse e con un collegamento ad Internet accedono ad un PC virtualizzato su un server. Realizzano un PC modulare, consentono il riutilizzo di preesistenti monitor, tastiere e mouse e di ridurre di circa 1/4 il costo di acquisizione di un nuovo PC, usando il cloud VDI.

2.2.3 Storage

Un importante aspetto nel cloud, ed in particolare nell'IaaS, è l'archiviazione e la gestione dei dati. Tale specifico servizio è chiamato ***DaaS***, Data Storage as a Service, dove il sottoscrittore paga per lo storage usato o allocato (on demand). L'unità di storage fornita può avere granularità diverse a seconda che si richieda l'allocazione di file, di blocchi o di oggetti.
Per compatibilità con le applicazioni ed i sistemi legacy, questo servizio deve in primo luogo supportare interfacce e protocolli esistenti, quali iSCSI[9] ed altri per strutture a blocchi e CIFS/NFS[10] o WebDAV[11] per i file storage di rete. Possono essere fornite ulteriori funzionalità, quali la compressione, la crittografia e la duplicazione.
La fig. 2-4 schematizza le diverse possibilità di data storage in un cloud.

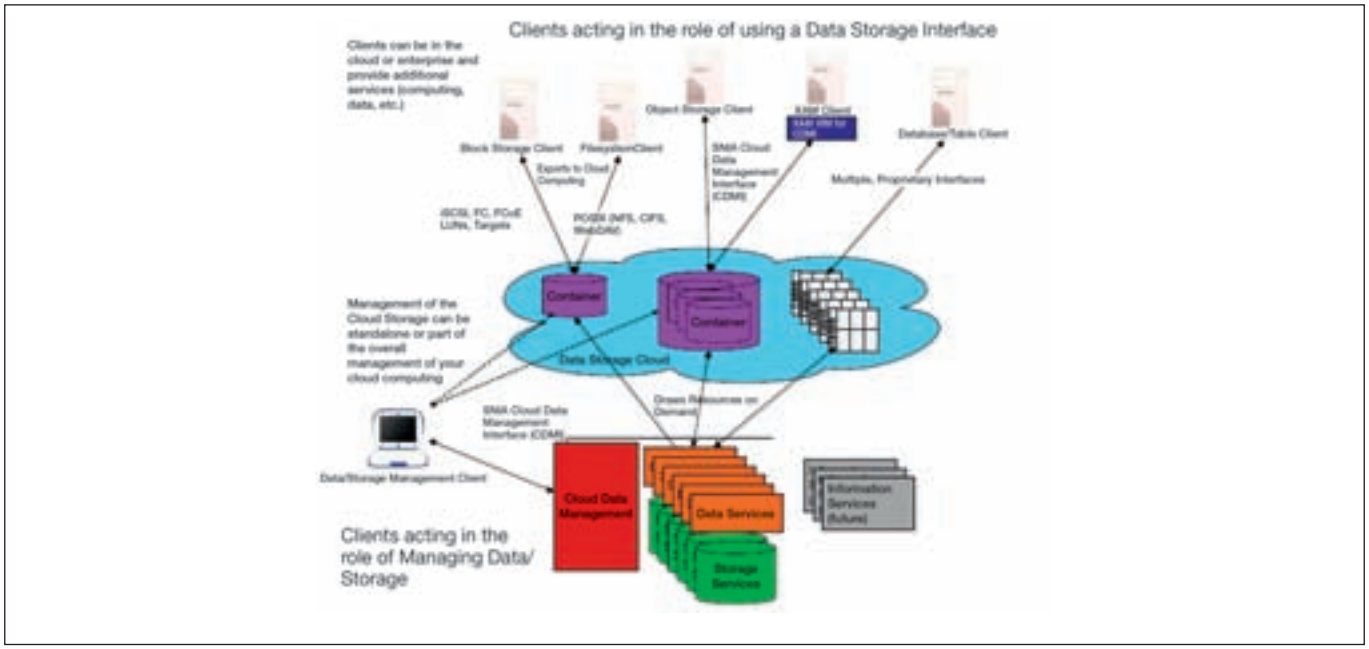


Fig. 2-4 Il modello di riferimento SNIA per le diverse modalità di storage in un cloud (Fonte: SNIA)

9 iSCSI, Internet Small Computer Systems Interface, permette di inviare comandi a dispositivi di memoria SCSI fisicamente collegati a server e/o altri dispositivi remoti (come ad esempio NAS o SAN).

10 CIFS, Common Internet File System, di Microsoft è l'evoluzione dell'SMB, Server Message Block, per consentire in ambito Windows la condivisione in rete di file e di altre risorse. NFS, Network File System, è il file system di rete standard (RFC 1094, 1813 e 3530), usato prevalentemente in ambito Unix e Linux e inizialmente sviluppato da Sun.

11 WebDAV, Web-based Distributed Authoring and Versioning, è un *set* di istruzioni che permette all'utente di gestire in modo collaborativo dei file in un server remoto via http.

Per poter garantire una forte e veloce scalabilità di operazioni tipo database sono state introdotte proprio in ambito cloud tecniche di allocazione di spazi di ***storage a tabelle***. Invece di virtualizzare istanze di un database, queste tecniche offrono una nuova interfaccia, per ora proprietaria, con funzionalità limitate ma con forti capacità per la scalabilità orizzontale. Le tabelle consentono di partizionare facilmente e velocemente lo storage richiesto su diversi nodi della nuvola.
Un terzo tipo di tecnica e di interfaccia sta emergendo in ambito cloud, lo ***storage di oggetti***, indicato anche con il termine inglese di Object Storage. Invece di gestire file, blocchi o tabelle, ogni oggetto contenente dati, chiamato "data object", è accessibile tramite un univoco URI ed il protocollo HTTP. Con il browser è possibile richiamare l'opportuna applicazione che tratterà il dato. Ogni "data object" è trattato come una singola risorsa, che può essere creata, trovata, aggiornata, cancellata (viene usato l'acronimo CRUD, Created, Retrieved, Updated, Deleted). Come mostra la figura, un insieme di "data object" può essere raggruppato in un "container", che a sua volta può essere strutturato in vari modi.

L'accessibilità alla risorsa dato via browser è molto efficace per il trattamento di grandi quantitativi di dati tipicamente non o semi strutturati, quali archivi statici e documentali, file audio/video, e così via.
L'Object Storage non è solo un nuovo modo di concepire lo storage nel cloud, ma fornisce alcune significative caratteristiche, ovviamente variabili a seconda dei fornitori:

- storage ultrascalabile: lo spazio di archiviazione è incrementabile su richiesta, senza necessità di fermo del servizio, dai Giga fino a Peta byte;
- ridondanza completa ad ogni livello; fino a "n" copie, tipicamente 5, per elemento, con possibilità di mettere dei vincoli per imporre che esistano copie su Data Center in specifiche nazioni, per poter garantire la compliance. Tale ridondanza assimilabile ad un Raid tra Data Center consente un Disaster Recovery integrato e in tempo reale;
- "Content Delivery Network" integrata (direct delivery degli oggetti);
- possibilità di accedere al sistema di storage in vari modi:
  - attraverso client specifici tipo FTP, File Transfer Protocol;
  - con un "connector" che ne fornisce una visione convenzionale tipo file system;
  - direttamente da un'applicazioni attraverso un'API specifica (ad esempio quella di Amazon S3);
  - direttamente usando il sistema di Cloud Storage come un servizio di "content delivery" verso il client con HTTP per oggetti statici.

2.2.4. Standard e best practice

Oltre agli standard "classici" della pila Internet e della SOA stanno emergendo specifici standard internazionali sulla virtualizzazione e sull'interoperabilità tra servizi in cloud, oltre che best practice e linee guida internazionali su come scegliere e gestire il/i fornitore/i più adatto/i.

Oltre alle attività di Enti di standardizzazione (de-jure e de-facto) ben noti e consolidati, quali ITU[12], ETSI[13], IEEE[14], IETF[15], Enisa[16], SNIA[17], DMTF[18], NIST, OASIS[19] ed OMG[20], sono attivi anche alcuni specifici consorzi ed associazioni, quali CSA[21], OGF[22], OCC[23].

Gli standard in corso di definizione riguardano prevalentemente le interfacce API, Application Program Interface, sia funzionali che gestionali, e la gestione del cloud, in particolare nelle soluzioni con più fornitori diversi. L'obiettivo di fondo delle varie attività di standardizzazione è di arrivare ad una condivisa, efficace ed efficiente soluzione di ***cloud open***, quindi non soggetta a soluzioni proprietarie con tutti i relativi costi e problemi di licenze, diritti, ecc.

I più interessanti standard già definiti o in corso di completamento includono:

- DMTF **OVF**, Open Virtualization Format: è il formato standard che permette la migrazione tra un ambiente virtuale ed un altro, in modo da evitare il così detto "locked in", ossia l'essere costretti a rimanere con un unico fornitore. OVF è accettato dalla maggior parte dei fornitori per la virtualizzazione ed il cloud, ma la conversione non è, per ora, semplice e facile e non copre funzioni di interoperabilità. Lo si può considerare uno standard ad interim; per i dettagli si rimanda a http://www.dmtf.org/standards/ovf;
- DMTF **CIMI**, Cloud Infrastructure Management Interface, definita dal **CMWG**, Cloud Management Work Group, il gruppo di lavoro del DMTF che ha anche ereditato la gestione e l'evoluzione dei documenti dell'Open Cloud Standards Incubator, struttura sempre di DMTF. CIMI definisce un modello logico per la gestione delle risorse ICT come un "service domain";
- DMTF **CADF,** Cloud Auditing Data Federation Work Group, un altro gruppo DMTF che ha emesso un primo documento di inquadramento sulla federazione tra cloud di fornitori diversi, sia pubblici che ibridi;
- **CDMI**, Cloud Data Management Interface, di SNIA: definisce protocolli ed API per accedere ai dati archiviati in un cloud e per gestirli;

---

12 ITU, International Telecommunication Union, è l'ente di standardizzazione de-jure per le telecomunicazioni a livello mondiale
13 ETSI, European Telecommunications Standards Institute
14 IEEE, Institute of Electrical and Electronic Engineers , è un'associazione che ha emanato e che gestisce innumerevoli standard.
15 IETF, Internet Engineering Task Force, è la comunità aperta per la standardizzazione dei protocolli e delle interfacce di Internet e del mondo web
16 Enisa, European Network and Information Security Agency
17 SNIA, Storage Networking Industry Association
18 DMTF, Distributed Management Task Force
19 OASIS, Organization for the Advancement of Structured Information Standards
20 OMG, The Object Management Group
21 CSA, Cloud Security Alliance
22 OGF, Open Grid Forum
23 OCC, Open Cloud Consortium

- **IEEE P2302**, Draft Standard for Intercloud Interoperability and Federation: l'omonimo Gruppo di Lavoro (GdL) sta lavorando sulla definizione di topologie, funzionalità e governance per l'interoperabilità e la federazione cloud-to-cloud. Per approfondimenti si rimanda a http://grouper.ieee.org/groups/2302/, http://standards.ieee.org/develop/wg/ICWG-2302_WG.html;
- **OASIS** Identity in the Cloud Use CasesVersione 1.0;
- **OASIS TOSCA** Draft 0.2, "Topology and Orchestration Specification for Cloud Applications"**,** Marzo 2012: è focalizzato sulla portabilità di servizi ed applicazioni cloud;
- **OCCI**, Open Cloud Computing Interface, definita dall'omonimo GdL e supportato da OGF: definisce un protocollo e le API per ogni attività di gestione delle infrastrutture cloud da remoto. Si veda http://occi-wg.org/, http://www.ogf.org/gf/group_info/view.php?group=occi-wg.

A livello internazionale negli ultimi anni sono state attivate ulteriori iniziative per il cloud, tendenti a supportare e a promuovere il fenomeno stesso, gli standard emergenti e la sicurezza (per questo tema si rimanda a §2.2.6) soprattutto grazie alla stesura di linee guida ed alla definizione di casi d'uso (use case) di riferimento. Tra queste iniziative è opportuno menzionare:

- **CSA**, Cloud Security Alliance: promuove linee guida e "buone pratiche" per l'utilizzo sicuro dei servizi cloud, di cui alcune sono riportate in §2.2.6;
- **CSCC**, Cloud Standards Customer Council: è un gruppo di patrocinatori per gli utenti finali (end user) con l'obiettivo di accelerare l'adozione di successo del cloud, aiutandoli sugli aspetti della sicurezza, dell'interoperabilità, degli standard, e più in generale della migrazione al cloud;
- **Cloud Cube Model**: Selecting Cloud Formations for Secure Collaboration (**Jericho Forum**): il documento è un "position paper" per aiutare il decisore nella scelta delle soluzioni cloud più adatte alle singole necessità di business, considerando anche gli aspetti della sicurezza;
- **ETSI**, European Telecommunications Standards Institute, ha attivato un Technical Committee (TC) per il Cloud, focalizzandosi in particolare sull'interoperabilità e sulle API standard;
- **Open Data Center Alliance:** un'iniziativa promossa da Intel per consentire lo sviluppo di data center cloud più sicuri, efficienti e semplificati che preservino le caratteristiche di flessibilità e possibilità di scelta dell'IT, con un aumento dell'efficienza e la riduzione dei costi;
- **SAJACC,** Standards Acceleration to Jumpstart Adoption of Cloud Computing, del NIST, per favorire una veloce diffusione ed accettazione degli standard sul cloud. In tale contesto sono stati pubblicati più di 25 casi d'uso con riferimento all'interoperabilità, alla portabilità, alla sicurezza;
- **The Open Group Cloud Work Group**: tra i vari progetti in corso per promuovere e migliorare la comprensione del cloud e dei suoi standard a livello di business, interessante quello per la valutazione della creazione di valore, chiamato "Building Return on Investment from Cloud Computing": alcuni dei concetti di quest'ultimo documento saranno ripresi in §2.5.

2.2.5 Le principali interfacce API proprietarie per il Cloud

Si è già evidenziato in precedenza come le *API, Application Program Interface*, dei servizi cloud siano basilari per permettere l'interoperabilità tra ambienti e tra fornitori diversi. Ma al di là delle attività di

standardizzazione per il cloud sopra evidenziate, oltre agli standard per i web services della SOA alle quali dovrebbero attenersi gli sviluppatori (che per semplicità però spesso preferiscono usare logiche REST che non sono standardizzate), la maggior parte delle API sia funzionali sia gestionali sono "proprietarie", realizzate dai vari provider o anche da progetti di open source, ed utilizzabili da diversi linguaggi ed ambienti di programmazione.
Si deve considerare come ogni ambiente di sviluppo (indicato anche in italiano con l'acronimo SDK, Software Development Kit), ogni Data Base ed ambiente di storage abbiano delle specifiche API; se questi ambienti sono offerti come PaaS o inseriti su IaaS, le relative interfacce sono visibili agli utenti autorizzati, ma non possono essere considerate vere API per il cloud, ma solo "visibili" dal cloud.
La maggior parte delle API specifiche per il cloud servono per costruire e gestire ambienti cloud pubblici e/o privati, sia a livello piattaforme che infrastrutture ed applicativi; altre fanno riferimento a ben noti social net, altre ancora a specifici applicativi in cloud, con i quali integrare ed interoperare con altri applicativi ed ambienti.
La maggior parte delle API cloud sono RESTful, ossia basate sui principi REST prima illustrati. In pratica utilizzano direttamente il protocollo HTTP senza bisogno di utilizzare ulteriori protocolli come il SOAP della SOA.
Le più diffuse e note API proprietarie o open source, ma non standard de jure, includono (elenco non esaustivo):

- Amazon EC2 API http://docs.amazonwebservices.com/AWSEC2/latest/APIReference/ per il cloud di Amazon;
- Apache Libcloud è una libreria Python open per interfacciarsi a diversi fornitori cloud, http://libcloud.apache.org/;
- App42 API specializzato per dispositivi mobili, http://apps.shephertz.com/;
- Daisen Cloud API open in ambito Java, http://dasein-cloud.sourceforge.net/;
- ElasticHosts API (http://www.elastichosts.com/cloud-hosting/api) per il cloud della londinese ElasticHost;
- Facebook API, https://developers.facebook.com/docs/reference/api/, basate su Open Graph (http://ogp.me/);
- FlexiScale API, http://www.flexiant.com/reference/api/, della scozzese Flexiant;
- Flickr API, http://code.flickr.com/;
- Force API di Salesforce.com, http://www.salesforce.com/platform/cloud-infrastructure/integration.jsp;
- GoGrid API, http://www.gogrid.com/cloud-hosting/cloud-api.php, della statunitense GoGrid;
- Google Cloud API nell'ambito del Google App Engine, include anche le interfacce per lo storage, https://developers.google.com/appengine/;
- IBM SmartCloud API http://thoughtsoncloud.com/index.php/2011/09/what-are-the-ibm-smartcloud-enterprise-apis/;
- Jcloud API, http://code.google.com/p/jclouds/;
- Joyent CloudAPI, https://us-west-1.api.joyentcloud.com/docs;

- LinkedIn API, https://developer.linkedin.com/apis;
- NetSuite API, http://www.netsuite.com/portal/developers/main.shtml;
- Windows Azure: è una piattaforma cloud di Microsoft con API e librerie per vari linguaggi supportati e sistemi operativi (Windows, Linux, Mac); fornisce anche degli specifici SDK, http://www.windowsazure.com/en-us/develop/overview/;
- OpenStack Cloud Software, http://openstack.org/;
- Rackspace API, http://www.rackspace.com/cloud/cloud_hosting_products/servers/api/;
- Red Hat Deltacloud, http://deltacloud.apache.org/;
- Simple Cloud API è una proposta congiunta di Zend, GoGrid, IBM, Microsoft, Nirvanix e Rackspace per delle API portabili come codice in grado di interoperare con diversi fornitori di cloud http://simplecloud.org/;
- VMWare vCloud API, proposto anche al DMTF come contributo per la standardizzazione, http://www.vmware.com/pdf/vcd_10_api_guide.pdf;
- Sun Cloud API, http://kenai.com/projects/suncloudapis/pages/Home della Sun-Oracle;
- Twitter API, https://dev.twitter.com/docs.

Il lungo elenco di API e l'approccio non standardizzato RESTful evidenziano i forti pericoli di non interoperabilità e di "lock-in", trattati in §2.2.6 e in §7.
Come illustrato nel paragrafo precedente, per superare queste difficoltà si stanno definendo standard specifici per il cloud (oltre ai web services SOA) che uniformino le modalità di accesso e di azione, ma la strada per un loro consolidamento e diffusione è ancora lunga.

2.2.6. Rischi e sicurezza ICT

La sicurezza ICT nel cloud include tutte le tematiche della sicurezza di un sistema informatico, cui si aggiungono i rischi tipici della terziarizzazione ed alcuni specifici del cloud, in particolare quelli legati alla virtualizzazione ed alla "compliance" a talune normative, come quelle sulla privacy.
Il cloud computing porta alcuni benefici alla sicurezza ICT, che sono per lo più bilanciati dall'insieme di rischi di cui sopra.
A livello di benefici, le misure di sicurezza su larga scala sono più economiche, garantiscono una maggior competenza e specializzazione da parte del personale di supporto, consentono una più forte sicurezza fisica e perimetrale, divengono un elemento di mercato differenziante tra le proposte dei fornitori, consentono una forte e rapida scalabilità on demand delle misure di difesa tale da migliorare la resilienza (capacità di difesa e di ripresa) complessiva del sistema; con il cloud le attività di auditing e di raccolta di prove in caso di attacchi o di incidenti sono assai facilitate, gli aggiornamenti del software sono più tempestivi, efficaci ed efficienti, viene migliorata la gestione del rischio anche grazie alle SLA ed alle azioni di audit.

I principali rischi tipici per il cloud, individuati anche da CSA, Enisa e Nist, riguardano (elenco non esaustivo e non in ordine di gravità):

a) rischi organizzativi e di policy

- ***mancanza di governance***: il sottoscrittore cede il controllo al provider di molti aspetti della sicurezza, difficilmente inquadrabili e controllabili con SLA contrattuali.
- ***lock-in***: difficoltà o impossibilità di passare da un provider ad un altro per la non portabilità delle risorse ICT terziarizzate ed in uso.
- **insicura o incompleta distruzione dei dati:** alla fine del ciclo di vita di un'informazione (o del servizio che la tratta) e/o alla fine dell'erogazione del servizio per scadenza del contratto, l'insieme dei dati oggetto del trattamento terziarizzato, oltre che tutte le informazioni complementari, devono essere totalmente eliminate e non più ricostruibili nella "nuvola".

b) rischi legali

- ***mancata compliance*** alle varie leggi e alle certificazioni già acquisite con il passaggio al cloud se il fornitore non fornisce l'evidenza e la documentazione dell'effettivo rispetto di tutte le normative (richieste anche a livello contrattuale), e non consente verifiche periodiche (audit). Il sottoscrittore deve assicurarsi che il fornitore non trasferisca dati sensibili o comunque critici-riservati su server in nazioni che non hanno le medesime norme in termini di privacy, e che tali dati vengano realmente trattati nelle modalità richieste. Molti articoli, anche su quotidiani a livello nazionale, hanno recentemente commentato alcune considerazioni dell'Autorità Garante della privacy[24], ed erroneamente concluso che il cloud è illegale in termini di privacy, in quanto alcuni fornitori non esplicitano dove sono fisicamente i server e come sono trattati i dati (si pensi ad esempio all'obbligo dei log delle singole attività sui server per un amministratore di sistema). Come anche ben precisato dal Garante della privacy, tutto dipende dalla trasparenza informativa del fornitore, oltre che dal tipo di contratto e di controlli "in profondità" che il sottoscrittore deve prevedere e realmente attuare.
- ***protezione dei dati***: il sottoscrittore non sempre è o può essere a conoscenza delle misure di protezione in essere e di come sono gestite. Il problema è acuito dall'eventuale uso di cloud federati e dallo scambio dei dati tra Data Center in nazioni diverse. Alcuni provider forniscono informazioni su dove e come sono archiviati i dati, come sono gestiti, ed alcuni sono certificati secondo ISO 27000 e SAS70 [25].

c) rischi tecnici

- ***abuso e/o uso malvagio***, soprattutto per IaaS e PaaS. La possibilità da parte di molti fornitori di poter attivare servizi in prova con una limitata identificazione dell'utente, o di venderli dispo-

[24] si veda http://www.garanteprivacy.it/

[25] Statement on Auditing Standards No. 70: Service Organizations, indicata normalmente con l'acronimo SAS 70, è rilasciata dall'Auditing Standards Board dell' AICPA, American Institute of Certified Public Accountants. SAS 70 individua linee guida per gli auditors che operano controlli interni per società di servizi,quindi anche per i fornitori di cloud computing.

nendo solo dei dati di una carta di credito valida, ha consentito a criminali di creare via cloud, con una relativa impunità, attacchi di spamming, di codici maligni, creazione di botnet, DDoS, apertura (cracking) di password e di chiavi, e così via.

- ***API insicure***. Sono le interfacce usate dall'utente per accedere ai servizi del cloud sia a livello funzionale che gestionale, e da loro dipende la sicurezza e la disponibilità del servizio usato. La maggior parte delle API sono proprietarie di ogni fornitore, ed è in corso lo sviluppo di API aperte e sicure come indicato in §2.2.4.
- ***perdita dell'isolamento*** (isolation failure): categoria di rischio che include la caduta dei meccanismi di separazione dello storage, delle memorie, del routing fino alla perdita di reputazione anche tra i diversi clienti del cloud.
- ***malicious insider***: la criticità di un operatore del fornitore di cloud, impreparato, disattento, o peggio con intenzioni criminali, è ben nota o facilmente immaginabile, soprattutto in mancanza di o in limitati controlli sul personale e sulle sue attività da parte del fornitore stesso. Tale criticità è ampliata dalla natura del cloud, distribuito su più Data Center magari in diverse nazioni con diverse leggi e norme, oltre che da gestioni e contratti spesso non trasparenti.
- **condivisione della tecnologia**, soprattutto per IaaS. L'infrastruttura ICT che consente scalabilità e condivisione delle risorse ICT non sempre garantisce proprietà per un forte e sicuro isolamento delle risorse e dei dati di un sottoscrittore dei servizi. Questo potrebbe consentire ad altri sottoscrittori, oltre che a "malicious insider", di poter accedere e manipolare tali risorse.
- **perdita o furto di dati.** Il mondo cloud enfatizza anche questo tipo di rischio, dovuto a carenze negli strumenti di identificazione, autenticazione, controllo degli accessi, oltre che di back-up e di disaster recovery. A tali tradizionali rischi si aggiungono, in mancanza di opportune politiche e di sistematici controlli, la non crittografia di dati in transito tra i vari nodi della nuvola, in primis i Data Center, e la facilità di prelievo con chiavette ed hard disk con interfaccia USB.
- **hijacking** di servizi e/o di account d'utenti sottoscrittori. Il non nuovo termine di "hijacking" sta ad indicare il tipico attacco in rete "dell'uomo in mezzo" tra i due interlocutori, in questo contesto tipicamente tra un utente di un servizio cloud ed il servizio stesso. Il cloud amplia le possibilità di intercettare l'identità digitale di utenti, o di intercettare o origliare attività, transazioni, informazioni, con tutti i rischi conseguenti per l'ignaro sottoscrittore.
- **profilo di rischio sconosciuto**. Il sottoscrittore di servizi cloud non sempre ha una chiara e totale conoscenza delle tecnologie e delle misure di sicurezza in uso, e di come sono gestite. Indipendentemente dal tipo di contratto sottoscritto, dal monitoraggio di SLA e KPI, e da eventuali audit, come può essere sicuro, ad esempio, che tutte le patch per le vulnerabilità siano sistematicamente ed immediatamente installate, che tutti gli antivirus siano aggiornati in tempo reale, che vengano registrati i log degli amministratori ed i tentativi di intrusione, e così via? La terziarizzazione porta ad un maggior numero di rischi ignoti e potenziali, che comunque devono essere considerati e valutati.

La responsabilità nella gestione della sicurezza è suddivisa tra il fornitore, o i più fornitori, e il sottoscrittore, in funzione del tipo di XaaS utilizzato. Da Iaas a SaaS maggiore è la responsabilità del fornitore per la sicurezza, e viceversa, come evidenziato nella fig. 2-5.
Alcuni dei rischi sono trasferibili dal sottoscrittore al fornitore, ma non tutti, e comunque è compito del primo verificare periodicamente che il fornitore attui correttamente tutte le misure di sicurezza necessarie; è quanto specificato anche dallo standard per la gestione della sicurezza ISO/IEC 27002, che nella sezione 6.2 sugli obiettivi di controllo delle terze parti specifica: "*...the security of the organization's information and information processing facilities should not be reduced by the introduction of external party products or services...*".

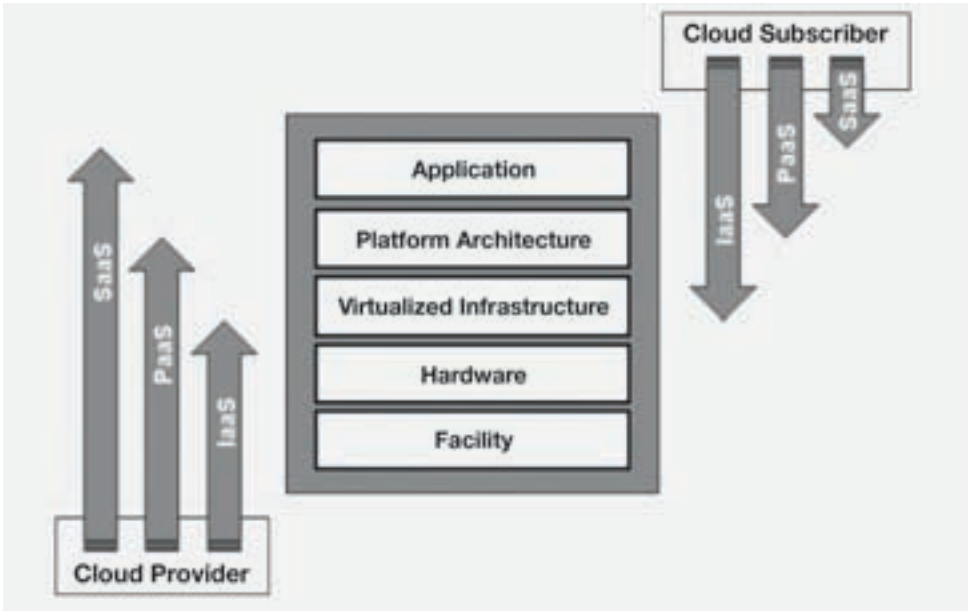


Fig. 2-5 Diversi livelli di responsabilità nel governo e nella sicurezza in funzione dei diversi XaaS

Le misure di sicurezza per una soluzione cloud sono tutte quelle tipiche per un sistema informatico, dalle misure di sicurezza fisica a quelle logiche, dalle misure di prevenzione e protezione a quelle di ripristino, cui si devono aggiungere quelle specifiche per la virtualizzazione.

Facendo riferimento anche alla fig. 2.5, è opportuno sottolineare le possibili differenze tra i livelli di sicurezza forniti a livello applicativo o di infrastruttura, e le relative responsabilità, soprattutto in caso

di soluzioni ibride e di più fornitori coinvolti. Ad esempio se si pone un applicativo "legacy" preesistente su un IaaS, il controllo dei diritti d'accesso all'applicativo è, nella maggior parte dei casi, intrinseco all'applicazione e deve essere gestito "internamente" con gli strumenti disponibili; il provider dell'IaaS che supporta tale applicazione sarà responsabile dell'affidabilità e disponibilità dell'infrastruttura e del controllo degli accessi alla stessa. Al contrario, nel caso d'uso di un applicativo in SaaS, tutte le misure di sicurezza ivi inclusi i controlli degli accessi saranno in carico al provider.
Un aspetto molto importante nella sicurezza dei servizi cloud è l'identificazione dei diversi interlocutori e dei loro diritti di accesso. La Tabella in fig. 2.6, tratta dal documento CSA " Domain 12: Guidance for Identity & Access Management V2.1", sintetizza le principali misure che possono essere applicate, e come, sia per l'identificazione degli utenti che degli amministratori dei servizi cloud.
Per meglio capire la tabella, si riportano nel seguito una legenda degli acronimi usati.

- *ACL*: Access Control List
- *N/A*: non disponibile
- *OAuth*: è un protocollo open standard per le autorizzazioni che consente ad un utente di condividere alcune sue risorse, quali foto, video, elenchi, memorizzate in un sito con un altro sito senza dover scambiare le reciproche credenziali, tipicamente il nome dell'utente e la sua password, per un dato e limitato periodo di tempo, ad esempio 1 o 2 ore. E' stato inizialmente progettato per la delega di autenticazione tra server e provider, ed utilizzato con Twitter. Attualmente il protocollo OAuth v. 1.0 è lo standard Internet RFC 5849, ed è in corso la messa a punto ed il consolidamento della nuova versione 2.0, gia disponibile su Google e Istagram.
- *PAP*, Password Authentication Protocol: è un semplice protocollo di autenticazione che utilizza una password; è usato in Internet dal Point to Point Protocol (PPP), ma trasferendo la password in chiaro sulla rete è considerato totalmente insicuro.
- *RBAC*, Rule Based Access Control: sono liste di controllo degli accessi basate sul ruolo che l'utente ha e può svolgere nell'accedere alle specificate risorse ICT.
- *SAML,* Security Assertion Markup Language: è un open standard OAIS basato su XML per lo scambio di diritti di autenticazione e di accesso. E' usato come standard per il SSO, Single Sign On, ossia l'uso di una sola password iniziale per accedere a diverse risorse ICT.
- *SPML*, Service Provisioning Markup Language: è un open standard OAIS basato su XML per lo scambio di informazioni sugli utenti, sulle risorse e sui servizi di "provisioning" tra organizzazione cooperanti.
- *XACML*, eXtensible Access Control Markup Language: linguaggio per la definizione di policy per il controllo degli accessi.
- XSPA, Cross-Enterprise Security and Privacy Authorization: specifica profili autorizzativi da scambiarsi tra organizzazioni diverse.

Data l'importanza del tema, alcuni degli Enti di standardizzazione e dei Consorzi citati in precedenza hanno emanato delle linee guida per l'analisi e la gestione dei rischi e per la sicurezza per il cloud, in particolare:

	Identity Mgmt Task	Consumer User	Corporate User	Web Service
1	Access Control Model	RBAC, ACL	RBAC, ACL	ACL RBAC if requests on behalf of specific user
2a	Authoritative Source – User Data	The user Local registration or OpenID	The user's organization The user SPML or SAML	Varies depending on type of user and the web service client SPML or SAML
2b	Authoritative Source – Policy Data	The cloud provider	The user's organization The cloud provider SPML or SAML	Information owner The cloud provider SPML or SAML
3	Privacy Policy	The cloud provider Implement locally	The user's organization XSPA profile for XACML	Client organization XSPA profile for XACML
4	Access Control Policy Format	XACML	XACML	XACML
5	Policy Transmission	N/A	SPML or SAML 2.0 profile of XACML	SPML or SAML 2.0 profile of XACML
6	User Profile Transmission	OAuth	SAML assertion OAuth	SAML assertion
7	Policy Decision Request	N/A	XACML, SAML2.0 profile of XACML	XACML, SAML2.0 profile of XACML
8	Policy Decision Enforcement	Do within application Locally specified ACLs for non-corporate entities OAuth to share with other sites	Do within application XACML for policy specification from PAP OAuth to share with other sites	Do within application or externalize to web service gateway product.
9	Audit Logs	Log activity – encrypt with time stamp	Log activity – encrypt with time stamp	Log activity – encrypt with time stamp

Fig. 2.6 Tabella delle principali misure di identificazione ed autenticazione (Fonte: CSA)

- CSA: "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", Dicembre 2009;
- CSA: "Guidance for Identity & Access Management V2.1", Aprile 2010;
- CSA: "TCI, Trusted Cloud Initiative, Reference Architecture Quick Guide", Gennaio 2011;
- CSA:"Cloud Controls Matrix (CCM) v.1.2", Agosto 2011, un frame work per il controllo della sicurezza per fornitori e clienti di cloud;

- Enisa: “Cloud Computing: Benefits, Risks and Recommendations for Information Security”, Novembre 2009;
- Enisa: “Cloud Computing Information Assurance Framework”, Novembre 2009;
- Enisa: “Cloud Computing Risk Assessment”, Novembre 2009;
- NIST Special Publication 800-125, Guide to Security for Full Virtualization Technologies, Gennaio 2011;
- NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing (DRAFT), Gennaio 2011;
- ISO/IEC 27036-IT Security-Security techniques-Information security for supplier relationships (DRAFT).

Da segnalare l’iniziativa di CSA, Cloud Security Alliance, per incoraggiare la chiarezza e la trasparenza nelle misure di sicurezze messe in atto dai fornitori. L’iniziativa, chiamata **STAR**, **Security, Trust & Assurance Registry**, realizza un pubblico e gratuito registro che documenta i controlli di sicurezza forniti dai vari cloud provider. STAR è accessibile liberamente all’indirizzo https://cloudsecurityalliance.org/research/initiatives/star-registry/.
Questo registro costituisce un valido strumento per aiutare nella scelta del fornitore e nel negoziare e definire con lui gli aspetti contrattuali di sicurezza dei servizi offerti.

In § 6 sono riportati suggerimenti operativi e le principali verifiche che un sottoscrittore dovrebbe effettuare per garantirsi il livello di sicurezza voluto. Nell’Allegato è riportato un tipico testo contrattuale sulle caratteristiche della sicurezza ICT che un fornitore dovrebbe specificare. Tale esempio può essere di ausilio e di riferimento da parte del cliente sottoscrittore sia per la scelta tra più offerte di fornitori diversi, sia per negoziare con il possibile fornitore prescelto, o infine per rinegoziare con il fornitore attuale.

2.2.7. Risparmio energetico e green computing

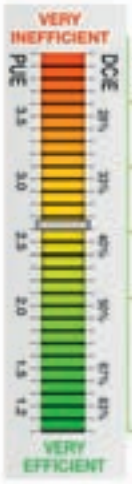
Un aspetto non trascurabile nell’utilizzo di soluzioni cloud è il risparmio energetico ottenibile, ed i conseguenti risparmi sia a livello del sottoscrittore sia più in generale per l’ambiente e la società.
I nuovi componenti integrati a basso consumo, la centralizzazione ed il consolidamento dei server (blade server, virtualizzazione), le nuove tecniche di raffreddamento dei rack, consentono di ridurre drasticamente i consumi sia per l’alimentazione che per il raffreddamento dei sistemi ICT.
Tipicamente la riduzione dei consumi è di un fattore 20, facilitata anche dall’incremento dell’uso delle CPU in ambito cloud (con il multi-tenant) dal 10 al 70% rispetto alle soluzioni “on premise”.
In effetti le architetture a silos nei “tradizionali” Data Center “on premise“ sotto utilizzano fortemente la maggior parte dei server “dedicati”.
E’ più facile, oltre che più conveniente, che sia un provider a sostituire nei propri Data Center server e dispositivi ICT di nuova tecnologia a basso consumo, il così detto “green computing”, dato che con queste riduzioni di consumi può non solo ridurre le sue spese ma anche i prezzi dei servizi ICT offerti.

Per meglio capire e soprattutto misurare l'efficacia e l'efficienza nell'alimentazione di un Data Center sono utilizzati ormai universalmente due indicatori:

- il **PUE**, Power Usage Effectiveness, calcolato come Total Facility Power / IT Equipment Power;
- il **DCiE**, Data Centre infrastructure Efficiency, calcolato come IT Equipment Power / Total Facility Power.

Si consideri che il tipico consumo di un rack (armadio) in un Data Center varia in funzione del numero e del tipo di unità alimentate nel rack stesso, e quindi in media varia tra i 3kW ed i 10kW; un modulo UPS[26] tipicamente consuma 40 kW, un CRAC, Computer Room Air Conditioner, 50 kW, Chiller[27] 220kW.
Un esempio di calcolo dei due indicatori: se il totale degli assorbimenti elettrici è di 100 KW, di cui 40KW per alimentare gli apparati ICT, allora PUE = 2,5 e DCiE 40%.

La fig. 2.7 mostra una Tabella dei livelli di efficienza di un Data Center con i riferimenti a tipici valori di PUE e di DCiE.



PUE	DCiE	Level of Efficiency
3.0	33%	Very Inefficient
2.5	40%	Inefficient
2.0	50%	Average
1.5	67%	Efficient
1.2	83%	Very Eff icient

Fig. 2.7 Scala dei livelli di efficienza con PUE e DCiE (Fonte: The Green Grid)

[26] UPS, Uninterruptible Power Supply, è il sistema di continuità statica che in caso di interruzione della corrente elettrica consente il funzionamento delle apparecchiature ICT, normalmente per una loro corretta chiusura.

[27] E' il termine inglese per indicare un compressore che elimina calore da un liquido (che viene messo sotto pressione); il liquido viene fatto circolare come refrigerante per rinfrescare/raffreddare l'aria o dispositivi.

Un'ultima considerazione "pratica": se i server in un Data Center non sono in media occupati più del 60%, non si può parlare ragionevolmente di Green ICT.

2.3 Cloud pubblico, privato, sociale (community) ed ibrido: cosa è meglio?

In §2.1 sono riportate le definizioni del NIST, ma al di là di queste è ampio ed acceso il dibattito su cosa sia meglio per un'azienda/ente, soprattutto come primo passo nel percorso evolutivo di un sistema informativo verso il cloud.
Nel seguito sono riportate alcune considerazioni dell'autore, frutto della sua esperienza maturata sul campo. Non esiste una soluzione a priori preferibile, non ha senso alcuna battaglia "ideologica": pubblico o privato può essere preferibile a secondo della specifica realtà, in termini di risorse ICT, competenze, cultura ICT, organizzazione, tipo di attività/business, strategia di business e dell'ICT, "commitment" del vertice.
A parere dell'autore il cloud è intrinsecamente pubblico, soprattutto per le piccole e medie imprese. Per le grandi imprese, ed in particolare per le holding e per quelle presenti con proprie società in numerosi paesi del mondo, può essere significativo creare al proprio interno un cloud privato.
Per una grande impresa è meglio partire con un cloud pubblico, magari acquisendo un'applicazione in SaaS, o con un cloud privato, ad esempio razionalizzando una parte della propria infrastruttura ICT in IaaS? Come precedentemente evidenziato, dipende dal contesto dell'azienda/ente e di quale è la "vision" del cloud: in taluni casi può essere più opportuno il primo approccio, in altri il secondo.
Va inoltre crescendo, sempre per le grandi organizzazioni, l'interesse e la preferenza per soluzioni ibride: un mix di servizi con cloud pubblici e privati. Tipicamente viene razionalizzata l'infrastruttura ICT in cloud privato per il supporto e la gestione interna degli applicativi "legacy", mentre alcuni applicativi, ad esempio di salesforce.com e di Microsoft Azure, sono in SaaS su cloud pubblici.
Come spiegato in §2.1, il concetto di ibrido viene anche utilizzato per indicare la gestione combinata di parti del sistema informativo "on premise" e parte in cloud: la coesistenza di questi due ambienti è tipica per gran parte delle aziende/enti che affrontano la migrazione verso il cloud, e soprattutto nelle fasi di start-up, di rodaggio delle soluzioni cloud e/o quando ci sono forti vincoli per la "compliance", in particolare per la privacy.
Leggendo alcuni articoli e blog, anche autorevoli, sembra che il cloud ibrido sia la soluzione preferibile.. Ma attenzione: perché sia possibile integrare e gestire vari cloud diversi, è basilare che tutti siano interfacciabili in maniera omogenea, quindi come minimo che siano basati su SOA o su un RESTful omogeneo. E da §2.2.5 si è visto che questo comporta una non facile selezione tra servizi cloud con API eterogenee.
A giudizio dell'autore solo un cloud pubblico, purché ben gestito, può fornire tutti i vantaggi e le economia di scala evidenziati nei paragrafi precedenti. Il cloud privato è una soluzione per grandissime organizzazioni, tipicamente corporation multinazionali ed holding multi brand, con un sistema informativo esteso all'intero gruppo e gestito da una propria società o divisione specializzata (logica

di “insourcing”); in questo caso l’ICT di Gruppo può considerare di gestire al proprio interno soluzioni di cloud privato per erogare servizi ICT alle sue varie società, con governance complessiva, policy ed i livelli di sicurezza più appropriati per i dati trattati. Solo grandi banche, assicurazioni, società finanziarie, gruppi industriali con decine o centinaia di società, migliaia di dipendenti ed operanti a livello internazionale possono trarre reali vantaggi da cloud privati. La maggior parte delle aziende/enti italiane hanno dimensioni e campi d’azione internazionali ben più limitati, e per questo motivo la più conveniente soluzione per loro è il cloud pubblico. E’ poi evidente che in taluni casi soluzioni di cloud ibrido o di community siano quelle che meglio soddisfano l’esigenza di una azienda/ente.

2.4 Cloud: aspetti organizzativi

L’utilizzo di soluzioni cloud porta ad impatti sull’organizzazione, sui processi e sulle competenze dell’Unità Organizzativa Sistemi Informativi (UOSI), impatti analoghi a quelli della terziarizzazione, completa o parziale, del sistema informativo.
L’impatto cambia a secondo del tipo di servizi acquisiti, dal IaaS al SaaS, e se l’azienda/ente intende gestire ancora talune risorse ICT al proprio interno (on premise).
Qualora anche si terziarizzasse l’intero sistema informativo e la sua gestione, il sottoscrittore, tipicamente la sua UOSI, non deve “perdere” tutte le competenze tecnologiche ICT, soprattutto quelle architetturali e quelle relative alle conoscenze delle esigenze informatiche per i processi di business.
Terziarizzare significa delegare principalmente la gestione operativa dei processi dell’UOSI, gestione che deve essere controllata e verificata non solo da un punto di vista legale-contrattuale ma anche tecnico. Il passaggio di responsabilità e competenze al fornitore favorisce l’orientamento e la trasformazione dell’UOSI all’orientamento ai servizi, ma richiede a quest’ultima un sistematico controllo e supervisione dei processi ICT terziarizzati.
Questi aspetti dovrebbero essere considerati nel contratto e nelle SLA-KPI concordate. Ma è evidente che non possono essere dettagliati tutti i casi possibili, pena un “mostruoso” contratto difficilmente sottoscrivibile: devono sussistere da un lato la disponibilità e la trasparenza del fornitore, dall’altro le competenze e le capacità anche tecniche del sottoscrittore.

Il quadro di riferimento per i processi ICT orientati ai servizi è dato da ITIL[28] v3, utile per definire attività e responsabilità del fornitore rispetto a quelle del sottoscrittore e basato su un modello “demand-delivery” schematizzato nella fig. 2-8 (che riprende i termini ITIL per le fasi dei processi ICT). I principali processi considerati sono elencati nella tabella di fig. 2.9, articolati nelle 5 fasi del ciclo di

[28] The Open Group (http://www.opengroup.org) è un consorzio mondiale impegnato nella definizione e diffusione di standard ICT nell’ottica di “flussi informativi senza frontiere”

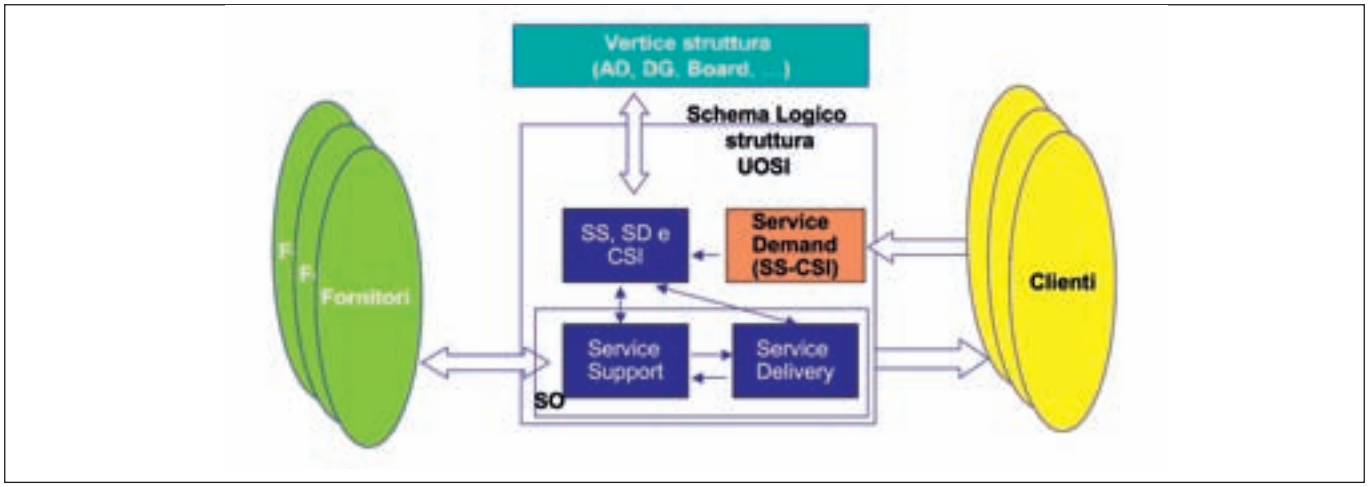


Fig. 2-8 Lo schema concettuale del modello "demand-delivery"

vita di un servizio ICT: la definizione della strategia del servizio ICT (service strategy), il suo progetto (service design), il suo test-controllo e messa in produzione (service transiction), la sua gestione in produzione (service operation), il continuo controllo-supervisione per apportare miglioramenti su tutte le fasi (CSI, Continual Service Improvements).
Dalla tabella in fig. 2-9 si evidenzia come alcuni processi coprano più fasi del ciclo di vita.

In base al modello "demand-delivery", le relazioni tra UOSI e le diverse direzioni-linee di business dell'azienda/ente sono schematizzate nella fig. 2.10. Lato linea di business si sono evidenziate alcune figure/ruoli centrali rispetto ai servizi ICT (visti nelle diverse fasi nella figura lato UOSI), in particolare: il responsabile del/dei processo/i (process owner), gli utenti "chiave" necessari per i test-collaudi, chi segue gli aspetti della sicurezza del processo/i di business (ivi inclusa la sicurezza degli strumenti informatici a supporto del processo), gli utenti finali dei servizi ICT. Nella figura sono evidenziati anche due team (o comitati) misti: l'ERT, Emergency Response Team, per la gestione delle emergenze, ed il CAB, Change Advisory Board, per la gestione delle modifiche all'ICT. Sia CAB che ERT sono previsti in ITIL v3.
L'inserimento del fornitore cloud (o più genericamente di una qualsiasi outsourcer) impatta i vari processi ICT come schematizzato nella fig. 2.11.
Facendo riferimento al modello "demand-delivery" della fig. 2.8, tutti i processi relativi alla parte demand devono essere presidiati e condotti da UOSI, mentre quelli del delivery sono a carico del fornitore: il sottoscrittore deve comunque verificare sistematicamente il livello di servizio erogato e la sua adeguatezza rispetto alle necessità del business.

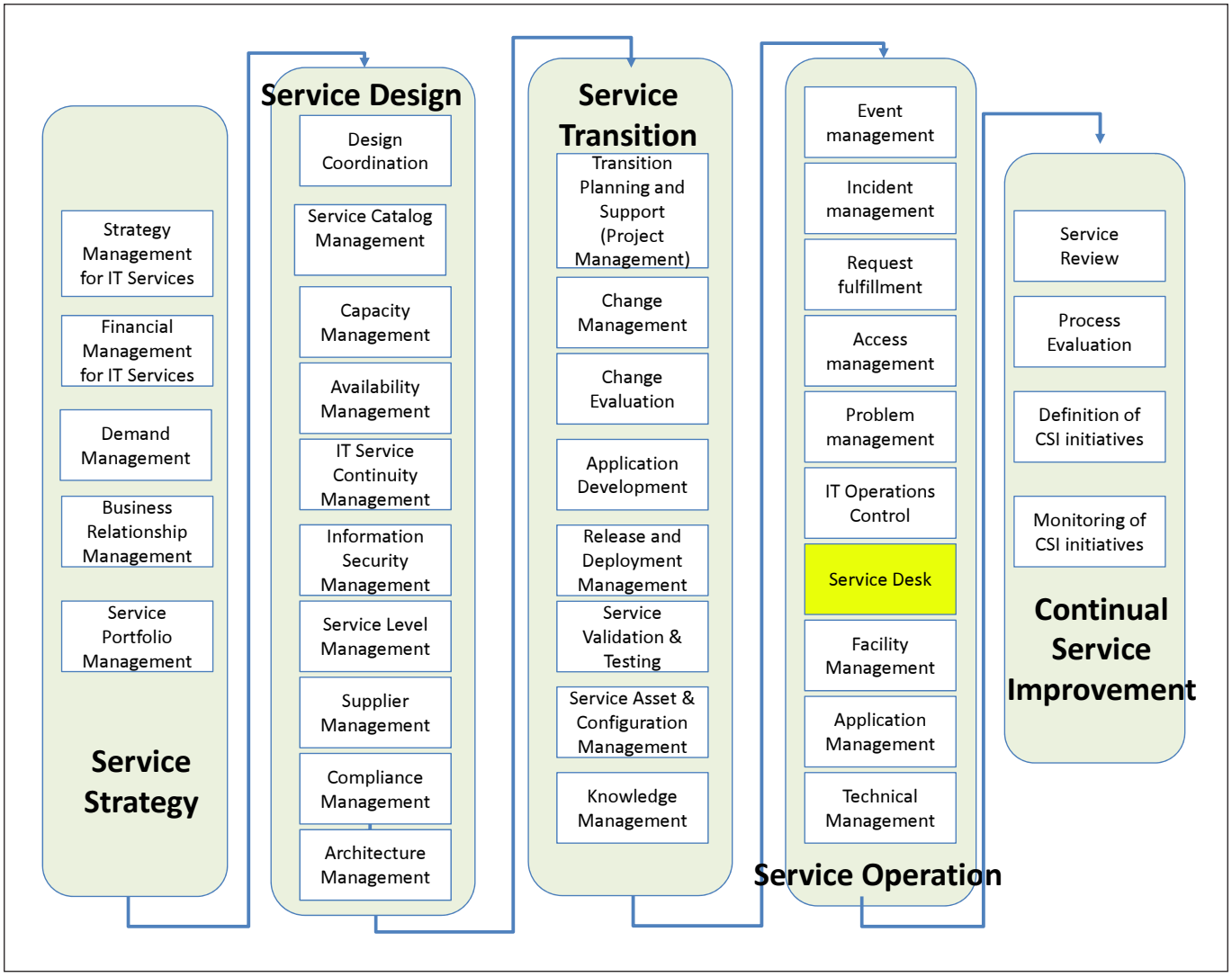


Fig. 2.9 I processi ITIL v3 suddivisi per fasi (Fonte: itSMF)

In particolare l'UOSI si deve focalizzare su una intelligente "governance" dell'ICT nel suo complesso, delegando le attività operative all'operatore ma aumentando il controllo e gestendo le attività più tattiche e strategiche, soprattutto nell'area del demand.

Una buona governance, sia lato fornitore che sottoscrittore, è l'elemento determinante per un effettivo successo dell'adozione del cloud.

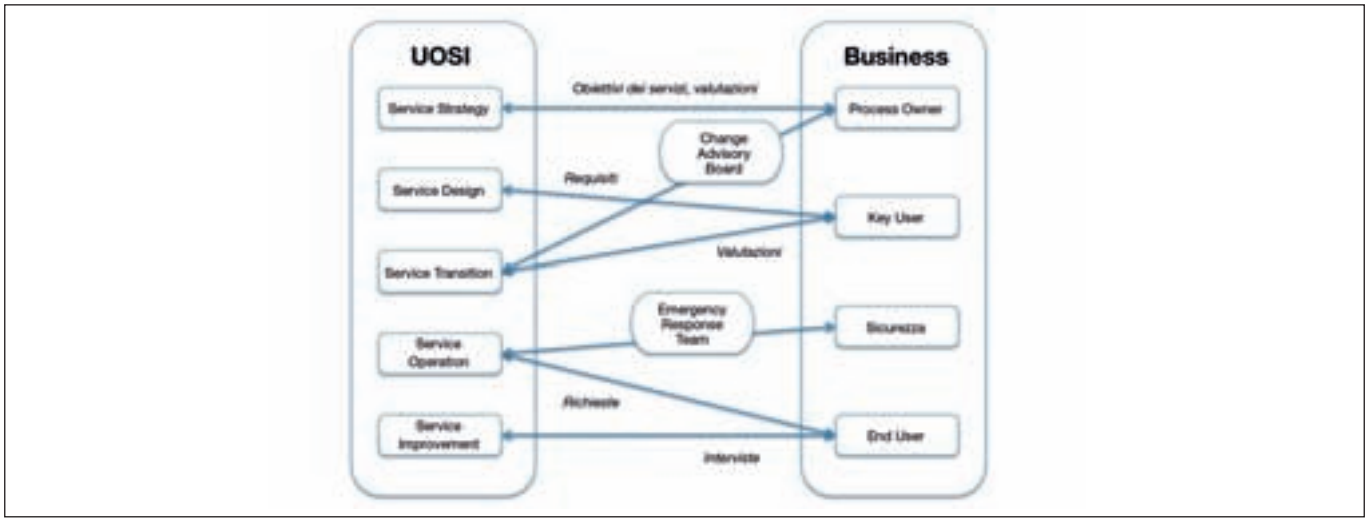


Fig. 2.10 Schema sintetico delle relazioni tra UOSI e le varie Direzioni/Linee di business

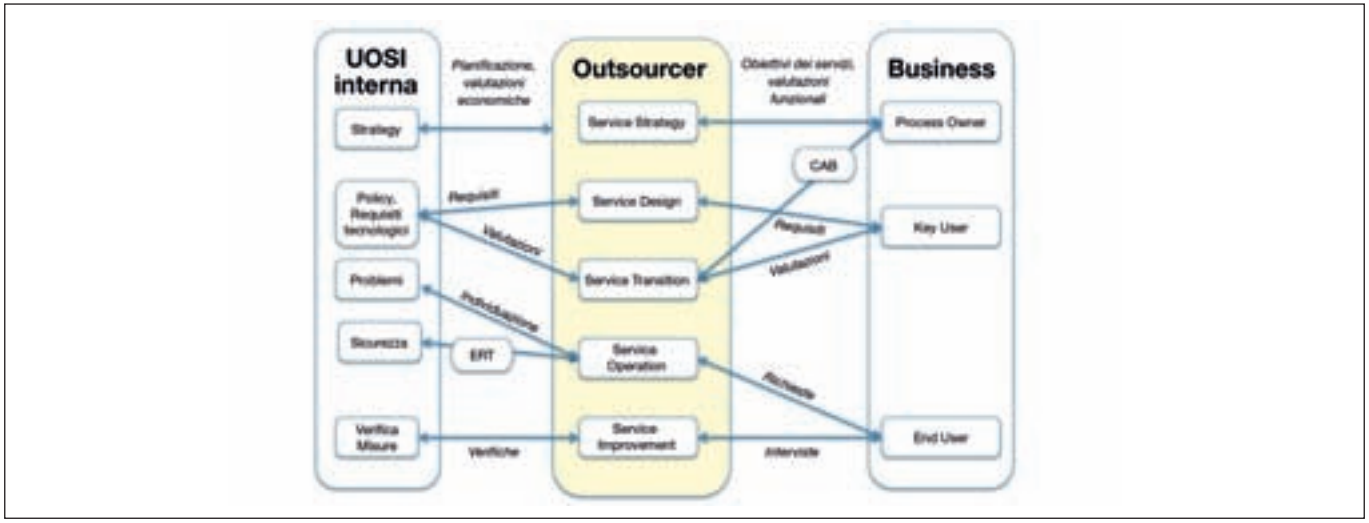


Fig. 2.11 L'impatto sulle relazioni UOSI – Direzione/Linea di business con l'inserimento del fornitore di cloud

Con l'adozione del cloud, lo stesso ruolo dell'UOSI cambia, soprattutto nella scelta degli applicativi; ogni singola direzione e linea di business può autonomamente acquisire in logica SaaS un applicativo da provare per poi eventualmente porlo in produzione, se ha potere e budget per poterlo fare, senza dover condividere decisioni ed aspettare i tempi di rilascio dell'UOSI.
Da una recente analisi del Gartner Group (a livello mondiale) emerge che l'83% delle "business unit" utilizzano servizi cloud senza che la struttura UOSI lo sappia. E' invece compito di quest'ultima definire con **l'ICT Enterprise Architecture** il quadro di riferimento ed il piano regolatore dell'evoluzione del sistema informativo, entro il quale le soluzioni SaaS individuate autonomamente dalle linee di business devono essere compatibili, per poter garantire l'interoperabilità e la consistenza dei dati.
Con il cloud i compiti dell'UOSI e del CIO sicuramente si modificano: e per questo devono considerare ed attuare un'opportuna riconfigurazione di ruoli e di processi.
In tale contesto e all'interno dell'UOSI sta emergendo il ruolo di **Cloud Manager**, con competenze sui processi interni all'azienda/ente, sui servizi cloud offerti, sulle loro SLA e sui relativi contratti: un ruolo che nelle realtà medio-piccole è e sarà probabilmente gestito direttamente dal responsabile UOSI.

2.5 Cloud: aspetti economici

Gli aspetti economici sono il primo e più importante criterio per la scelta di una soluzione cloud.
Con la terziarizzazione di nuove infrastrutture (IaaS), di nuove piattaforme per lo sviluppo (PaaS) o di nuovi applicativi (SaaS) si passa da spese per investimenti (tipicamente di bene durevoli) a spese operative, in termini inglesi ormai usati anche italiano, da CapEX, CAPital EXpenditure[29], a OpEX, OPerating EXpense[30]. Tale passaggio di per sé può non essere significativo, dipende dalle logiche di bilancio e di piano dei conti; ma sempre una spesa è, indipendentemente poi da come venga considerata in contabilità. Nella logica del cloud, la spesa confrontata con quella equivalente se quel bene avesse dovuto essere acquisito "on premise" dovrebbe essere, e nella maggior parte dei casi è, sensibilmente inferiore.
Se si portano in cloud beni ICT già disponibili ed operanti "on premise", ad esempio perché ormai obsoleti, la spesa è tutta di tipo OpEX. In molti casi, se già internamente sono state attuate significative riduzioni dei costi ICT, come spesso avviene in Data Center aziendali, la spesa per il cloud potrebbe essere superiore all'equivalente "on premise", dato che vengono richiesti livelli di servizio ben maggiori di quelli attuabili localmente. Si pensi ad esempio alle competenze del personale del fornitore, alle misure di sicurezza più severe e meglio controllate, al back-up, al disaster recovery.

[29] Sono le spese per capitale per l'acquisto di beni (relativamente) durevoli, come sistemi ICT. Tali spese vengono ammortizzate su più anni e rientrano in bilancio nello stato patrimoniale.
[30] Sono le spese operative necessarie per svolgere le attività tipiche dell'azienda/ente. Tali spese sono inserite in bilancio nel conto economico.

Nel complesso l'adozione di una soluzione cloud, confrontata all'analoga "on premise", dovrebbe portare ad una forte riduzione dei costi, nella maggior parte dei casi tra il 30 ed il 90%, e ad un altrettanto forte risparmio energetico, che si traduce anche in riduzione di costi, come trattato in §2.2.7.

In una situazione come l'attuale, di alto costo del denaro e di elevata tassazione, il passaggio da CapEx a OpEx può essere conveniente, ma occorre sempre ben valutare i flussi di cassa (cash flow) e le modalità di bilancio, e quindi interfacciarsi con il responsabile amministrativo e finanziario, il CFO, Chief Financial Officer.
Occorre soprattutto ben considerare tutti i costi, il TCO, Total Cost of Ownership, e l'arco temporale complessivo nel cui ambito si misurano costi e risparmi/ritorni. Nell'ambito ICT il più delle volte gli effettivi ritorni sono rilevabili e significativi ben oltre il tempo considerato, tipicamente 3-5 anni: è il caso dei sistemi ERP e CRM. Con il cloud i tempi sono generalmente ben più brevi, ma devono comunque essere ben valutati.
Sul mercato si stanno moltiplicando le offerte di servizi cloud, e con prezzi talora molto diversi all'apparenza per il medesimo servizio.
Dato che nessun fornitore, come impresa, può regalare mai nulla, le differenze di prezzo tra una soluzione e l'altra, soprattutto se significative, implicano differenti livelli di servizio, tipicamente in termini di affidabilità e di prestazioni, oppure eventuali offerte promozionali ma dalla durata limitata.
Determinati servizi e la loro disponibilità sono essenziali al funzionamento dell'azienda/ente: risulta quindi evidente che non si può solo considerare il prezzo "minimo" tra le offerte disponibili, che normalmente non garantisce la disponibilità necessaria per un buon funzionamento dei processi di business; occorre considerare la soluzione più conveniente in termini di rapporto tra prezzo e prestazioni-livelli di servizio assicurati.
Come approfondito in §3, l'adozione del cloud non è e non può essere dettata solo dalla riduzione dei costi; la dinamica ed in tempo quasi reale disponibilità di capacità di calcolo e di applicazioni in funzione dei fabbisogni fornisce all'azienda/ente una nuova leva per l'innovazione e la competitività che non può essere non considerata anche come vantaggio economico, in particolare per le PMI.
E comunque la riduzione dei costi è uno dei principali elementi di valutazione: occorre però cercare di valutarlo correttamente e in tempi brevi (l'analisi dei costi e dei ritorni non deve a sua volta comportare un costo significativo).
L'analisi dei costi tra diverse offerte di cloud e la gestione "on premise" deve in primo luogo confrontare parametri omogenei: in altri termini non confrontare patate con carote.
In secondo luogo occorre sempre valutare il rischio del "lock-in", per poter valutare la possibilità di cambiare fornitore e di acquisire in cloud nuovi servizi da altri fornitori: come più volte evidenziato, questo dipende dalle API usate, e se sono basate o no su web services. Il costo del cambiamento in cloud è inferiore rispetto ai cambiamenti in un tradizionale ambiente "on premise", ed è tanto più inferiore quanto più stabili e standardizzati sono i servizi cloud prescelti.
Importante verificare la effettiva scalabilità non solo in crescita, ma anche in riduzione: superati i picchi di utilizzo, si devono poter ridurre le risorse ICT allocate per i picchi, riducendo i costi da sostenere.

La fig. 2.12 confronta su scala temporale i costi legati ai cambiamenti di configurazione e di tecnologie rispetto alla riduzione dei costi tra un ambiente tradizionale “on premise“ ed un ambiente cloud.

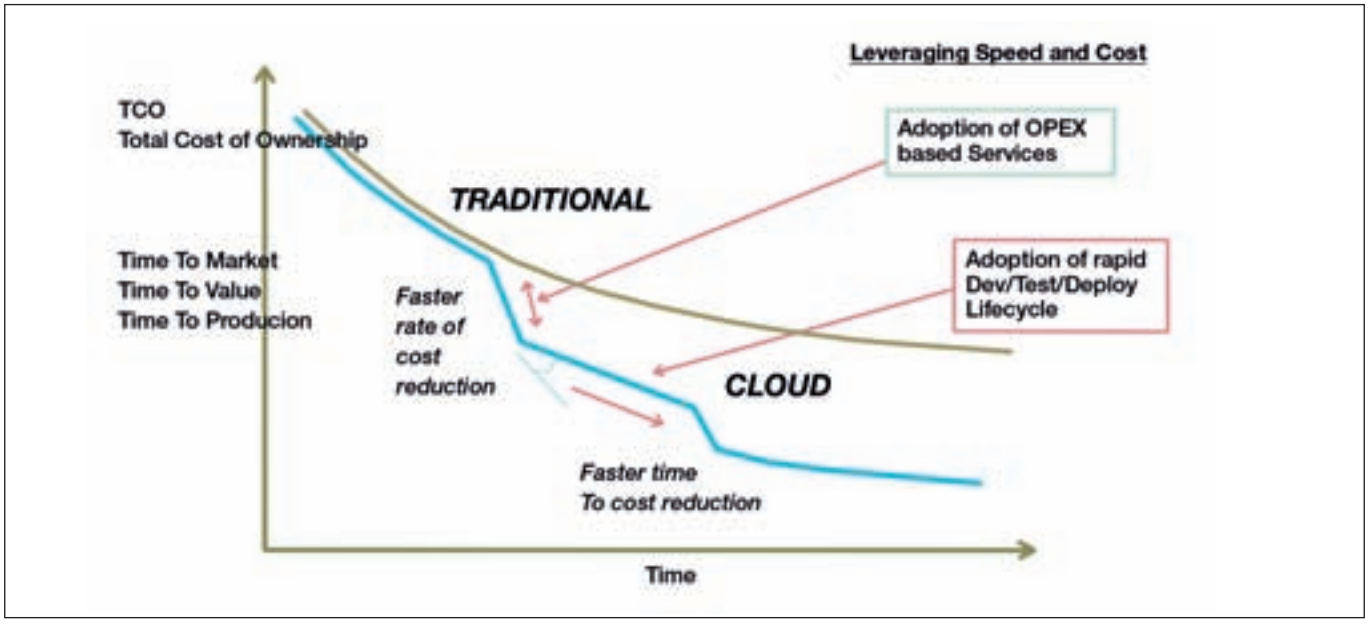


Fig. 2.12 Confronto tra velocità della riduzione dei costi rispetto al costo dei cambiamenti (Fonte: The Open Group)

In un ambito cloud i tempi di progetto, di configurazione e di messa in produzione sono fortemente ridotti:un elemento chiave è l’abilità di scegliere la soluzione cloud che più si avvicina alle proprie esigenze e che più velocemente è configurabile per andare in produzione. L’errore da evitare nel cloud è l’ “over“ o l’“under provisioning“, ossia sovra o sottodimensionare il sistema richiesto.
Oltre alla riduzione dei costi, alla flessibilità ed al miglioramento delle prestazioni, il cloud consente l’immediata attivazione di servizi ICT per provare nuove opportunità e modelli di business oltre a nuovi mercati: tanto che si parla di “pay as yuo go” o “pay as you grow”. E questa è un’opportunità molto significativa soprattutto per le PMI.
Il Cloud Computing ha impatto sui margini grazie alla riduzione dei costi e alle economie di scala, come evidenziato nella fig. 2.13.

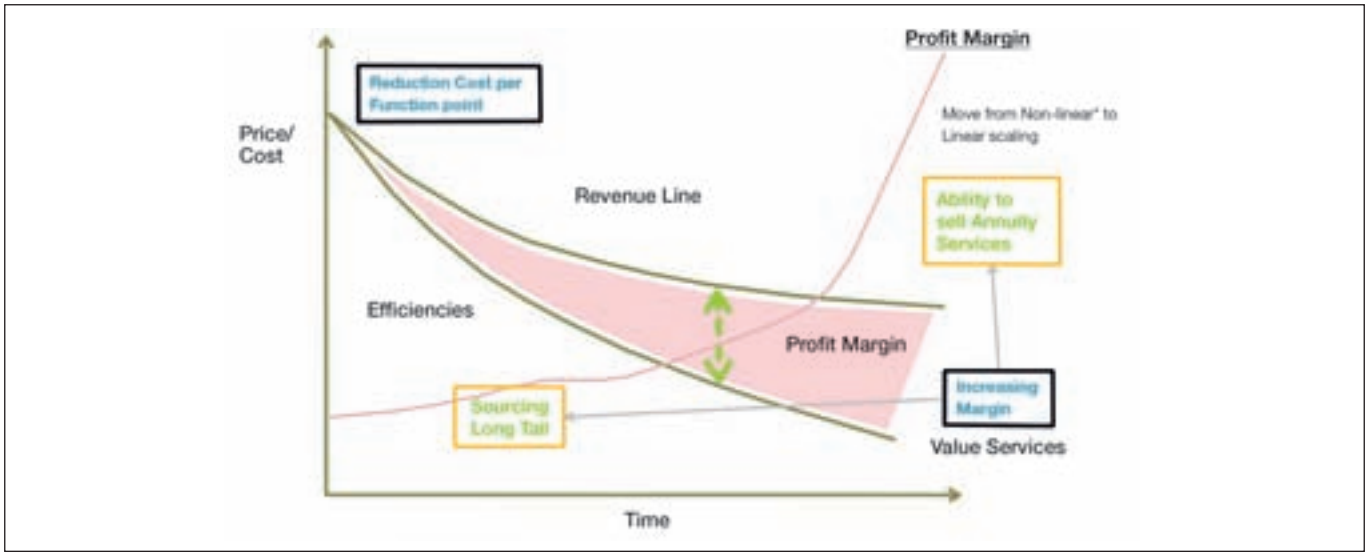


Fig. 2.13 Ottimizzazione dei margini con il cloud (Fonte: The Open Group)

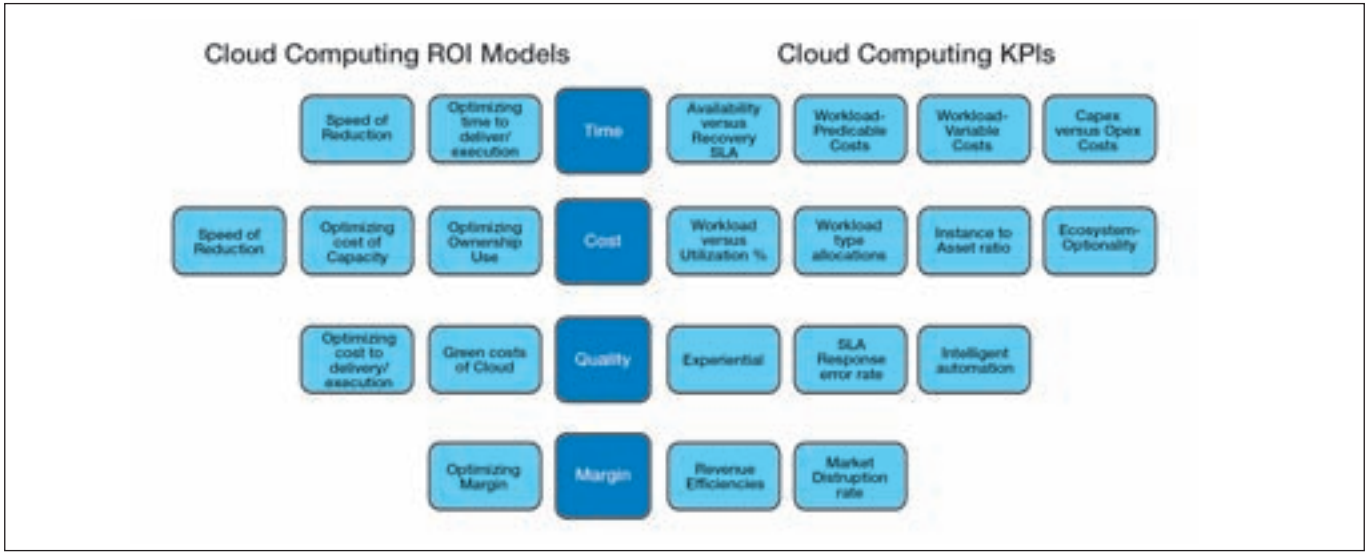


Fig. 2.14 Modello Cloud Computing ROI e KPI (Fonte: The Open Group)

Per la valutazione del ritorno economico nella scelta del cloud, The Open Group[31] ha rilasciato un modello con l'elenco degli indicatori (KPI, Key Performace Indicator), schematizzato in fig. 2.14.

Il modello si articola in due parti:
- la prima fa riferimento ai KPI che confrontano l'adozione del Cloud Computing voluto rispetto alla tradizionale soluzione ICT. La metrica usata considera indicatori relativi alle caratteristiche della soluzione cloud articolati nelle categorie del costo, del tempo, della qualità, del profitto;
- la seconda fa riferimento a logiche di indicatori sul ritorno dell'investimento (Key Return on Investment) per dimostrare il miglioramento in termini di costo, tempo, qualità, compliance, ritorno e profitto rispetto alla tradizionale soluzione ICT.

Esistono vari modelli e metodiche per la valutazione del "valore dell'ICT" per l'organizzazione che lo usa, ma questo del The Open Group è il primo specializzato per il cloud e può essere utilizzato anche in maniera leggera per una valutazione economica sia tra diverse soluzioni/offerte cloud sia per il loro confronto con una soluzione tradizionale "on premise"; gli indicatori specificati sono inoltre utili per richiedere ai fornitori informazioni più dettagliate sui servizi offerti, o per richiedere agli eventuali consulenti (o per selezionarli) di seguire tale metodica.
Per facilitarne l'uso, nel seguito vengono chiariti i vari indicatori della fig. 2.14, articolati per le categorie di costo, tempo, qualità, compliance, ritorno e profitto; per un più facile riscontro con la figura alcuni termini sono lasciati in inglese. Si tenga conto che alcuni degli indicatori fanno riferimento a dati riscontrabili effettivamente solo in esercizio; in caso di analisi di fattibilità pre-progetto e/o pre decisioni, occorre fare delle stime.

A) Cloud Computing KPI
- **indicatori temporali**
  - rado del tempo di risposta del servizio;
  - throughput:
    - la latenza delle transazioni;
    - il volume per unità del tempo di throughput;
    - un indicatore dell'efficienza del carico di lavoro (workload);
  - periodicità:
    - la frequenza delle attività di richiesta e di erogazione;
    - le dimensioni (ampiezza) della richiesta e le relative attività di erogazione per soddisfarle;
  - la frequenza di eventi che richiedono interventi immediati (in tempo reale) ed i relativi risultati.

[31] The Open Group (http://www.opengroup.org) è un consorzio mondiale impegnato nella definizione e diffusione di standard ICT nell'ottica di "flussi informativi senza frontiere"

- **Indicatori di costo**
  - SLA di disponibilità verso recovery (availability vs recovery SLA)**:** indicatori prestazionali della disponibilità confrontati con gli attuali livelli di servizio in produzione;
  - costi fissi per il carico di lavoro (workload predictable costs**):** costo CAPEX della proprietà delle risorse ICT "on premise" rispetto al costo in Cloud;
  - costi variabili per il carico di lavoro (workload – variable costs): costo OPEX della proprietà delle risorse ICT "on premise" rispetto al costo in Cloud;
  - costi CAPEX verso OPEX**:** TCO delle risorse ICT fisiche on-premise verso TCO Cloud;
  - % del workload del cloud verso sua effettiva utilizzazione**;**
  - allocazione dei tipi di workload: dimensione del carico di lavoro rispetto alla distribuzione dei processori e delle memorie; è un indicatore della % degli asset ICT per il carico di lavoro usando il cloud;
  - "instance to asset ratio"**:** indicatore della % e del costo della razionalizzazione/consolidamento delle risorse ICT; è in pratica un indicatore della riduzione del grado di complessità dell'architettura ICT;
  - "ecosystem-optionality": indicatore del numero delle risorse, di API, di servizi a catalogo, di quelli in self service.

- **Indicatori della qualità**
  - "experiential" (soddisfazione nell'uso da parte dell'utenza):
    - la qualità percepita dell'"user experience";
    - la qualità e la facilità d'uso dell'"User Interface" (UI) a livello sia dell'interazione che di come è stata progettata (design);
  - tasso d'errore nelle risposte (anche come indicato nelle SLA);
  - "intelligent automation"**:** livello di automazione delle risposte (ad esempio con uso di agenti).

- **indicatori di profitto**
  - Efficienza dei ritorni economici (revenue efficiencies)**:**
    - capacità di incrementare la generazione di margini/ efficienza del budget per margine;
    - tasso dei ritorni annuale;
  - "Market disruption rate"**:**
    - tasso di crescita dei ritorni
    - tasso di acquisizione di nuovi mercati

B) Cloud ROI Savings Models

- velocità della riduzione dei tempi (speed of time reduction):
  - compressione della riduzione dei tempi grazie all'adozione del Cloud
  - tasso di riduzione del TCO dovuto all'adozione del cloud" (rate of change of TCO reduction by cloud adoption);
- ottimizzazione del tempo per (optimizing time to deliver/execution):

  - incremento nella velocità di provisioning;
  - velocità del multi-sourcing (più fornitori contemporaneamente);
- velocità della riduzione dei costi (speed of cost reduction):
  - compressione della riduzione dei costi grazie all'adozione del Cloud
  - tasso di riduzione del TCO dovuto all'adozione del cloud" (rate of change of TCO reduction by cloud adoption);
- ottimizzazione del costo della capacità (optimizing cost of capacity):
  - allineamento dei costi con l'utilizzo, riduzione costi nell'utilizzo da CAPEX a OPEX grazie all'adozione del Cloud (pay-as-you-go savings from Cloud adoption)
  - miglioramento dei costi grazie alla scalabilità flessibile (elastic scaling)
- ottimizzazione dell'uso della proprietà (optimizing ownership use):
  - Portfolio TCO, riduzione dei costi di licenza grazie all'adozione del Cloud
  - adozione di soluzioni Open Source
  - riutilizzo moduli architetture SOA
- costi "green" del cloud:
  - sostenibilità ambientale;
- ottimizzazione dei tempi di consegna/esecuzione (optimizing time to deliver/execution):
  - incremento della velocità di provisioning;
  - riduzione dei costi della supply chain;
  - velocità del multi-sourcing;
  - rapporto flessibilità/scelta;
- ottimizzazione dei margini (optimizing margin):
  - rapporto incremento nei ritorni/ margine profitto con l'adozione del cloud.

2.6 Cloud: le tendenze del mercato in Italia

In termini di analisi del mercato del cloud computing, è difficile separare questo dal più generico mercato della terziarizzazione, in particolare per l'housing e per l'hosting.
Gli analisti a livello mondiale ed italiano sono tutti concordi nel prevedere una forte e rapida crescita del mercato cloud. Ma questo segmento del mercato ICT, con la sua crescita, è un "divoratore" di altri segmenti ICT: si pensi ai server piccoli e medi "on premise" che tendenzialmente andranno a ridursi drasticamente, così come l'acquisto e le licenze del software, la manutenzione, ecc.
Per quanto riguarda il sottoscrittore, il cloud ha un duplice vantaggio: da un lato una sensibile riduzione dei costi, dall'altro l'opportunità di poter disporre di nuove applicazioni ed infrastrutture "on demand" con un conseguente miglioramento per la competizione e l'innovazione.
Le indagini di mercato sul cloud a livello nazionale ed internazionale sono numerose e, seppur forniscano dati talvolta molto diversi, tutte concordano in elevati tassi di crescita, a due cifre.
Nel seguito vengono ripresi i principali trend a livello mondiale ed italiano, ed approfondendo in particolare i dati per l'Italia.

A livello mondiale

- Secondo ***Gartner Group***: tra 2011-2014 il mercato complessivo del cloud sarà in forte crescita, ma non tutti i segmenti cresceranno allo stresso modo. A livello mondiale:
  - Il PaaS crescerà maggiormente ma rimarrà il più piccolo, da 306 a 998 mln $;
  - IaaS da 4,4 a 12,4 Mldi $;
  - SaaS da 10 a 20 Mldi $.
- Secondo ***IDC***, la spesa mondiale per servizi in cloud arriverà nel 2012 a 42 Mldi $.
- Per ***Wintergreen Research***, il mercato mondiale del cloud passerà dai 36 Mldi $ del 2008 ai 160,2 Mldi $ del 2015.
- **Nextvalue-CIOnet** Rapporto 2011: da $ 30,1 Mldi nel 2010 a 60,6 Mldi nel 2013.

A livello italiano

- ***Assinform*** (Netconsulting):
  - Cloud computing: 130 mln di euro nel 2010, previsione 2013: 410 mlni;
  - la dinamica dei grandi server (Sistemi High End), la cui domanda è cresciuta del 18,4% nel 2010 rispetto al 2009, è uno degli indicatori del potenziamento e della razionalizzazione dei grandi Data Center, tipicamente dei fornitori dei cloud.

- ***Assintel*** (NextValue):
  - il cloud rappresenterà è un giro d'affari da 660 milioni di euro entro due anni, ossia nel 2013.

- ***Nextvalue-CIOnet*** Rapporto 2011
  - spesa cloud in Italia da € 280 Mlni nel 2010 a € 660 Mlni nel 2013;
  - a livello europeo il decisore è nel 66% dei casi il Responsabile ICT (CIO), nel 34% dei casi il responsabile del business, a livello italiano l'85% ed il 15%;
  - a livello italiano, nei prossimi 3 anni il modello di riferimento considerato è ibrido per il 51%, privato per il 31%, pubblico per il 5%, community per il 6% (non lo sa per il 7%).

- ***Osservatorio MIP*** 2012 sul cloud: la fig. 2.15 riassume l'analisi del mercato del cloud in Italia, evidenziando la bassa spesa per le medie-piccole organizzazioni;
  - complessivamente nell'anno 2012 la spesa per il cloud è stimata in € 443 mlni, di cui € 240 mlni per il cloud privato;
  - per le PMI la spesa è stimata in solo €18 mlni, con una leggera prevalenza di soluzioni di private cloud.

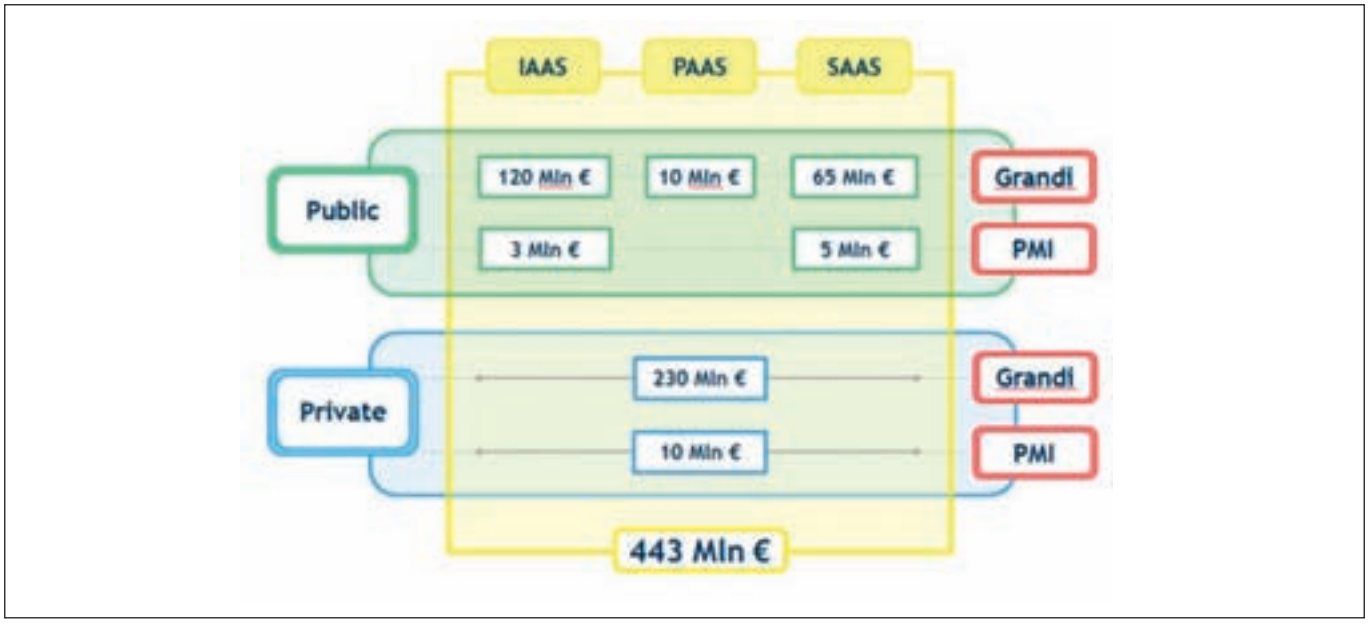


Fig. 2.15 La spesa per il cloud computing in Italia nel 2012 (Fonte: MIP)

Considerando altre indagini, e sempre a scopo puramente indicativo, per l'Italia si ha uno stato dell'arte riassumibile nei seguenti punti:

- sei su dieci delle grandi aziende hanno in cantiere progetti di cloud computing;
- sei PMI italiane su dieci hanno trasferito nella "nuvola" informatica le risorse di storage e le applicazioni per gestire la posta elettronica;
- il 69% hanno trasportato nella "nuvola" una parte dell'infrastruttura e delle applicazioni che erano già virtualizzate;
- Il 27% hanno spostato in cloud il desktop computing (informatica individuale).

Facendo riferimento ai dati elaborati dal MIP, la spesa in cloud computing in Italia nel 2012 è di 443 milioni di euro, in crescita del 25% rispetto al 2011, ma che rappresenta solo il 2,5% della spesa IT totale: questo dato indica il ritardo italiano, poiché tale percentuale in molti altri Paesi europei è più alta e negli Usa è già oltre il 5%".

Tale indagine evidenzia come in Italia prevalga il private rispetto al public cloud, con un 54% e soprattutto che il 95% della spesa cloud proviene da grandi aziende ed enti.

Per le piccole e medie imprese i (PMI) la stessa indagine fotografa un quadro abbastanza preoccupante, schematizzato dalla fig. 2.16.

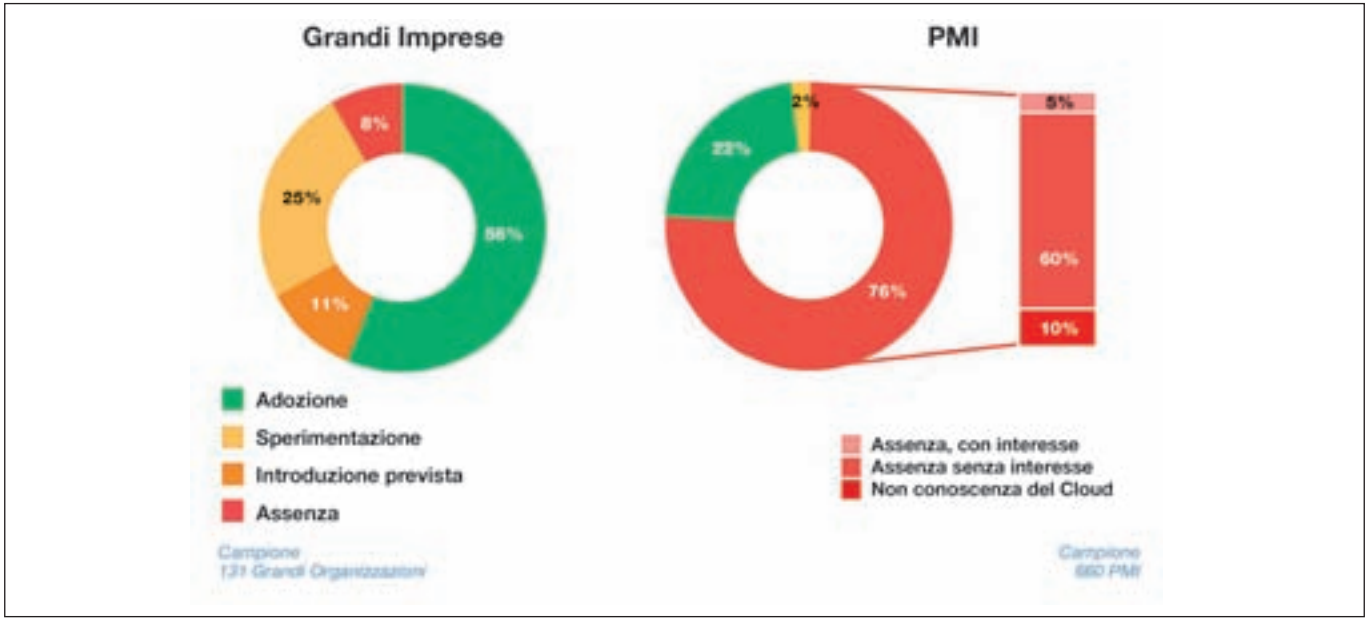


Fig. 2.16 L'adozione del cloud al 2012 tra grandi imprese e PMI (Fonte: MIP)

Dalla figura emerge che solo il il 22% del campione ha avviato progetti cloud, l'8% intende introdurli, ma il 60% dichiara di non avere alcun interesse e il 10% addirittura non sa cosa sia il cloud computing.
Il problema riguarda in primo luogo la mancanza di larga banda, poi il canale di vendita dell'offerta ed infine, ultimo ma non ultimo, la scarsa cultura informatica (in media) delle PMI.
Per le PMI e le PAL, Pubbliche Amministrazioni Locali, che operano distanti dalle grandi città esistono spesso seri problemi di connettività: in molti casi non sono disponibili nemmeno connessioni xDSL, e con una banda limitata e di bassa qualità non sono sicuramente perseguibili soluzioni cloud. Ed il problema si aggrava con la scarsa propensione del rivenditore a proporre il cloud. L'offerta di soluzioni cloud arriva alle PMI tramite rivenditori, componenti del canale delle grandi aziende dell'offerta. Il rivenditore tipicamente ha margini con la vendita di prodotti, di licenze, di assistenza e di supporto, di progetti di integrazione. Con le soluzioni cloud tutte erogate ed erogabili on line, l'intermediazione del rivenditore viene eliminata. Anche il rivenditore deve trasformarsi e da selezionatore ed integratore di

prodotti e sistemi ICT diventare selezionatore ed integratore di servizi cloud. Trasformazione radicale e non facile, soprattutto in questo periodo di perdurante crisi economica e finanziaria.
Infine la cultura informatica degli imprenditori e dei vertici delle aziende/enti: le cattive esperienze degli anni passati, la poca propensione all'innovazione, il considerare l'ICT una pura commodity e non una tecnologia abilitante al business, se mai un male necessario, frenano ulteriormente l'adozione del cloud. In molte piccole e piccolissime realtà si devono ancora esaurire i periodi di ammortamento dei sistemi ICT acquisiti e non c'è nessun interesse ad acquisire nuovi servizi in cloud sostitutivi di quelli già esistenti "in house", e per di più spesso non consigliati dai rivenditori di fiducia per le ragioni sopra esposte.

Una recente ricerca di Gartner Group evidenzia quali sono i settori in Italia che più utilizzano servizi cloud, come riportato nella fig. 2.17. I macro-settori dominanti sono quattro: comunicazione-media-servizi, istituti finanziari ed assicurativi, Pubbliche Amministrazioni, industria manifatturiera.

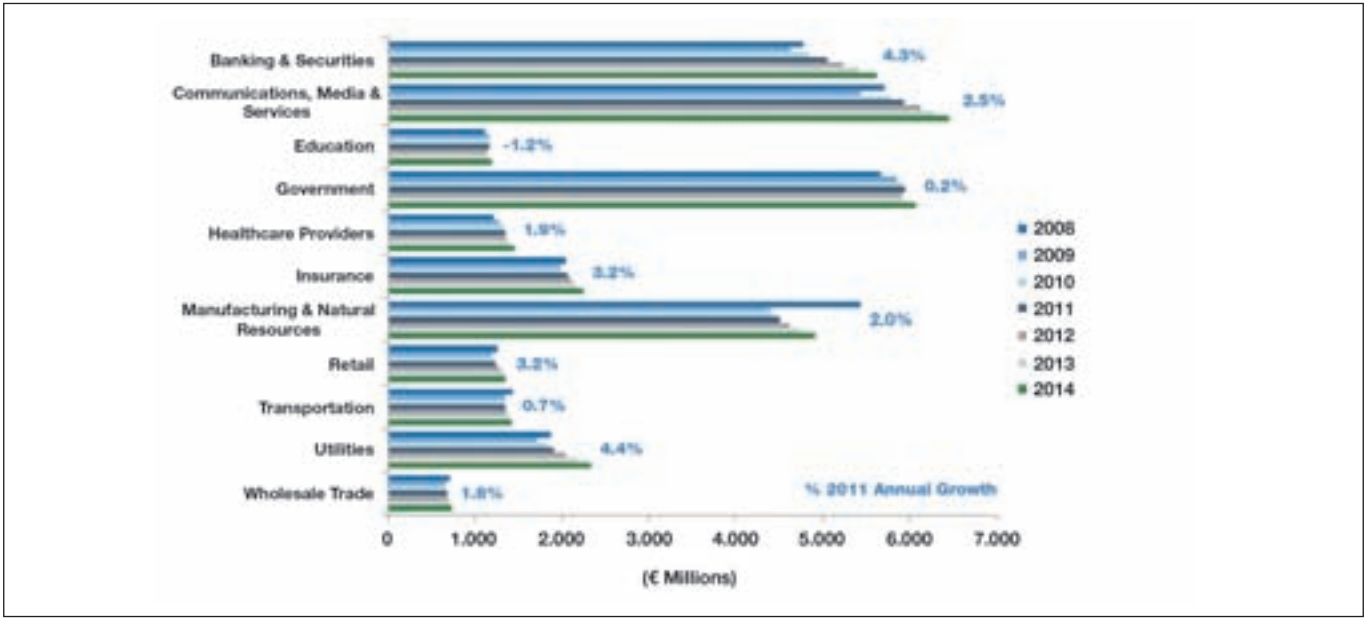


Fig. 2.17 La spesa per servizi clouid in Italia per settore (Fonte: Gartner Group)

E' da evidenziare come la Pubblica Amministrazione, sia Centrale (PAC) che Locale (PAL) rientra tra i quattro settori dominanti, ma ha un tasso di crescita nel periodo considerato di poco superiore allo zero.

Il settore scuola ha un tasso di crescita addirittura negativo, a fronte di una spesa assai più limitata. Facendo riferimento ad altri paesi occidentali, il cloud è una grande risorsa proprio per le PA e per creare relazioni digitali con gli interlocutori, cittadini, imprese, altre PAC e PAL. La realizzazione in Italia dell' **e-government** è in corso da anni, e stando agli ultimi dati ISTAT ed europei[32] è tra i primi in Europa a fornire servizi digitali al pubblico (media UE dell'84,3%) con un grado di interattività pari al 98% per le imprese e al 99% per i cittadini: ma la stragrande maggioranza dei servizi è ancora erogata "on-premise". Nell'ambito dei servizi ICT erogabili dalle PAL emergono quelli relativi alle **smart city**[33], evoluzione del concetto di "digital city" per un nuovo urbanesimo in grado di migliorare sensibilmente la qualità della vita e del lavoro in una società sempre più digitalizzata. La città intelligente diviene elemento di attrazione e di competitività, sul territorio e le logiche cloud, in particolare IaaS e SaaS, sono per le loro caratteristiche un elemento chiave per la sua attuazione. Non è quindi un caso che l'Agenda Digitale Italiana[34] abbia definito due iniziative, una sull'e-gov l'altra sulle "smart city" e le "smart community".

Il cloud impatta sia il mercato business che quello domestico, anche se questi due mercati hanno crescenti aree di sovrapposizione, ed in taluni casi non è più possibile distinguere ciò che è orientato al business e ciò che è orientato all'ambiente e all'uso domestico: le applicazioni per gli smartphone ed i tablet ne sono un esempio. Tutti i grandi player hanno attivato dei negozi virtuali di applicazioni, gli "application store", per acquisire per pochissimi euro o dollari e scaricare sui propri smartphone delle applicazioni sia per il mondo del lavoro che per per quello domestico e di intrattenimento. Basti pensare all' App Store di Apple, a quello di Google per il circuito Android, il BlackBerry App World di RIM, il Nokia Ovi Store, il Windows Market Place di Microsoft, l'Amazon Appstore.
Sono tutte applicazioni scaricabili da web, che hanno fatto rinascere l'"e-commerce" ed i relativi "market place" del decennio scorso, anche se con modalità di offerta e di pagamento diverse.
Il mercato della telefonia mobile è un mercato di massa ove ambiente di lavoro e domestico-personale si sovrappongono, ma sono questi ambienti che hanno, a livello mondiale, tassi di crescita a più cifre. E proprio le applicazioni per i dispositivi mobili risultano lo strumento citato più frequentemente tra quelli che svolgeranno un ruolo chiave in futuro.

2.7 Le tipiche applicazioni del cloud

L'utilizzo o l'interesse ad utilizzare soluzioni di cloud dipende dal tipo di azienda ed ente, ed indipendentemente dalle tipologie deve garantire le seguenti caratteristiche chiave: prestazioni, affidabilità, sicurezza, scalabilità.

---

[32] Nell'indagine "European eGovernment Benchmarking 2010" l'e-gov italiano risulta primo per disponibilità e secondo per la qualità e l'innovazione dei 20 servizi prioritari per i cittadini e le imprese definiti dall'agenda digitale europea.

[33] La città "intelligente" ha infrastrutture ICT a larga banda e servizi digitali per i cittadini e per le imprese capaci di fornire innovazione a livello urbano sulle seguenti 6 principali direzioni di "smart", di intelligente: economia, mobilità, ambiente, persone, vita, "governance".

[34] Per approfondimenti si veda http://www.agenda-digitale.it/agenda_digitale/.

Facendo riferimento alla citata indagine Netxtvalue-CIOnet, le aree di business più interessate in Italia all'adozione di soluzioni cloud sono, oltre ovviamente all'area ICT, le aree marketing, di vendita e di servizi ai clienti; seguono poi l'area personale, logistica, amministrazione e finanza, ed infine l'area produzione.

2.7.1 IaaS

L'adozione di soluzioni IaaS permette l'ampliamento e la razionalizzazione del Data Center, e con l'esponenziale crescita dei dati (i così detti "big data") è di particolare interesse, oltre che per i server, per lo storage, per il Disaster Recovery e per la sicurezza. Unitamente al PaaS, viene poi utilizzato per la realizzazione di ambienti di sviluppo e di test.

2.7.2 PaaS

L'adozione di soluzioni PaaS è estremamente significativa per tutto il settore dell'offerta ICT, oltre che per le grandi organizzazioni che hanno capacità interne di sviluppo e test.
L'interesse maggiore è per gli ambienti di sviluppo e di gestione di siti web e portali, oltre chi di applicazioni, dei servizi di data base e di storage degli oggetti, delle piattaforme di integrazione.

2.7.3 SaaS

Varie indagini a campione, a livello nazionale ed internazionale, hanno analizzato quali sono gli applicativi più terziarizzati, o che si intendono terziarizzare, in logica SaaS.
Lo spettro emerso copre praticamente tutte le applicazioni possibili, e vede soprattutto i seguenti ambiti applicativi come i preferiti:

- posta elettronica ed altri servizi di comunicazione (chat, audio-video conferenza, VoIP, ...);
- ERP, SCM, SFA, HR, AFC, CRM, procurement (acquisti);
- strumenti collaborativi B2C e B2B (web 2.0);
- informatica individuale;
- gestione documentale ed archiviazione sostitutiva;
- sistemi di supporto alle decisioni e di "Business Intelligence";
- gestione progetti;
- sistemi di gestione, controllo e monitoraggio sicurezza ICT;
- Sistemi di gestione, controllo e monitoraggio intero sistema informativo;
- sistemi di discovery e di gestione degli asset ICT.

La fig.2-18 tratta dal Rapporto 2011 dell'Osservatorio Cloud&ICT as a Service del MIP dettaglia le applicazioni in uso o previste in ottica SaaS, evidenziando qualitativamente anche l'entità della spesa e

le applicazioni che per prime sono state realizzate: la conservazione sostitutiva dei documenti e la gestione delle risorse umane.

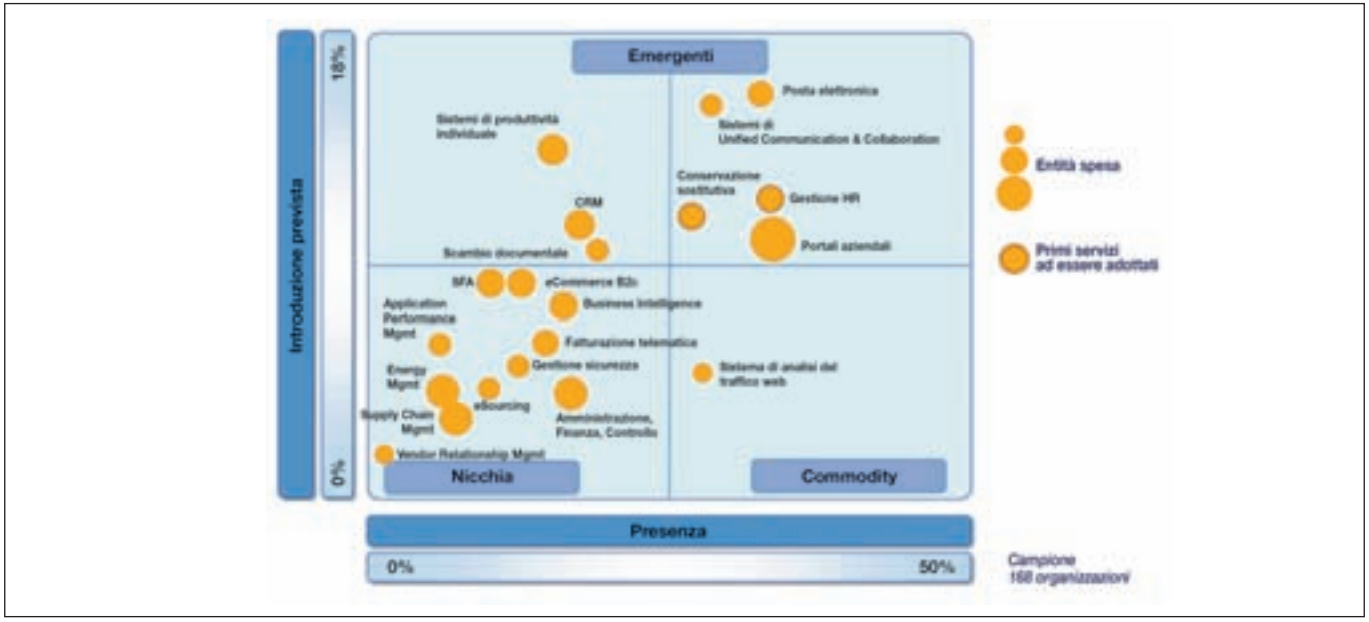


Fig. 2-18 L'adozione e l'introduzione di SaaS (Fonte: MIP)

La fig. 2-19 mostra gli applicativi più usati in cloud dalle PMI in Europa, da un'indagine effettuata da Enisa[35]. Da questa indagine le applicazioni più usate in cloud sono quelle di CRM, cui seguono quelle per lo sviluppo di software, che rientrano nell'ambito PaaS. Al terzo posto gli strumenti per la gestione dei progetti.

E' da evidenziare infine come molti sottoscrittori utilizzino le risorse in cloud, ed in particolare il SaaS, per far fronte a momenti di picco o di malfunzionamento delle risorse "on premise": tale approccio viene chiamato in inglese "cloudbursting".

[35] Enisa, European Network and Information Security Agency, è la struttura dell'UE per la sicurezza ICT: http://www.enisa.europa.eu

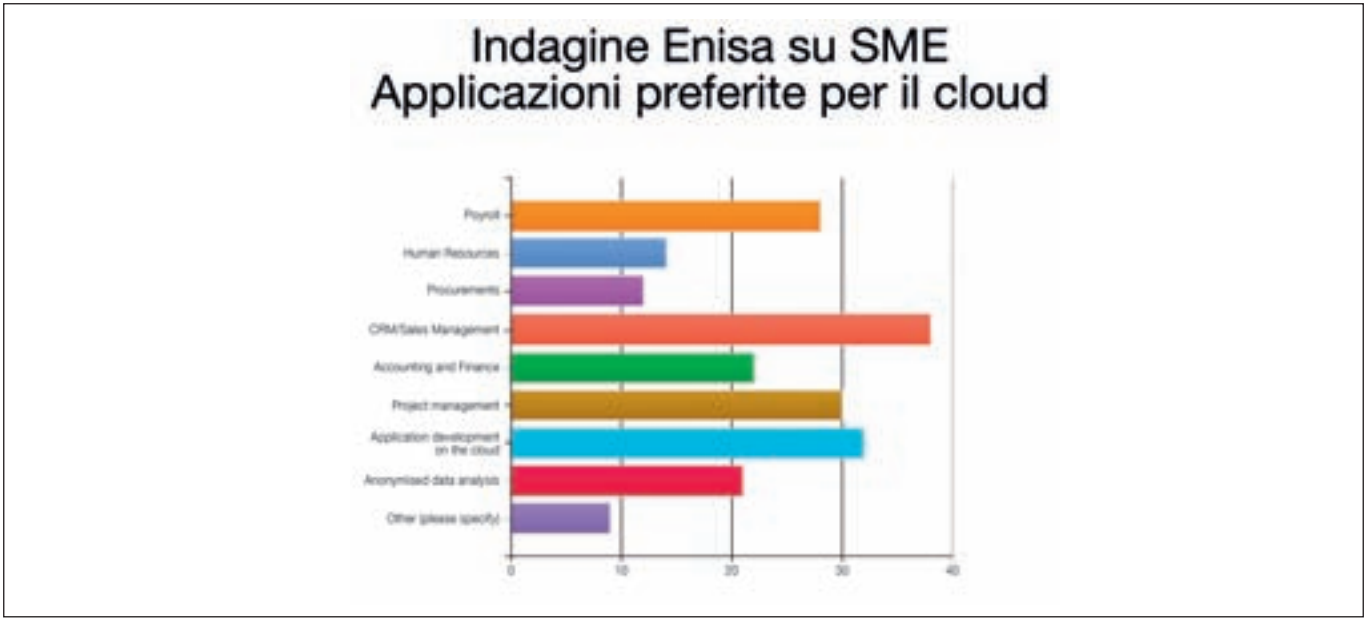


Fig. 2-19 Le applicazioni più usate in cloud dalle PMI europee (Fonte: Enisa)

Per quanto riguarda le Pubbliche Amministrazioni, l'adozione "intelligente" di soluzioni cloud condivise permetterà una significativa riduzione dei costi degli innumerevoli Data Center, soprattutto a livello PAL, migliorando al contempo il loro aggiornamento tecnologico, la loro sicurezza, affidabilità, disponibilità, flessibilità, gestibilità, oltre alla fornitura di nuovi servizi.
Il cloud potrà essere basilare per la riduzione dei tempi e dei costi dell'e-gov, oltre che renderlo più efficace ed efficiente.
L'entrata in vigore del Nuovo Codice dell'Amministrazione Digitale nel 2011, e l'approvazione del Decreto Semplificazioni spingono fortemente alla razionalizzazione dei Data Center delle PA, 1023 solo per le PAC secondo l'ultimo censimento DigitPA, all'apertura e alla valorizzazione del patrimonio informativo (il così detto "open data"), all'offerta di nuovi servizi digitali ed alla riduzione dei costi: il cloud diviene una naturale risposta a tali esigenze.
Di particolare interesse per il mondo sanitario, pubblico e non, il cloud per la telemedicina ed i servizi per gli operatori sanitari e per i pazienti. A livello scolastico ed universitario, e più in generale per la formazione e la ricerca, soluzioni cloud sono e saranno sempre più determinanti per l'alfabetizzazione informatica, per la condivisione di contenuti e di strumenti (in particolare modelli e sistemi di progettazione e di simulazione), per la collaborazione ed il superamento del "digital divide".

3 A chi, quando e come conviene una soluzione cloud

La scelta di una soluzione cloud è logicamente simile alla decisione se terziarizzare o no alcune attività o processi. Il cloud in più consente anche di sostituire vecchi applicativi o vecchie infrastrutture ICT con nuove, oppure di acquisirne di totalmente nuove.
Il corretto modello d'uso delle risorse ICT dipende strettamente dalle strategie dell'impresa o dell'ente, e dal ruolo che l'ICT vi riveste. Si può avere un'infrastruttura tecnologica non più dimensionata sui picchi d'uso ma sui valori medi. Si può individuare un corretto mix di servizi e di risorse, minimizzando l'impatto economico ed operativo della manutenzione di componenti tecnologiche ed applicative. E soprattutto, come già introdotto nei paragrafi precedenti, la possibilità di utilizzare, anche solo in prova, nuove applicazioni e nuovi strumenti ICT di supporto al business (si pensi alle possibilità del "mobile") consente all'azienda/ente di essere **molto più agile ed innovativa sul suo business e sulle sue attività**.

E' importante evidenziare come il cloud impatti sia le aziende/enti lato domanda (che include le Pubbliche Amministrazioni Centrali e Locali), ma anche quelle lato offerta, e questo specificatamente in Italia, che vede una miriade di piccole aziende quali rivenditori, sviluppatori e system integrator.

Per tutti i principali driver per l'utilizzo di una soluzione cloud sono sintetizzabili in un più veloce "***time to value***" e "***time to market***", quali lo sgravo delle risorse interne, la disponibilità "quasi in tempo reale" e su richiesta (on demand) di infrastrutture e di software, la semplificazione dell'aggiornamento dei sistemi, la scalabilità delle risorse ICT in maniera dinamica e in funzione delle esigenze, il miglioramento dei livelli di servizio, in particolare della disponibilità, della sicurezza e dell'affidabilità dei sistemi.
Gli obiettivi principali del "cloud computing" non si limitano ad una mera riduzione dei costi nel trattamento dei dati, ma includono:

- **aumento dell'efficienza dell'ICT**, grazie alla riduzione delle spese in conto capitale (l'ICT "on demand" a costi variabili), all'eliminazione dei costi per la gestione di un "Data Center" e per l'acquisto di risorse ICT non strettamente necessarie (ad esempio l'"over- provisioning"), alla maggior velocità di sviluppo software e di integrazione-interoperabilità, alla maggior concorrenza (e quindi riduzione dei prezzi) tra i diversi Fornitori, alla disponibilità di più sofisticati ed efficienti strumenti di governo dell'ICT, tra cui un aumento del livello di sicurezza e di disponibilità-affidabilità;
- **agilità per il business**: maggior allineamento tra ICT e business, grazie alla razionalizzazione dei "business service" ed alla maggior facilità di attuazione di nuovi applicativi o di modifiche agli esistenti, maggior flessibilità nell'uso di risorse ICT ad alte prestazioni e distribuite;
- possibilità di **far evolvere l'ICT** in vero e proprio motore di cambiamento per il business, permettendo l'accesso a servizi forniti "over the cloud" e la loro immediata integrazione nei processi di business, secondo un modello ibrido di erogazione dei servizi verso gli utenti finali, interni ed esterni.

La conferma sui benefici previsti nell'adozione di soluzioni viene anche dall'indagine nel novembre 2010 del World Economic Forum: come mostrato nella fig. 3-1, al primo posto è la possibilità di usare nuovi servizi e nuovi prodotti, e solo al secondo posto, con uno scarto di 15 punti percentuali, la non trascurabile riduzione dei costi. La possibilità di accedere velocemente ed a basso costo a funzionalità ICT nuove per l'azienda/ente costituisce un fattore determinante per l'innovazione e la competitività: il cloud gioca o può giocare il ruolo non solo di governo della complessità, ma di acceleratore dell'innovazione all'interno della struttura organizzativa.
Significativo che il beneficio posto percentualmente alla pari (con il medesimo 71%) della riduzione dei costi sia la disponibilità in cloud ed il conseguente utilizzo di strumenti per la collaborazione e la condivisione di informazioni.

Da una recente indagine di CIONet, il principale motivo per spingere sull'adozione del cloud è il supporto per singole problematiche (75%) o la trasformazione dell'intera filiera dell'ICT (16%). Restano ostacoli che frenano, però, la diffusione dell'utilizzo di infrastrutture, software e piattaforme nella "nuvola" informatica. Le cause segnalate sono soprattutto sicurezza e privacy (67%) e la difficoltà di integrazione con le applicazioni esistenti (64%). Inoltre, in Italia prevale l'interesse per il cloud ibrido attorno al perimetro aziendale (51%), seguita dal cloud privato (31%). Pochi hanno scelto il cloud pubblico (5%) che in Europa, invece, è un modello di riferimento per la metà degli intervistati.

Con il cloud cambiano per l'utente, ed anche per il fornitore, le tradizionali logiche di licenze software: cambiano in primo luogo per la virtualizzazione. Tradizionalmente le licenze software si basano sul numero di utenti, o autorizzati o contemporaneamente operanti, oppure sul numero di istanze attivate, o di CPU e di sistemi operativi sui quali è attivato il software. Talune licenze si basano su un mix di questi due principi.
Con la virtualizzazione e con l'uso "on demand" del software, il numero di utenti, CPU e sistemi operativi possono variare in maniera significativa anche in tempi molto brevi. Usando le logiche tradizionali di licenza, questo da un lato comporta la necessità di sofisticati strumenti di monitoraggio per il calcolo in tempo reale delle risorse usate, dall'altro può portare a costi molto diversi rispetto a quelli previsti, normalmente ben più alti, per la gestione dinamica e distribuita delle risorse ICT utilizzate.
Il cloud, con la logica di pagamento a consumo, in qualche misura supera per l'utente finale le tradizionali logiche di licenza software, ma non per il fornitore di cloud, che deve ripensare e rinegoziare con le case produttrici di software le licenze nell'ottica delle nuove modalità dinamiche di configurazione e d'uso.
Attenzione che, per l'utente finale, la logica a consumo può rappresentare a sua volta un freno all'adozione del cloud, in quanto non si ha la certezza della spesa complessiva finale, e può risultare difficile fare stime corrette dei budget o bloccare l'uso eccessivo dei servizi.
La logica a consumo deve essere quindi bilanciata con tariffe forfettarie ("flat") che specificano il livello di soglia per un determinato prezzo; ad esempio numero di transazioni e traffico illimitato in Internet ma al massimo un predeterminato numero di utenti registrati o contemporaneamente attivi.

La tabella in fig. 3-2 elenca alcune tipiche necessità per l'UOSI e per ciascuna indica quale XaaS è da considerare.

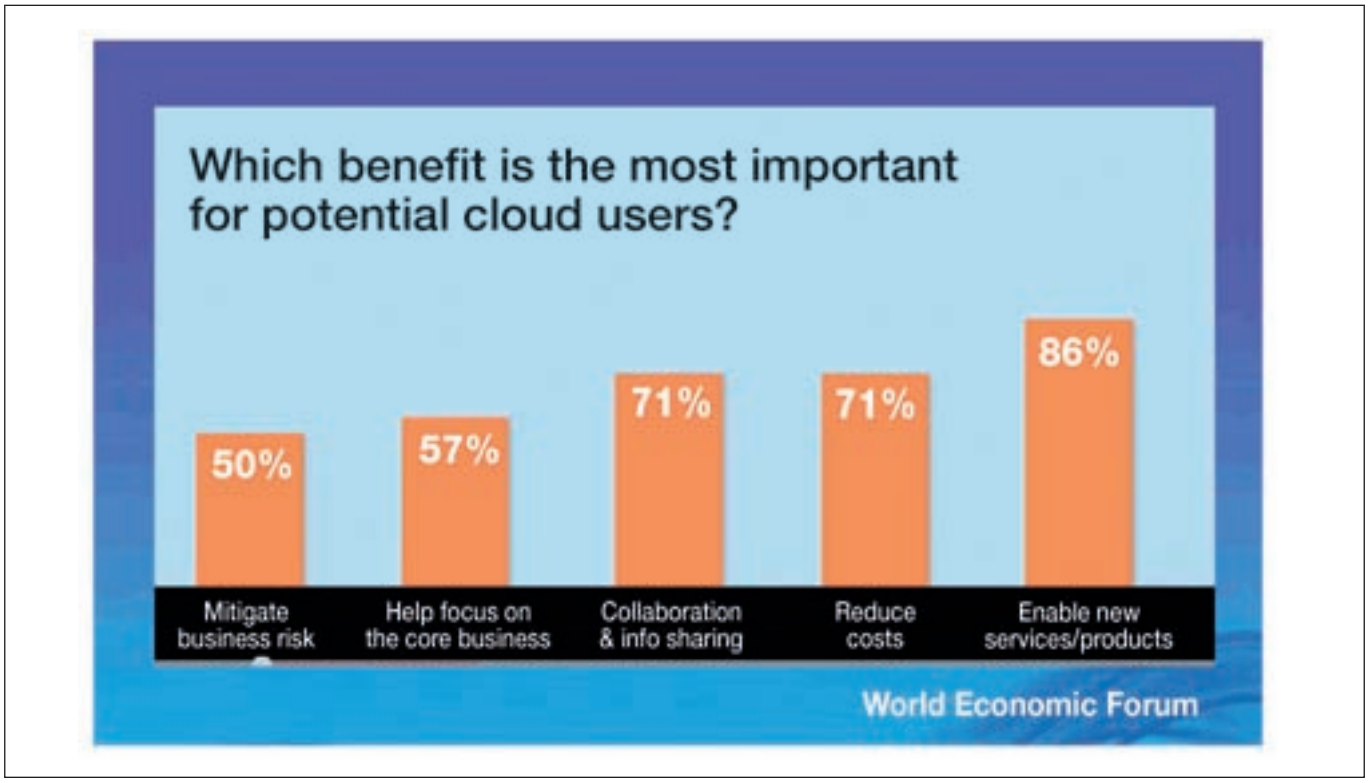


Fig. 3-1 I principali benefici per un utente del cloud (Fonte: World Economic Forum)

Necessità/problema	***possibile soluzione cloud***
Necessità ulteriore capacità elaborativa (magari temporanea)	IaaS
Terziarizzare e migliorare la gestione operativa	IaaS
Rinnovare parco server	IaaS
Migliorare livello sicurezza	IaaS e SaaS
Disporre di back-up più affidabili e di un Disaster Recovery	IaaS
Sostituire un applicativo	SaaS
Acquisire un nuovo applicativo	SaaS
Adottare strumenti collaborativi	IaaS e SaaS
Migliorare la governance complessiva dell'ICT	IaaS e SaaS
Provare una nuova soluzione informatica	IaaS e SaaS
Mobilità e comunicazioni unificate	IaaS e SaaS
Nuovi ambienti di sviluppo e nuovi linguaggi di programmazione	PaaS

Fig. 3-2 Quale XaaS per quale necessità

Il cloud non è solo un'opportunità/necessità lato domanda, ma anche lato offerta, soprattutto in Italia dove a fronte di pochi grandi produttori di software, tipicamente le rappresentanze delle grandi case multinazionali, esiste una miriade di piccole e medie aziende operanti come rivenditori, installatori, integratori di sistemi, consulenti. La maggior parte di queste aziende fanno parte del canale di distribuzione delle grandi case, ed i loro maggiori margini dipendono dalle licenze, dalla installazione e personalizzazione, talvolta con sviluppi ad hoc, dalla manutenzione ed assistenza in locale, dalla formazione e addestramento. Ma l'erogazione di servizi in cloud direttamente e centralmente da parte delle grandi case, si pensi ad esempio all'offerta di Office tramite Azure, riduce o addirittura elimina questo livello di intermediazione, con la perdita di molta parte dei guadagni dei rivenditori fino ad oggi possibili.
Risulta evidente che queste aziende dell'offerta devono in qualche modo trasformarsi e riqualificarsi con l'avvento del cloud, pena la loro sparizione dal mercato. Le opportunità, a giudizio dell'autore, ci sono in quanto, analogamente a quanto è successo e succede con la proliferazione di sistemi e di applicativi, ogni produttore, grande o piccolo, sta offrendo i propri prodotti in cloud con forti azioni di marketing. Il cliente finale è subissato di offerte, non ha spesso tempo o competenze per valutarle, e rimane disorientato: ecco che il "rivenditore" può aiutarlo nella scelta, un "**service selection**" invece

del precedente "software selection" ed aiutarlo nella integrazione del servizio con altri e con i preesistenti sistemi ICT gestiti "on-premise", nell'ottica dell'esempio di fig. 2.3. In tal senso da "system integrator" diviene "**service integrator**". L'uso di PaaS può inoltre essere un elemento di riduzione dei costi, di alta flessibilità e quindi di vantaggio competitivo: possibilità di accedere ad ambienti di svi-

Tema	***Soluzione cloud***	***Soluzione on premise***
Aggiornamento hardware	Sistematico	Richiede approvazione ed acquisto; temi lunghi
Aggiornamento software	Sistematico	Richiede approvazione ed acquisto; tempi lunghi
Maggior capacità elaborativa	On demand, praticamente in tempo quasi reale	Richiede acquisizione nuovo hw e sw con disponibilità budget; tempi lunghi
Sicurezza	Elevato livello sicurezza fisica e logica	
Gestione SLA e KPI	Come da contratto	Raramente gestite
Monitoraggio e controllo prestazioni	Accurata	Dipende molto società per società
Gestione policy	Accurata	Dipende molto società per società
Manutenzione	Sistematica	Spesso non sistematica
Gestione incidenti	Ben organizzata, proceduralizzata e automatizzata	Il più delle volte empirica
Supporto processi ICT	Segue best practice, proceduralizzato e almeno in parte automatizzato	Dipende molto società per società, il più delle volte embrionale
Monitoraggio e controllo	Centralizzato, sistematico e in dettaglio	Dipende molto società per società, il più delle volte a silos
Compliance normative	Per i fornitori europei accurata	Dipende molto società per società
Competenze	Ampie e di dettaglio	Limitate
Consumo energetico	ridotto	Elevato

Fig. 3-3 Schematico confronto tra soluzioni ICT in cloud e on premise

luppo allo stato dell'arte e totalmente scalabili, utilizzare di volta in volta l'ambiante più adatto o richiesto dal cliente, e così via.
La Tabella in fig. 3-3 evidenzia i principali pro e contro di una soluzione cloud rispetto all'analoga "on premise".

L'adozione di una soluzione cloud non è la panacea dell'ICT, e non è sempre adottabile in tutti i casi e per ogni sistema informatico. Si pensi ad esempio alla disponibilità o meno di connessioni ad Internet di banda adeguata nelle sedi dell'azienda/ente, oppure la gestione di banche dati e sistemi di conoscenza con segreti industriali, e così via.
In §2.3 sono riportate le considerazioni dell'autore di quale possa essere, contesto per contesto, la soluzione cloud preferibile tra pubblica, privata ed ibrida.
Qualunque sia il modello di erogazione dei servizi in cloud, ma soprattutto per il cloud pubblico, il ***contratto di servizio*** tra l'azienda/ente cliente, il sottoscrittore, ed il fornitore è l'elemento fondamentale.
Il sottoscrittore deve assicurarsi che il contratto (spesso standardizzato e poco personalizzabile):

- sia conforme alle normative europee ed italiane;
- chiaramente definisca, anche come terminologia, i servizi e come sono erogati, precisando i Data Center dove possono essere trattati i dati;
- specifichi le modalità di monitoraggio in termini di SLA e KPI;
- dettagli gli strumenti di sicurezza in uso e come sono gestiti (ad esempio scadenze password, protezione dei dati critici e sensibili, ecc.);
- dettagli come sono gestiti gli eventuali incidenti e la risoluzione dei problemi;
- specifichi che cosa succede se il fornitore non mantiene i livelli di servizio sottoscritti: eventuali penali, possibilità di recesso, ecc.;
- specifichi le modalità di cessazione del contratto e la salvaguardia e portabilità dei dati e del software, per evitare il "locked-in".

In §7 sono riportati alcuni suggerimenti e considerazioni sugli aspetti legali e contrattuali che è opportuno considerare.

4. Lato offerta: i principali attori in Italia e le loro proposte di cloud

La quasi totalità dei fornitori di software applicativo, di piattaforme e di housing-hosting offre soluzioni cloud di vario livello. Praticamente qualsiasi programma software è ormai disponibile in cloud "as a service".
Diverse le tipologie d'offerta dell'XaaS, prevalentemente in funzione dei prodotti-sistemi-servizi che tradizionalmente erano vendute. Usando la tipica terminologia inglese, è possibili classificare i diversi fornitori come:

Nome cloud	***Fornitore***	***Italiano/ mondiale***	***IaaS***	***PaaS***	***SaaS***	***BPaaS***
Accenture	Accenture				x	x
Acrobat.Com	Adobe				x	
Aruba	Aruba	x	x	x	x	
ASP Italia	ASP Italia	x	x	x	x	
Azure	Microsoft		x	x	x	
Bungee Connect	Bungee Lab			x		
CBT	CBT	x			x	
Cloe	Engineering	x	x	x	x	
CloudAssure	HP		x	x	x	
Elastic Computing Cloud (EC2)	Amazon		x	x		
ElasticHosts	ElasticHosts Ltd		x			
FlexiScale	Flexiant		x			
Force.com	SalesForce.com,			x	x	
Google App Engine	Google			x		
GoGrid	GoGrid		x			
Nuvola	Telecom Italia	x	x			
Platform Computing	Platform Computing		x	x	x	
Rackspace Hosting	Rackspace		x	x	x	
Reply Cloud	Reply	x	x	x	x	
SBI Italia	SBI Italia	x	x	x	x	
Seeweb	Seeweb	X	x	x		
SmartCloud Enterprise	IBM		x			
SuiteCloud	NetSuite				x	
Sun Cloud Compute Utility	Sun-Oracle		x			
Verizon Business	Verizon Business		x			

Fig. 4-1 Esempio di fornitori XaaS a livello mondiale ed italiano

- ***"component developer"***: fornitore dei componenti hardware e software per la costruzione di infrastrutture cloud;
- ***"service provider"***: fornitore di un insieme specifico di XaaS;
- ***"cloud broker"***: aggregatore e rivenditori di servizi erogati da fornitori diversi;
- ***"solution provider"***: fornitore che progetta e realizza soluzioni ad hoc per soddisfare le esigenze di un cliente o di un gruppo di clienti.

Un'ulteriore classificazione indica come ***"pure player"*** le aziende che sono focalizzate prevalentemente, se non esclusivamente, sull'offerta di cloud, come "***incumbent***", le tradizionali grandi aziende dell'ICT a livello mondiale che offrono i loro "tradizionali" prodotti hardware e software, come ***new player*** o di recentissima costituzione o aziende già esistenti dell'ICT, come i carrier delle telecomunicazioni fisse o mobili, che partendo dai loro prodotti e servizi offrono cloud.

A parte i già citati "application store" per applicativi per gli smartphone ed i tablet, la parte del leone a livello mondiale è svolta da alcuni "incumbent" da Microsoft a Google.
In Italia sono già presenti numerosi attori, come Telecom con Nuvola, e "pure player" come Seeweb, che stanno ritagliandosi a livello nazionale ed internazionale (prevalentemente europeo) un proprio crescente spazio nel settore cloud.

La Tabella in fig. 4-1 riporta alcuni dei principali fornitori a livello mondiale e nazionale (nella colonna italiano/mondiale sono evidenziate con un marcatore le società italiane). Questa tabella è puramente indicativa, perché sono ormai migliaia le aziende italiane che a vario titolo offrono servizi cloud: quasi ogni produttore o rivenditore di un programma software lo rende infatti disponibile in logica cloud.

La crescita del mercato cloud erode fortemente altri segmenti del mercato ICT, dalla vendita di hardware e di software ai contratti per la loro manutenzione.
Il fenomeno cloud rappresenta quindi un inderogabile momento di ripensamento della strategia e del futuro business per un attore dell'offerta. Trasformare l'azienda da venditore di hardware e/o software in venditore di servizi cloud rappresenta un forte cambiamento sui processi di business, sulle competenze del personale, sul tipo di relazione con i clienti; e richiede investimenti, anche culturali, non trascurabili.

5. Esempi di caso d'uso lato domanda

L'Italia ha ormai una nutrita serie di esperienze nell'adozione di soluzioni di cloud sia presso grandi strutture, sia presso medie e piccole.
Nel seguito si elencano alcuni casi d'adozione di soluzioni cloud in Italia, per aziende totalmente italiane o per sussidiarie italiane di corporate straniere, suddividendoli tra grandi, piccole medie aziende/enti, considerando sia casi del settore privato che del settore pubblico.

5.1 Grandi organizzazioni

5.1.1 Ferrovie dello Stato

L'outsourcing dei sistemi informativi delle Ferrovie dello Stato (FS) risale al secolo scorso: la prima terziarizzazione data 1996 e la successiva a fine 2010, a seguito di una nuova gara,per la gestione e lo sviluppo dell'intero sistema informativo, a supporto del piano di business pluriennale.
Gli obiettivi del piano industriale delle FS, focalizzato sul raggiungimento dell'equilibrio economico e finanziario dell'azienda, includono elementi chiave quali la leadership nel mercato domestico, la concentrazione della produzione nelle aree a maggior valore e la specializzazione delle società del Gruppo lungo la filiera produttiva, l' eccellenza operativa, l'internazionalizzazione, il miglioramento tecnologico continuo.
Il sistema informativo FS diviene l'elemento abilitante per raggiungere tali obiettivi di business, e con il nuovo contratto tra FS ed il Raggruppamento Temporaneo d'Impresa che si aggiudicò la gara del 2010, è stato realizzato un "*Corporate Private Cloud*" dedicato ai servizi FS, che usufruisce anche dell' infrastruttura cloud Nuvola Italiana di Telecom Italia, partecipante all'RTI vincitore. Gli obiettivi conseguenti a livello ICT includono la sostenibilità ambientale, un forte miglioramento della continuità operativa e della sicurezza, una migliore governance anche dei fornitori, ed orientata ai servizi per l'utente finale e con l'accentramento di responsabilità.
Il consolidamento e la razionalizzazione dei server nei Data Center FS ha portato alla riduzione dei server fisici da 1810 a 411, creando 2006 server virtuali. Gli stessi Hypervisor per la virtualizzazione sono stati ridotti da 142 a 79. Il risparmio energetico complessivo, con la razionalizzazione dei Data Center, è del 70%.

5.1.2 Gruppo Eni

Il Gruppo si è focalizzato su un cloud privato, con una roadmap iniziata nel 2007 e da completarsi nel 2013, articolata, anno per anno, nei seguenti passi: consolidamento infrastrutture, virtualizzazione, "capacity planning", Green Data Center, semplificazione e razionalizzazione applicativa, completamento del cloud privato ENI, chiamato eDI, EniDynamic Infrastructure.
I principali obiettivi includono la riduzione dei consumi energetici e dell'emissione di CO_2 con la realizzazione di Green Data Center, l'ulteriore consolidamento di server e storage, la semplificazione degli ambienti con una forte loro standardizzazione, l'orientamento ai servizi con una gestione proattiva del "demand" e del "capacity planning", il miglioramento della governance dei sistemi e dei fornitori.
Il consolidamento dei sistemi è avvenuto prevalentemente nel 2008, con la virtualizzazione di 800 server su 20 server fisici per gli ambienti Windows e 400 server virtuali su 30 server fisici per gli ambienti Unix.
La semplificazione degli ambienti, basata su una forte standardizzazione nell'ambito dell'ICT Enterprise Architecture, ha ridotto:

- i sistemi operativi da 6 a 2, le loro versioni da 25 a 4;
- i data base da 9 a 2, le loro versioni da 45 a 4.

5.1.3 Poste Italiane

Per le Poste Italiane l'ICT è a supporto dell'evoluzione del nuovo modello di business, orientato all'agilità dell'impresa (enterprise agility) grazie alla SOA: dai tradizionali servizi postali e finanziari all'estensione di nuovi canali, all'e-communication ed ai nuovi mercati.
Il cloud computing si inserisce nel piano di sviluppo iniziato nel 2004 ed articolato nei seguenti principali passi: consolidamento funzioni ICT, evoluzione ed integrazione delle reti, consolidamento e razionalizzazione dei Data Center, progetti evolutivi infrastrutture, progetti evolutivi applicazioni. Il quadro di riferimento è l'architettura SOA sulla cui base sono in corso progetti di cloud privato nell'ottica di realizzare una "Business Partner Integration" (BPI): Poste Italiane, operando sempre più come una "network company", intende svolgere anche il ruolo di "one-stop-shopping" erogando servizi di terze parti (i business partner) integrandoli con i propri.
A livello cloud è stata definita la piattaforma BPI, e a livello applicativo l'obiettivo è di fornire SaaS per i processi di business, in particolare BPM, Business Process Management, BAM, Business Activity Monitoring, Business Intelligence.

5.1.4 EMC²

Questa grande multinazionale dell'ICT ha intrapreso la trasformazione del proprio sistema informatico nel 2004, avendo una "vision" finale di "ICT as a service" basata su un modello di cloud ibrido, con virtualizzazione dei "client" fissi e mobili, a fronte di un grande sviluppo sintetizzabile nei seguenti dati tra il 2004 e 2012:

- da 24.000 a 53.000 utenti interni;
- da 70.000 a più di 400.000 tra clienti e partner;
- operante da 50 a più di 80 paesi, passando da 15 a oltre 20 lingue;
- da 2000 server fisici con 400 applicazioni circa in 5 Data Center a 6500 immagini di sistemi operativi con più di 500 applicazioni, con l'86% dei server virtualizzati, sempre nei 5 Data Center iniziali;
- da 960 TB di storage a circa 12 PB complessivi, con ora 52 Mlni di Transazioni/giorno su una delle più grandi singole istanze di Oracle 11i eBusiness Suite.

Il percorso per questa trasformazione è stato articolato in tre fasi principali:

a) 2004-2008: focalizzazione sulla razionalizzazione delle infrastrutture, con la virtualizzazione di circa il 38% dei server;
b) 2008-2010: focalizzazione sulla razionalizzazione delle applicazioni, con la virtualizzazione di circa il 72% dei server;
c) 2010-2012 ed oltre: focalizzazione sul business e sull'ICT come servizio, con la virtualizzazione di circa il 86% dei server alla data attuale.

Il rapporto di Virtualizzazione tra ambiente virtuale e fisico (V:P) è in media di 22:1, con picchi di 38:1. Significativi i risparmi economici ed energetici. Nella prima fase si è avuto un risparmio di $ 74 Mlni di dispositivi nei Data Center, e di $ 12 Mlni di spazi e di energia, a fronte di un aumento del 170% della

produttività nella gestione archivi e del 34% dell'efficienza energetica, con un risparmio di 60 Mlni di pound di CO_2.
Nella seconda fase si è ottenuto un risparmio di $ 11 Mlni nelle spese operative (OpEx) e di $ 6 Mlni di dispositivi nei Data Center; a livello ambientale un risparmio di 30 Mlni di pound di CO_2.
Questa grande trasformazione ha permesso di dedicare % crescenti del budget ICT a nuovi progetti (nel 2011 tale quota era del 42% sul totale del budget) e di ridurre drasticamente il tempo di provisioning per un'applicazione, passando dai 90 giorni del 2004 all'attuale 1 solo giorno. La razionalizzazione dell'infrastruttura ICT per la realizzazione del cloud privato ha portato ad un guadagno in prestazioni di un fattore x10, con uno specifico risparmio di circa $ 7 Mlni.
Il lungo percorso di cloudizzazione ha portato anche profondi cambiamenti sul ruolo dell'UOSI, che è diventata un fornitore interno di servizi ICT, misurabili e controllabili da SLA, in piena trasparenza e con il ri-addebito delle spese alle linee di business utenti.

5.2 Medie e piccole organizzazioni

5.2.1 Ospedale Pediatrico Bambin Gesù

L'Ospedale è un punto di eccellenza a livello nazionale per la cura dei bambini e si articola su quattro sedi, due in Roma e due sulla costa tirrenica, una a Palidoro ed una a Santa Marinella.
L'ICT rappresenta uno strumento fondamentale per il funzionamento della sua complessa struttura, che conta circa 2500 dipendenti, strumento focalizzato sui servizi per i pazienti, per gli operatori sanitari e per la gestione dell'ospedale nel suo complesso.
In tale contesto la posta elettronica riveste un ruolo chiave sia all'interno dell'intera organizzazione sia verso l'esterno; essa richiede funzionalità diverse per i diversi interlocutori, l'accesso da un'ampia gamma di dispositivi d'utente, un elevato livello di autenticazione degli utenti e di confidenzialità, ed in taluni casi la capacità di gestire allegati di grandi dimensioni.
Con tali obiettivi l'Ospedale ha deciso di passare da una soluzione "on premise" ad una soluzione cloud di posta elettronica molto avanzata, scegliendo un servizio leader sul mercato soggetto non solo al confronto ma alla continua concorrenza con i vari fornitori.
I benefici ottenuti con la soluzione cloud includono la velocità di realizzazione del nuovo servizio di posta elettronica, un livello di sicurezza molto maggiore rispetto alla precedenti soluzioni, la diversificazione delle caratteristiche della casella di posta per tipologia d'utente, una migliore e più efficace compliance per la privacy, una riduzione complessiva dei costi, una affidabilità quasi totale garantita anche a livello contrattuale, con SLA molto stringenti e con penali in caso di loro mancato rispetto.

5.2.2 Wolters Kluwer Italia

Wolters Kluwer Italia (WKI) è la struttura italiana di uno dei principali provider internazionali di soluzioni editoriali, formative e software per i professionisti e le aziende. Il Gruppo fornisce prodotti e servizi per i mercati legale, fiscale, amministrativo e finanziario, medico scientifico e giuslavoristico.

In Italia WKI riunisce undici tra i più autorevoli e accreditati brand che realizzano prodotti e servizi editoriali specializzati, formazione e software per il mercato professionale e aziendale, da Artel a Il Fisco, da IPSOA a UTET Giuridica.
WKI da anni forniva un servizio di rilevazione presenze (chiamato "To Check") in hosting via web in logica ASP, che ha passato ora in logica SaaS su cloud pubblico fornito da Seeweb, per servire contemporaneamente più di 300 aziende con oltre 52.000 utenti.
Gli obiettivi raggiunti con questo SaaS includono:

- di gestire l'obsolescenza delle macchine, che rendeva complesso il loro aggiornamento e la loro riparazione in caso di guasti;
- di non sviluppare o acquisire competenze specifiche per la gestione dei sistemi ICT;
- di mantenere un ottimo livello di servizio, con tempi di ripristino di 3 ore in caso di danno macchina garantiti attraverso SLA definite a livello contrattuale, con una copertura globale per 24 (ore) x7 (giorni) x52 (settimane);
- per i clienti di gestire dinamicamente e in modo molto rapido i picchi di carico delle richieste del servizio.

5.2.3 YouReporter.it

YouReporter (www.youreporter.it) è un portale di informazioni online, fornite anche dagli stessi utenti, con grandi variazioni di accessi a seconda degli eventi occorsi. Questo portale è passato da una in-

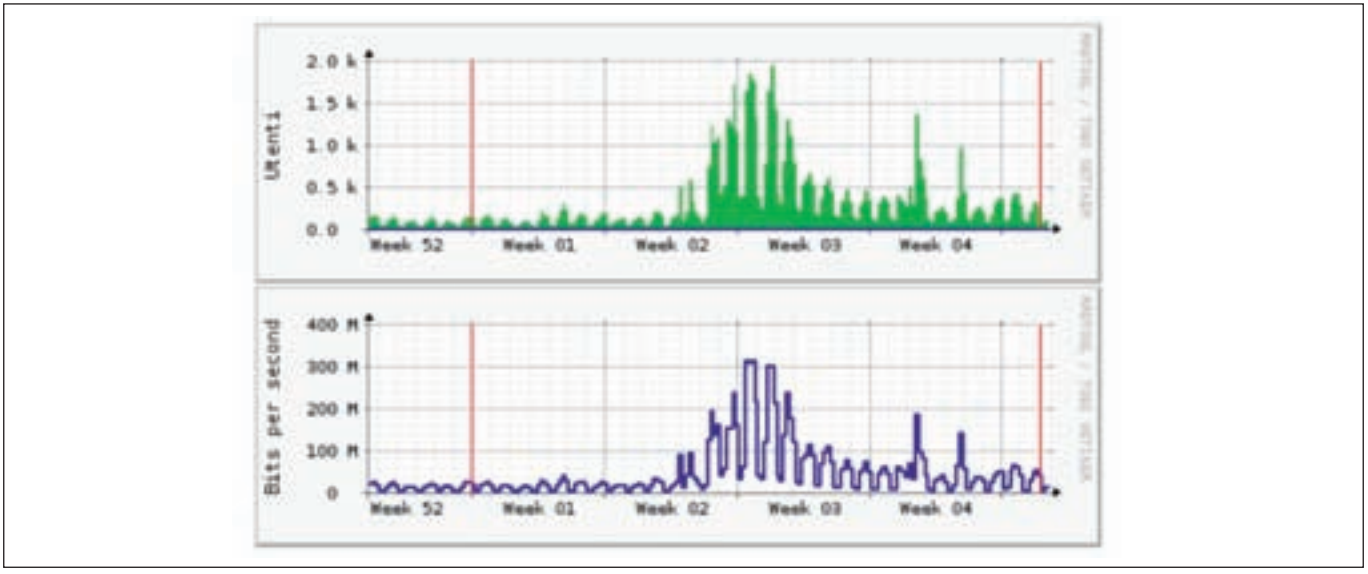


Fig. 5.1 Picco di accessi e di downstreaming di YouReporter.it (Fonte: Seeweb)

frastruttura “on premise“ gestita internamente ad un’infrastruttura cloud pubblica, passando da picchi di 10.000 utenti /giorno a picchi da 3.000.000 di utenti /giorno. La fig. 5.1 evidenzia questa capacità di gestire, “on time e on budget”, forti variazioni di numero d’utenti e di traffico.

Questi picchi rappresentano 808’000 video visualizzati per 1152 GBytes complessivi di traffico.
Il costo base dell’intera infrastruttura su cloud pubblico è dell’ordine dei 200,00 Euro / mese se non ci sono picchi di accesso e di traffico.
Un significativo esempio di picco di accessi e di “down-streaming“ di filmati fu a seguito della seconda scossa di terremoto in Emilia, evidenziato dal sottostante grafico di fig. 5.2 che fa riferimento all’ultima settimana di maggio 2012.

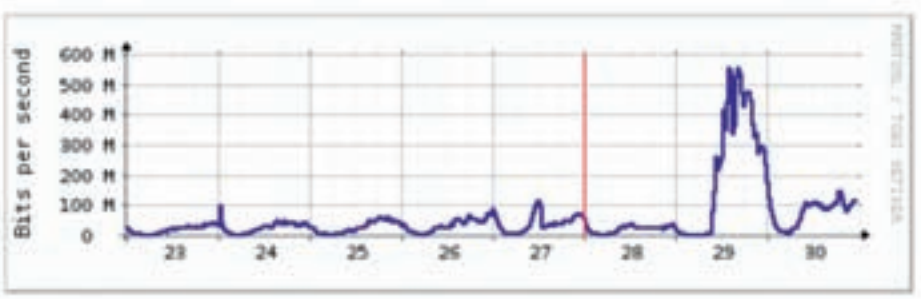


Fig. 5.2 Grafico del picco di traffico su YouReporter.it in occasione della seconda scossa tellurica in Emilia (Fonte: Seeweb)

In questa eccezionale e tragica occasione, YouReporter.it ha dovuto reagire in tempo reale ad una situazione di picco caratterizzata da 4.756.000 visite al sito, con 1.667.000 video visti e circa 2300 GB di traffico. Grazie al cloud pubblico YouReporter.it è riuscita a far fronte a queste esigenze istantanee al solo costo delle componenti a consumo e solo per i giorni di reale utilizzo. La spesa complessiva per l’intero mese di maggio 2012 è stata di 2.332,00 Euro.

5.2.4 Docebo

Docebo (http://www.docebo.com/it) è un’azienda italiana che fornisce servizi di formazione a distanza (e-learning) tramite la piattaforma LMS Docebo che consente di erogare, tracciare e certificare processi di formazione in più di 25 lingue diverse, e che si basa sugli standard SCORM[36] v. 1.2 e 1.3.

[36] SCORM, Shareable Content Object Reference Model, definisce per l’e-learning le specifiche relative al riutilizzo, tracciamento e catalogazione degli oggetti didattici che costituiscono i componenti di base per realizzare i corsi a distanza, nell’ambito della piattaforma LMS, Learning Management System, che interagisce con tali oggetti.

Alla sua nascita nel 2005, Docebo aveva una soluzione “on-premise“ che nel 2008 contava su 8 server con uno storage su NAS ed una posta elettronica interna; alla data, il costo annuo per il Data Center era di €40.863,00.
Con il crescere dei clienti e con la necessità di variazioni anche forti del carico sui sistemi, Docebo ha deciso non solo di migrare su soluzioni IaaS, ma anche di utilizzare servizi SaaS e di erogare essa stessa l’e-learning in modalità SaaS.
La trasformazione intrapresa ha portato ad un totale passaggio su un cloud ibrido. Da un lato servizi IaaS da Seeweb, che fornisce 5 Cloud server, 1 Cloud Hosting e 1 Cloud Storage, servizi che sostituiscono e potenziano le funzionalità che erano degli 8 server e dei NAS. Dall’altro lato alcuni servizi in SaaS con Google che prima erano gestiti sulla infrastruttura “on-premise“: in particolare la posta elettronica con Gmail e Google Docs per l’informatica individuale e la condivisione dei documenti.
L’attuale costo per i servizi cloud di Google e Seeweb è attorno a € 15.500 all’anno.
Dal 2011 Docebo ha iniziato ad offrire LMS Docebo come SaaS, che ora copre il 75% del venduto di e-learning.

6. Linee guida per una corretta scelta e gestione del cloud

Senza alcuna pretesa di descrivere una metodologia, ma sulla base delle “best practice” emergenti e dell’esperienza in campo dell’autore, si evidenziano nel seguito alcuni suggerimenti per una scelta ed una gestione efficace. Questi suggerimenti sono per il proponente ed il decisore che, soprattutto nelle piccole realtà, spesso coincidono nella stessa persona.
Per non ampliare troppo le dimensioni del presente Rapporto, i suggerimenti sono esposti in maniera sintetica e per punti. Talune delle attività elencate possono essere svolte in parallelo, altre devono essere sequenziali.

Con queste note si cerca di dare un quadro completo, anche se sintetico: può apparire di una certa complessità e, nel seguirlo dettagliatamente, può richiedere competenze e tempi non trascurabili. E’ evidente che per effettuare una scelta non si possono spendere tante o maggiori risorse di quelle che si vorrebbero risparmiare con l’adozione della soluzione scelta. Occorre quindi approcciare il processo decisionale in maniera corretta ma “leggera”, in maniera “**lean**“ come si usa dire derivando il termine dai processi di produzione.
Ma “lean“ non significa superficiale: occorre considerare e conoscere i dati essenziali per poter decidere nello specifico contesto, cercando di non farsi influenzare da preconcetti o da “sentito dire” non riscontrabili.
Il cloud inoltre offre un’opportunità in più: poter provare un determinato servizio per un breve periodo di tempo, con un’immediata sua attivazione e coinvolgendo nella prova poche persone con elevata esperienza sul processo supportato. Nel giro di breve tempo, ossia giorni, è possibile avere una chiara idea dell’usabilità e della convenienza del servizio, e decidere se porlo in produzione per la propria organizzazione oppure no.

La fig. 6.1 schematizza i punti chiave dell'intero processo.

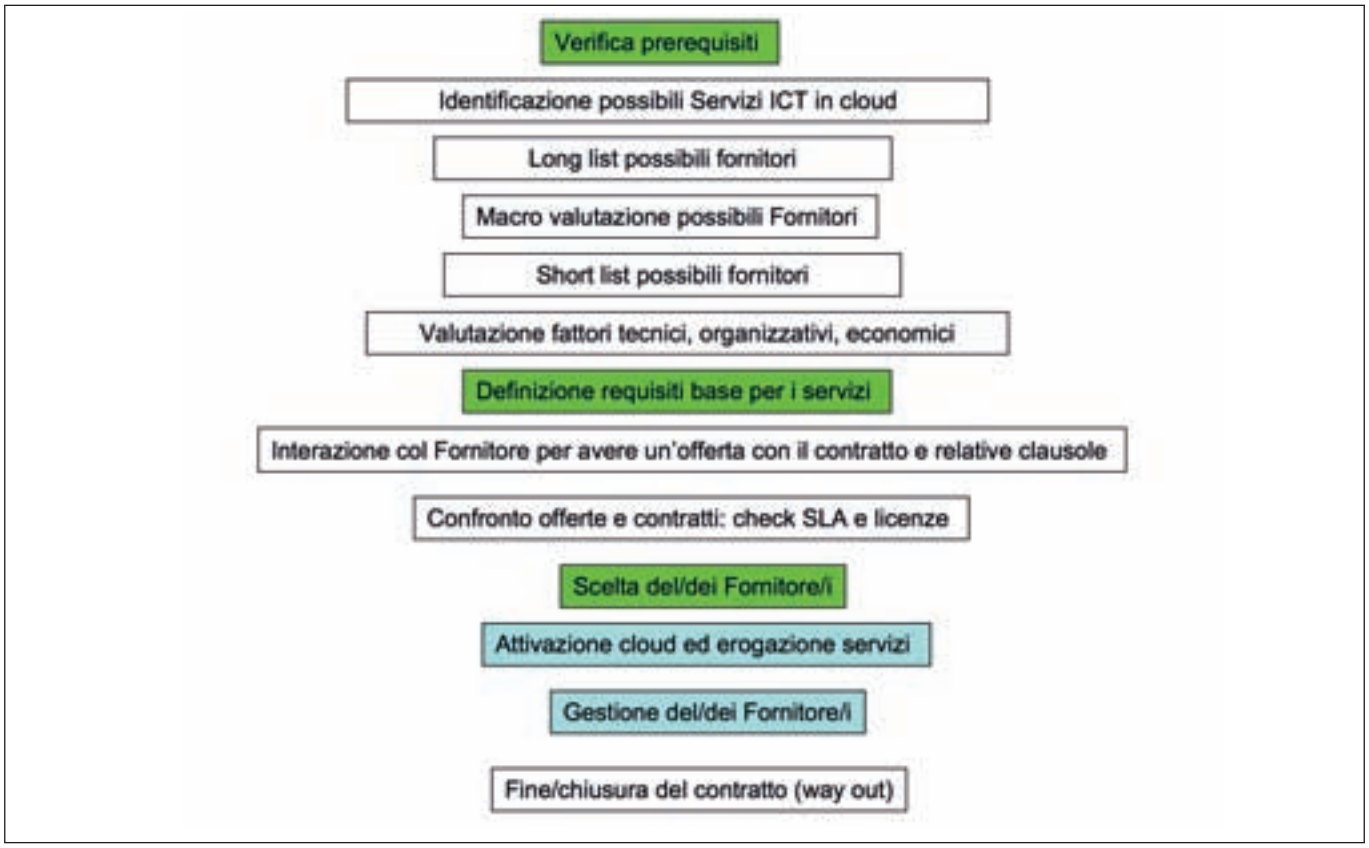


Fig. 6.1 Schematizzazione principali passi per la scelta e la gestione di soluzioni cloud

Nel processo decisionale per la scelta di una soluzione cloud, è bene tener conto di molteplici fattori tra loro correlati, di natura tecnica, economica ed organizzativa.
I **fattori organizzativi** includono il "commitment" del vertice, ossia la sua volontà di adottare il cloud, l'accettabilità da parte dell'utenza finale legata al suo coinvolgimento, la collaborazione ed il coordinamento tra utenti ed UOSI, l'ottimizzazione dei processi operativi supportati dal cloud, la criticità dell'applicazione (per SaaS) ed il suo uso presso aziende/enti simili e/o concorrenti (imitare quello che fanno gli altri). Per quanto riguarda il fornitore, i fattori organizzativi principali riguardano la sua

reputazione, quindi la sua affidabilità e qualità (percepite o acquisite precedentemente), le caratteristiche e le tipicità dei servizi offerti.
I **fattori economici** includono le logiche e le politiche finanziarie e di bilancio (tipicamente per la valutazione Capex vs Opex ed i temi trattati in §2.5), il miglioramento dei costi ICT e del personale, la riduzione del rischio operativo, i miglioramenti prestazionali, le economie di scala, il ritorno del valore più rapido e più elevato, così come approfondito sempre in §2.5.
I **fattori tecnici**, trattati in §2.2, includono la facilità d'uso e di personalizzazione, il supporto di standard consolidati in particolare per l'interfacciamento e l'interoperabilità, la sicurezza, la scalabilità, le prestazioni, l'assistenza e l'aggiornamento.

6.1 Prerequisiti

I prerequisiti riguardano il sottoscrittore, non sono obbligatori ma fortemente suggeriti, ed includono:
- disponibilità nelle sedi che utilizzerebbero le soluzioni cloud di connessioni primarie ad Internet con velocità effettive sia in "up" che "down load" a partire da 2 Mbps, tipicamente in xDSL;
- chiara e condivisa (con il vertice aziendale e con le linee di business) identificazione di quali specifici servizi ICT (asset infrastrutturali e/o applicativi) si potrebbero passare o acquisire (se nuovi) in cloud, rispetto alla soluzione "on premise";
- mappa degli asset ICT in uso, incluse le licenze disponibili, il loro costo ed il periodo di validità;
- disponibilità degli attuali costi ICT: personale interno ed esterno, risorse ICT, contratti, ecc.
- piano evolutivo del sistema informatico per i prossimi 2-3 anni che dovrebbe includere la definizione dell'ICT Enterprise Architecture (EA) attuale e prevista nel prossimo futuro, allineata alle esigenze del business e del piano di sviluppo pluriennale dell'azienda/ente. In particolare l'ICT EA deve classificare/evidenziare quali sono le applicazioni e le informazioni vitali per il business, e quali gli standard di riferimento soprattutto per l'interoperabilità e la sicurezza;
- definizione policy per la sicurezza ICT e per la "compliance" alle normative in vigore e per le eventuali certificazioni;
- realistica ipotesi di budget per l'ICT per i prossimi 2-3 anni;
- analisi dei rischi;
- analisi dell'impatto organizzativo sulle Direzioni-Linee di business e sull'UOSI;
- analisi per la gestione dei cambiamenti.

6.2 Per scegliere il Fornitore ... riducendo i rischi

I criteri per la scelta di un fornitore di cloud sono in gran parte analoghi a quelli per la scelta di un outsourcer, e più in generale di un qualsiasi fornitore, cui si devono/dovrebbero aggiungere alcuni parametri-caratteristiche riassumibili in:
- trasparenza sui luoghi e sulle modalità del trattamento dei dati;
- esistenza di una policy pubblica del fornitore in merito alla riservatezza dei dati;

- personalizzazione della sicurezza lato utente;
- controllo del servizio per tutta la durata del rapporto;
- interoperabilità della soluzione cloud.

In maggior dettaglio e seguendo un processo a passi successivi, di cui alcuni possono essere in parallelo:

1. per ogni risorsa ICT che potrebbe passare o essere acquisita in cloud, elencare i possibili fornitori conosciuti ed operanti in Italia (la così detta "long list");
2. selezionare da questo primo elenco un sottoinsieme ristretto (chiamato "short list") scelto tramite una prima macro-analisi effettuata con visite on line ai loro siti, verifica della loro reputazione su Internet (blog di loro utenti, siti riviste on line, ecc.), passa parola da altre aziende/enti, contatti con associazioni, e così via. Per creare la "short list" dei possibili fornitori, verificare per ciascuno (elenco indicativo e non esaustivo):
   - i fornitori che potrebbero fornire due o più dei servizi ICT individuati;
   - la presenza di supporto tecnico e amministrativo in Italia;
   - il bilancio e il patrimonio: sono dati pubblici e disponibili;
   - la durata minima del contratto proposto;
   - il numero e tipo di clienti in Italia;
   - le certificazioni e accreditamenti;
   - la tipologia di servizi, architetture e piattaforme supportate;
   - il numero di Data Center (a livello mondiale) e disponibilità di banda complessiva per accedervi;
   - le policy di sicurezza e compliance;
   - i rapporti periodici e cruscotti on line forniti;
   - le garanzie e le penalità disponibili in funzioni delle SLA;
   - i contratti e listini con i prezzi standard (normalmente disponibili sul loro sito web);
3. specificare le caratteristiche di base/essenziali richieste per ogni servizio. Tra le caratteristiche da considerare, con l'appropriato livello di dettaglio (elenco indicativo e non esaustivo):
   - livello del servizio in termini di disponibilità, sicurezza e prestazioni, possibilmente dettagliate con SLA;
   - modalità di Backup e ripristino;
   - configurazione e gestione delle "patch";
   - modalità di "accounting" e possibilità di ripartizione dei costi tra unità organizzative;
   - individuazione degli inconvenienti, loro segnalazione, gestione e risoluzione;
   - gestione delle licenze;
   - reportistica periodica;
   - tempi e modalità pagamento;
4. contattare direttamente i fornitori della "short list" con l'elenco delle caratteristiche richieste per servizio e richiedere offerta scritta dettagliata con le varie clausole contrattuali;
5. nel caso si portassero in cloud infrastrutture, piattaforme ed applicativi gestiti localmente (on

premise), è fondamentale che sia dettagliato dal fornitore un preciso programma di migrazione degli ambienti e dei dati;

6. analisi e confronto delle offerte. Si devono raffrontare i prezzi a parità di livello di servizio erogato. Particolare attenzione deve essere posta all'eventuale programma di migrazione, alle misure di sicurezza, sia fisiche che logiche, alle SLA specificate ed alle clausole contrattuali. Per suggerimenti sugli aspetti legali e contrattuali si rimanda sia a §7 sia all'Allegato, ma è bene evidenziare che ci deve essere nel contratto la possibilità di rescissione, da parte del sottoscrittore, qualora i servizi erogati siano manifestamente e sistematicamente inferiori a quanto richiesto;
7. scelta finale del fornitore (o dei fornitori), firma del contratto ed attivazione del servizio.

6.3 Per gestire al meglio il Fornitore prescelto

Scelto il o i fornitori, occorre gestirli. Come per ogni contratto di terziarizzazione, il sottoscrittore deve sistematicamente verificare che l'erogazione del servizio da parte del fornitore prescelto soddisfi le sue esigenze e quanto sottoscritto nel contratto. Talvolta le informazioni del fornitore su KPI ed altri indicatori divergono rispetto al percepito/misurato da parte del sottoscrittore e dei suoi utenti. Spesso questo capita in quanto gli indicatori misurati da fornitore e sottoscrittore sono diversi. Tipico il caso del tempo di risposta: per l'utente finale deve essere end-to-end ed includere i tempi di attraversamento delle reti; per il fornitore, che non gestisce e non può influire sulle connessioni, il tempo di risposta è sovente valutato al punto d'uscita del Data Center.
Questo esempio evidenzia anche il problema dei termini e delle definizioni dei servizi, delle SLA, dei KPI e più in generale di quanto specificato nel contratto.
I principali suggerimenti, per una buona gestione del fornitore, includono, al di là delle metodologie e delle "best practice" presentate e dei dettagli specificati nel contratto (nell'Allegato un esempio per gli aspetti di sicurezza):

- verifica sistematica del livello di servizio come percepito dai clienti finali;
- controllo, sistematico o a campione, dell'ottemperanza delle SLA concordate, con analisi dai rapporti del fornitore e dei dati verificabili dagli eventuali cruscotti on line;
- efficacia, tempestività e trasparenza dell'interfaccia fornitore-sottoscrittore su qualsiasi tema, da quelli amministrativi-contrattuali a quelli tecnici, in particolare per la soluzione di guasti e di problemi nei servizi erogati;
- verifica dell'ottemperanza alle policy sulla sicurezza e sulla compliance, in particolare per la privacy (si veda Allegato);
- possibilità di effettuare delle verifiche e dei controlli di auditing, anche grazie a terze parti.

6.4 Per la chiusura del rapporto con il Fornitore

La chiusura del rapporto e l'eventuale passaggio ad altro fornitore o un ritorno ad una gestione interna del servizio ICT (on premise) può avvenire alla fine concordata del contratto o durante il suo

svolgimento per il recesso da una delle due parti causato da gravi inadempienze (sia lato fornitore che sottoscrittore).
Nel caso di recesso, la contrapposizione delle ragioni delle parti può arrivare in tribunale. Per il sottoscrittore è fondamentale poter migrare, avendo tutti i suoi ambienti e dati corretti, consistenti, integri e trasportabili su altre piattaforme per evitare il "locked-in". Se al momento della scelta del fornitore non sono stati considerati gli aspetti della portabilità, tenendo in particolar conto degli standard internazionali e della ICT EA, purtroppo difficilmente esistono "vie d'uscita" semplici, veloci e quindi poco costose.
Gli aspetti di recesso dovrebbero essere contemplati nel contratto stesso.
In un contratto di cloud, e più in generale di outsourcing, motivi di contenzioso possono essere frequenti. Occorre tenere presente che il passare all'azione legale è l'"ultima spiaggia": per l'azienda/ente l'obiettivo primario è garantire la continuità operativa con i livelli di servizio idonei.
Anche come fattore deterrente, ma comunque necessario per far valere le proprie ragioni a livello legale (se si hanno), è bene che il sottoscrittore documenti ed archivi tutti i problemi e/o i KPI con valori diversi, in senso negativo, rispetto a quelli specificati nelle SLA concordate.

7. Aspetti giuridici e contrattuali

I principali fornitori di cloud hanno contratti standard difficilmente modificabili, a meno di non essere un grande cliente in grado di stabilire contratti economicamente significativi.

7.1 Aspetti di compliance

Non sempre il contratto standard può essere accettabile dal sottoscrittore, soprattutto se quest'ultimo è soggetto a specifiche leggi, a livello nazionale ed internazionale, che impongono determinati trattamenti dei dati a livello sia di segretezza o riservatezza (normativa privacy, normativa suilla sicurra sul lavoro, L. 231 sulla responsabilità d'impresa, HACCP sulla salubrità degli alimenti, ecc.) sia per le sedi dove devono essere trattati. I dati possono essere soggetti a "disclosure" qualora i cloud server si trovino in un'area geografica con un diverso regime giuridico, e possono esserci responsabilità diverse da parte dei titolari del trattamento e diritti diversi per gli interessati.
Il primo serio problema da un punto di vista contrattuale e giuridico è quindi relativo al trattamento ed al trasferimento dei dati ed alla compliance alla normativa italiana sulla privacy.
La Direttiva 95/46/CE è l'origine di tutte le legislazioni sulla privacy, in Italia recepita dal D.Lgs. 675/1996 poi sostituita dalla 196/2003, cui sono seguiti vari, anche importanti aggiornamenti, elencati nella Tabella di fig. 7.1.
La normativa stabilisce che sono permessi i trasferimenti dei dati all'interno dell'Unione Europea (UE), mentre per paesi non UE sono permessi solo se:

- l'interessato ha manifestato il proprio consenso espresso e, se si tratta di dati sensibili, in forma scritta;

- è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;
- è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale.

decreto legislativo 28 maggio 2012, n. 69;
decreto legge 9 febbraio 2012, n. 5 convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35;
decreto legge 6 dicembre 2011, n. 201 convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214;
decreto legge 13 maggio 2011, n. 70, convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106;
legge 4 novembre 2010, n. 183;
legge 29luglio 2010, n. 120;
decreto-legge del 25 settembre 2009, n. 135 convertito, con modificazioni, dalla legge 20 novembre 2009, n. 166;
legge 4 marzo 2009, n. 15;
decreto-legge del 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14;
decreto-legge 25 giugno 2008, n. 112 convertito, con modificazioni, dalla legge 6 agosto 2008 n. 133;
decreto legislativo 30 maggio 2008, n. 109;
legge 18 marzo 2008, n. 48, ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno
decreto-legge 28 dicembre 2006, n. 300 convertito, con modificazioni, dalla legge 26 febbraio 2007, n. 17;
decreto-legge 12 maggio 2006, n. 173 convertito, con modificazioni, dalla legge 12 luglio 2006, n. 228;
decreto-legge 30 dicembre 2005, n. 273 convertito, con modificazioni, dalla legge 23 febbraio 2006, n. 51;
decreto legge 30 novembre 2005, n. 245 convertito, con modificazioni, dalla legge 27 gennaio 2006, n. 21;
decreto legislativo 7 settembre 2005, n. 209;
decreto-legge 27 luglio 2005, n. 144 convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155;
decreto-legge 30 dicembre 2004, n. 314 convertito, con modificazioni, dalla legge 1 marzo 2005, n. 26;
decreto-legge 9 novembre 2004, n. 66 convertito, con modificazioni, dalla legge 27 dicembre 2004, n. 306;
decreto-legge 24 giugno 2004, n. 158 convertito, con modificazioni, dalla legge 27 luglio 2004, n. 188;
decreto-legge 29 marzo 2004, n. 81 convertito, con modificazioni, dalla legge 26 maggio 2004, n. 138;
decreto legislativo 22 gennaio 2004, n. 42;
decreto-legge 24 dicembre 2003, n. 354 convertito, con modificazioni, dalla legge 26 febbraio 2004, n. 45.

Fig.7.1: I principali aggiornamenti della legge sulla privacy

Il trasferimento di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è altresì consentito quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato:

- individuate dal Garante anche in relazione a garanzie prestate con un contratto o mediante regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo. L'interessato può far valere i propri diritti nel territorio dello Stato, in base al presente codice sulla privacy, anche in ordine all'inosservanza delle garanzie medesime;
- individuate con le decisioni previste dagli articoli 25, paragrafo 6, e 26, paragrafo 4, della direttiva 95/46/CE del Parlamento Europeo e del Consiglio, del 24 ottobre 1995, con le quali la Commissione europea constata che un Paese non appartenente all'Unione Europea garantisce un livello di protezione adeguato o che alcune clausole contrattuali offrono garanzie sufficienti.

Tra le norme sulla privacy che hanno impatto sulle aziende/enti è imoportante menzionare il DPS, Documento Programmatico sulla Sicurezza, che documenta la politica (la policy) sulla sicurezza ICT che l'azienda/ente intende perseguire: doveva essere messo per iscritto nel caso si trattino dati sensibili, e dovevano essere dettagliate le modalità di protezione adottate per tali trattamenti, in accordo a quanto specificato nell'Allegato B del D.Lgs, il Disciplinare Tecnico sulle misure minime.
Importante come documento programmatico per specificare gli interventi e le misure tecniche ed organizzative di sicurezza per la protezione del trattamento dati, il DPS è **stato eliminato** con il Decreto Legge n. 5 del 9 febbraio 2012 (il così detto "Decreto semplificazioni 2012"), così come tutte le precedenti forme sostitutive, in termini di Autocertificazione e di DPS semplificato, introdotte dalla Legge 6 agosto 2008 n. 133 e successivamente modificate dalla Legge 12 luglio 2011, n. 106. Queste ultime normative supportavano il Provvedimento del Garante del 27 novembre 2008, disciplinante procedure semplificate, tra cui la stessa struttura del DPS, per i soggetti pubblici e privati che trattano dati personali solo per finalità amministrativo-contabile.

Si deve tener presente che le normative per la privacy europee e quelle statunitensi, dove esistono molti Data Center per il cloud, sono diverse, soprattutto a seguito dell' *USA Patriot Act*, emesso nel 2001 dopo l'attentato alle Torri Gemelle a New York, che per contrastare simili attacchi terroristici ha ristretto, anche fortemente, i diritti dei cittadini sulla privacy (peraltro già molto più lasca rispetto all'UE anche prima del 2001). Al fine di non rovinare i rapporti commerciali e di business tra UE e USA è stato siglato l'accordo chiamato *Safe Harbour*, tramite il quale sono autorizzate a trattare dati europei quelle aziende statunitensi che sottoscrivono l'adesione ai principi e alle normative europee, quali proteggere le informazioni trattate e assicurarne l'integrità, informare e garantire i diritti degli interessati, e così via.

Si ricordi infine che, anche se viene formalmente e totalmente delegata la responsabilità del trattamento dati e della sua sicurezza all'outsourcer, il titolare del trattamento del cliente-sottoscrittore (normalmente è il legale rappresentante) è comunque il responsabile finale che, in caso di ispezioni

e/o di contenziosi, deve comprovare di aver fornito tutte le indicazioni necessarie e di aver effettuato controlli sistematici sull'operato del fornitori. La legge sulla privacy, così come le altre che richiedono compliance ed hanno impatti sui sistemi ICT, prevedono l'inversione dell'onere della prova.

7.2 SLA e penali

Alcuni contratti standard prevedono alcune elementari SLA, come ad esempio la disponibilità del servizio in produzione in percentuale su un determinato arco temporale, normalmente l'anno solare. Un tipico esempio è garantire una disponibilità al 98%. A molti può sembrare un ottimo livello, non considerando che questo significa, in un anno, la possibilità di fermi non concordati del servizio per ben 7,3 giorni. Anche una affidabilità del 99% significa possibili fermi per 3,65 giorni.
Questi valori non sono in assoluto alti o bassi, dipende da quanto il processo supportato dal servizio in questione può rimanere fermo per un determinato arco temporale senza compromettere il business e/o l'immagine dell'organizzazione. Ed anche "senza compromettere", che impatto può avere un fermo non programmato per quella specifica azienda/ente? Occorre effettuare un'analisi del rischio.
Al di là di questo "prerequisito", trattato in § 6.1, gli indicatori delle SLA devono essere ben definiti, anche come termini linguistici per non lasciare adito a dubbi, e correttamente misurati. Ma i cruscotti on line ed i rapporti periodici sul funzionamento e sulle prestazione dei servizi in cloud sono forniti dall'outsourcer stesso: essi fornisco in maniera reale e trasparente ciò che succede o è successo? Si può fidare il sottoscrittore delle analisi, quando talvolta dai suoi utenti finali ha rendiconti funzionali e prestazionali ben diversi? Dipende da fornitore a fornitore e dai suoi strumenti di misura e rilevazione, ma i controlli si possono e si devono fare: a livello contrattuale deve essere, specificato che al sottoscrittore è consentito fare controlli con strumenti suoi o di terzi.

Per quanto concerne le penali, in alcuni contratti il fornitore, a fronte dell' erogazione di un livello di servizio al di sotto di una predefinita (contrattualmente) soglia, rimborsa il sottoscrittore. La presenza in un contratto di cloud computing di clausole con penali è percepita come un sintomo della correttezza e della trasparenza del fornitore. Una penale talvolta può comportare contenziosi tra le parti e difficilmente può ripagare dai danni di un disservizio, soprattutto se il disservizio, magari in maniera intermittente, si prolunga nel tempo.
Le clausole sulle penali devono pertanto essere molto chiare e dettagliate nel contratto, e soprattutto devono essere previste le modalità di recesso dal contratto, così come indicato in § 6.4, per evitare il problema più volte evidenziato del "locked-in".

Allegato: esempio contrattuale delle caratteristiche di sicurezza ICT per servizi cloud

Nel seguito è riportato un esempio di riferimento di caratteristiche tecniche-organizzative della sicurezza ICT che un buon contratto di cloud dovrebbe contenere.

Questo esempio può essere una traccia per verificare le offerte di fornitori cloud e per chiedere a loro precisazioni e chiarimenti.

Misure fisiche

Tutti i servizi ..... descritti funzionalmente e tecnicamente sul sito ..... / nei documenti ..... vengono erogati da apparecchiature installate presso i nostri datacenter in nostra completa gestione siti in:

- datacenter 1: .....
- datacenter 2: .....
- .....
- datacenter N: .....

L'accesso ai locali è regolato dalle procedure di sicurezza come da DPS predisposto ai sensi del D.Lgs 196/2003, separatamente riassunte.
I locali dei datacenter che ospitano le apparecchiature sono dotati delle seguenti infrastrutture:

- sorveglianza elettronica contro l'intrusione, l'incendio e anomalie ambientali critiche con segnalazione via radio, ..., e intervento in sede da parte di istituti di polizia privata autorizzati;
- sistema ridondante di controllo del clima delle sale macchine con allarmi locali e remoti (telelallarmi su istituto di vigilanza) su valori critici predefiniti;
- sistema di alimentazione ridondante su doppia rete di distribuzione a norme EIE-CE per ogni fila di armadi con prese e spine di sicurezza antistrappo e antifuoco;
- impianto di sicurezza dell'alimentazione mediante impianto di terra certificato conforme D.Lgs 81/2008 e successivi aggiornamenti, e separazione galvanica delle sorgenti;
- sistema di commutazione statica della sorgente duale di alimentazione per ogni armadio a servizio delle apparecchiature non dotate di alimentatori ridondanti;
- condizionamento statico dell'alimentazione per ogni modulo tramite gruppi di continuità statici on line:
  - datacenter 1 xxx KVA (...con riferimento di frequenza PLL)
  - .....
  - datacenter N xxx KVA

- Gruppo elettrogeno diesel ad alta autonomia, con avvio automatico e cicli di diagnostica bisettimanale automatici, dalla capacità di:
  - datacenter 1 xxx KVA
  - .....
  - datacenter N xxx KVA

Misure logiche

1. Ogni incaricato è dotato di password e username univoci e personali costituenti le sue credenziali di autenticazione.
2. Le password sono cambiate almeno ogni xx (max 3) mesi (per i dati sensibili/giudiziari e quelli ritenuti riservati dalla società, unitariamente definiti come dati particolari) con le procedure di cui alla legge. Per i dati personali comuni. sono cambiate almeno ogni xxx (max 6) mesi.
3. I codici identificativi personali sono disattivati in caso di non utilizzo per più di xxx (es. 6) mesi.
4. Ai dati particolari hanno accesso solo ed esclusivamente gli incaricati grazie ad un sistema di verifica che gli permette di accedere alle parti degli elaboratori in cui sono conservati i dati particolari.
5. I sistemi sono dotati dei seguenti software e delle componenti hardware riportate nella tabella qui di seguito,come sistemi di protezione:
   a. gli antivirus sono aggiornati con le nuove impronte virali ogni giorno;
   b. il firewall viene verificato periodicamente nella sua efficienza dagli amministratori di sistema che ne tengono traccia in apposito verbale;
   c. ai sistemi vengono applicate le c.d. “patch“ non appena le medesime sono disponibili e sufficientemente testate. Ai programmi acquisiti con licenza le patch vengono applicate dai fornitori come da specifici contratti;
   d. tutti i sistemi sono verificati dagli amministratori di sistema con cadenza xxxx (es. trimestrale).
6. La logica con cui sono stati scelti i sistemi di protezione è all’insegna della indipendenza dal venditore per le operazioni di aggiornamento/manutenzione e la disponibilità, per ogni componente di aggiornamenti e “patch“ nel minor tempo possibile.
7. L’azienda adotta le procedure di esecuzione di back up specifiche per ogni famiglia di servizi; le prestazioni minime di backup sono di seguito riportate:
   a. viene effettuato un backup giornaliero di tutti i dati presenti nei vari archivi, il backup viene effettuato tramite sistema/i ..... per gli archivi non strategici o comunque facilmente ricostruibili, con sistema/i ..... per gli altri. I dati di backup vengono conservati sia su un pool di dischi fissi sia su .....(es. Nastri rimovibili);
   b. i dati relativi a servizi di tipo .....(es: Cloud Server e Cloud Infrastructure), relativamente alla parte di gestione degli account, spazio web e dati contenuti negli eventuali database a richiesta di servizio da parte del cliente, hanno un backup ..... (es. settimanale) di tutti i dati presenti, effettuato ..... salvo specifica più restrittiva concordata con il cliente;

c. La procedura di backup viene avviata automaticamente attraverso il sistema centralizzato di gestione .....; lo stesso sistema centralizzato provvede all'audit sull'esecuzione e sulla correttezza dei cicli di backup.

8. I supporti di memorizzazione removibili contenenti dati particolari, se non utilizzati, sono distrutti o resi inutilizzati e inutilizzabili attraverso questi sistemi:
   a. gli unici dispositivi di memorizzazione in uso sono ..... (es: i nastri del sistema di backup), la loro distruzione alla fine dell'utilizzo specifico e/o del ciclo di vita avviene tramite formattazione non invertibile;
   b. qualora non siano recuperabili i dati, i supporti possono essere riutilizzati. I dati precedenti non sono recuperabili grazie ai seguenti sistemi: .....(es: formattazione non invertibile).

Le procedure di ripristino prevedono il recupero dei dati con le seguenti modalità ..... (es: un'opportuna area di "spool" non coincidente con l'area di produzione). I dati recuperati vengono poi sottoposti a validazione tramite ..... (es: ispezione manuale o automatica) e quindi re-immessi negli archivi di produzione.
L'eventuale interruzione di servizio non collegata con la perdita di dati ma derivante da problemi di connessione e/o da malfunzionamento dei dispositivi hardware (server, terminali, router) viene trattata in maniera autonoma dalla gestione/conservazione degli archivi.
Per le procedure di Backup, verifica, Disaster Recovery ci si avvale di .....
Il software assicura l'esecuzione dei backup in base alle politiche stabilite, verifica inoltre il contenuto delle copie di sicurezza e la loro congruità con gli archivi da proteggere.
Il sistema ..... si occupa inoltre dell'"assesment" delle procedure di Disaster Recovery per i dati oggetto del backup.
A livello fisico i dati sono conservati in ..... (es: cartucce di nastro), normalmente ospitate in .....(es: caricatori automatici) presso la sede .....

Analisi dei rischi

La profilazione seguente si riferisce alla prestazione xxxxx (es: di base) prevista dal servizio, è pos-

Tipo Danno Sistema Informatico	Conseguenza per i dati	Causa Danno	Valutazione del rischio in base alle cause
Distruzione o manomissione fisica o logica del sistema	Distruzione Non conformità alle caratteristiche originali Trattamento non autorizzato	Eventi non dipendenti dall'Azienda (fulmini, incendi, furti con danni) Eventi dolosi (Mano-missione interna o esterna, volontaria o non)	Rischio Basso
Intrusioni nel sistema dall'esterno dell'Azienda	Distruzione Non conformità alle caratteristiche originali Trattamento non autorizzato	Intrusione da parte di pirati informatici	Rischio Medio

sibile mitigare i rischi attraverso specifiche procedure e tecnologie negoziate in via specifica con il cliente

In caso di perdita dei dati il tempo stimato per il loro recupero sarebbe quello certificato dalla ditta fornitrice dell'assistenza hardware e software, stimabile comunque nel limite superiore di xx (es: 24) ore.

Individuazione e ruolo degli amministratori di sistema

E' stata predisposta una specifica procedura di compliance per quanto richiesto dal D. Lgs 196/2003 circa l'individuazione del ruolo, delle competenze e delle responsabilità degli amministratori di sistema; tale procedura è stata integrata con le indicazioni della *determina del Garante per la protezione dei dati personali del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)* attraverso la predisposizione di opportuni accorgimenti di tracciamento delle attività svolte e l'individuazione delle opportune figure professionali abilitate all'esecuzione delle attività di amministrazione dei sistemi nel rispetto delle linee guida proposte dall'autorità Garante.

NOTE

Via Caldera, 21 - edificio B
20153 Milano - Italia

www.seeweb.it