consip

quaderni consip

ricerche, analisi, prospettive

II [2011]

Cloud Security: una sfida per il futuro

MEF Ministero dell'Economia e delle Finanze

consip

quaderni consip

ricerche, analisi, prospettive

Matteo Cavallini

II [2011]

Cloud Security: una sfida per il futuro

MEF Ministero dell'Economia e delle Finanze

I 'Quaderni Consip' sono una testata registrata presso il Tribunale Civile di Roma
versione cartacea iscr. n. 11 del 16 gennaio 2009
versione elettronica iscr. n. 14 del 16 gennaio 2009

Direttore responsabile
Alessandro Grilli

Redazione
Consip S.p.A.
Via Isonzo, 19/e
00198 Roma
T + 39 06 85449.1

corporateidentity.consip@tesoro.it

I Quaderni Consip sono pubblicati all'indirizzo:
www.consip.it

Prefazione

Di cloud computing si è parlato e discusso molto nell'ultimo periodo. I fornitori e i fruitori dei servizi, le università e le istituzioni di ricerca si sono fatti promotori di numerosi convegni, analisi e studi, molti dei quali sono ancora in corso. Il problema della sicurezza è considerato cruciale per lo sviluppo del cloud computing. La caratteristica dei sistemi cloud di utilizzare risorse elaborative (intese in senso lato) che possono essere distribuite su siti diversi, allocate dinamicamente a seconda delle richieste e dei carichi di lavoro e condivise tra più clienti genera problematiche di sicurezza nuove rispetto a quelle dei tradizionali sistemi informativi.

Il settore pubblico, nell'avvicinarsi al cloud computing, deve tener conto di alcune ulteriori specificità che richiedono una maggiore attenzione per quanto riguarda: il rispetto della privacy, la proprietà dei dati, la conservazione nel tempo delle informazioni, l'indipendenza da soluzioni proprietarie e la possibilità di cambiare periodicamente i fornitori. Non affrontare e risolvere i problemi connessi a queste specificità costituisce un freno, forse un ostacolo insormontabile, alla diffusione del cloud computing nella PA.

Questo quaderno affronta il problema della "cloud security" prendendo in considerazione il sistema di governo e le policy da adottare, i controlli e le verifiche da effettuare, la conformità agli standard, l'utilizzo di architetture e tecniche per migliorare la sicurezza dei sistemi e delle applicazioni.

I potenziali vantaggi e benefici che i fornitori di servizi cloud prospettano sono messi a confronto con le preoccupazioni degli utenti e con i costi del superamento degli ostacoli che si frappongono alla loro diffusione. Una particolare attenzione è dedicata all'analisi dei rischi che le modalità di acquisizione e di erogazione dei servizi cloud pongono.

Queste analisi hanno portato a due conclusioni. Da un lato una singola amministrazione deve seguire un "approccio consapevole ai servizi cloud", con la definizione di una strategia, degli specifici requisiti, dei livelli di servizio necessari e di un Piano della Sicurezza. Dall'altro il settore pubblico nel suo complesso, anche sul piano transnazionale, è chiamato ad affrontare e risolvere problemi di carattere generale: una normativa aggiornata e adeguata, un piano di lotta al cyber crime, l'adozione di regole per la portabilità dei dati e delle applicazioni, la definizione di standard e di criteri di certificazione.

Per redigere questo Quaderno sono state impiegate competenze di eccellenza presenti in Consip sui temi della sicurezza, maturate nello sviluppo di progetti e nella gestione di sistemi complessi. Il primo utilizzo diretto di questo Quaderno riguarda i progetti già avviati da Consip per il Ministero dell'Economia e Finanze:

- la realizzazione di una private cloud per il Dipartimento del Tesoro;
- l'utilizzo di servizi public cloud di comunicazione unificata per il Dipartimento dell'Amministrazione Generale;
- l'utilizzo di servizi public cloud di collaborazione per la Ragioneria Generale dello Stato.

Inoltre dei contenuti del Quaderno possono avvantaggiarsi tutte le PA che intendano avviare progetti o acquisire servizi in chiave di cloud computing.

Gaetano Santucci

Indice

Indice delle figure e tabelle

Introduzione

"**Lady, I never walk into a place that I don't know how to walk out of.**"
Robert De Niro in "Ronin"

Questa memorabile battuta può essere presa a simbolo del corretto approccio verso il mondo cloud. In essa, infatti, sono contenute tutte quelle attitudini alla prudenza e alla sicurezza che dovrebbero fungere da guida nella preventiva valutazione dei cambiamenti di strategia dei sistemi IT.

Pensare prima ai possibili scenari e alle necessarie "exit strategy", rende percorribili anche i cambiamenti più impervi. Inoltre, la consapevolezza delle modalità di approccio a un cambiamento, sempre in via preventiva, consente di valutare pienamente i rischi che si corrono, scegliendo quindi i migliori criteri di garanzia.

Tutto ciò, nello specifico dei servizi cloud, permette di cogliere i vantaggi che questa modalità di fruizione dei servizi offre senza esporsi a inutili rischi e a potenziali danni.

In questo Quaderno sono quindi riportati e analizzati i migliori criteri di approccio al mondo del cloud computing con particolare riferimento alla cloud security, evidenziando i punti critici che devono essere affrontati e mettendo a fuoco le migliori pratiche che, allo stato, sono disponibili.

Questo Quaderno è organizzato in modo da dare nei primi paragrafi una visione complessiva delle caratteristiche e delle problematiche del cloud computing, per poi passare in rassegna i temi legati alla sicurezza. Viene così proposto un percorso logico che parte dai rischi legati al cloud, passa per le maggiori problematiche di sicurezza per arrivare alla definizione di un approccio consapevole al mondo della cloud security. Il Quaderno termina infine con una visione orientata al futuro e alle sfide che devono essere colte a livello globale per consentire al cloud computing di esprimere appieno tutto il potenziale di innovazione che tanta attenzione ha suscitato in tutto il mondo.

1. Il Cloud Computing

Il cloud computing non è un concetto totalmente nuovo; infatti, ha alcune relazioni con il grid computing e con altre tecnologie come l'utility computing, il clustering e i sistemi distribuiti in generale.

Citando ENISA – l'Agenzia Europea sulla Sicurezza informatica – il cloud computing è un nuovo modo di erogare servizi IT, non una nuova tecnologia. Questa circostanza ha comportato, tra l'altro, che esistano numerosissime definizioni di cloud computing.

I servizi cloud, inoltre, sono erogati generalmente da grandi provider internazionali; condizione che contribuisce a far confondere il concetto di outsourcing, erogato in modalità evolute, con il concetto di cloud computing.

Il cloud computing è diventato una parola d'ordine, quasi un modo di dire e, in maniera analoga a come si utilizzano altri slogan (come ad esempio Web 2.0), viene speso in molti contesti diversi e con molti significati differenti. Non sembra esserci, dunque, un vero consenso su che cosa davvero sia una "nuvola".

Nel seguito si cerca di fornire una definizione di cloud computing che sia il più possibile concreta e che metta correttamente in evidenza le caratteristiche peculiari di questo approccio innovativo.

1.1 La definizione del NIST

Il NIST (National Institute of Standards and Technology), ovvero l'ente di standardizzazione americano, ha prodotto la definizione di cloud computing che ha trovato il consenso più ampio. Dopo quindici versioni successive, questa definizione è stata considerata sufficientemente matura e, a gennaio 2011, è stata inserita in un documento ufficiale(1), ancorché in "Draft". Secondo il NIST, il cloud è un modello per abilitare un accesso ubiquo, conveniente e basato sulle effettive richieste, a risorse computazionali condivise (ad esempio reti, server, storage, applicazioni e servizi) secondo una modalità tale da consentire che queste ultime siano rapidamente allocate e rilasciate dagli utenti con il minimo sforzo gestionale o interazione con il fornitore. Questo modello prevede: cinque caratteristiche essenziali, tre modelli di servizio e quattro modelli di erogazione[1].

[1] Il NIST ha pubblicato a fine maggio 2011 un documento dal titolo "Cloud Computing Synopsis and Reccomendations", attualmente ancora in draft, che parte dalle definizioni dei servizi cloud e tratta molti dei temi affrontati in questo Quaderno. Il documento del NIST può essere utilizzato come utile riferimento per approfondire i temi più importanti del cloud computing. http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

1.1.1 Caratteristiche essenziali

Il NIST ha individuato cinque caratteristiche essenziali che devono essere sempre presenti quando si tratta di servizi cloud. Queste caratteristiche sono mostrate nella tabella seguente.

Tabella 1 – Le caratteristiche essenziali del cloud computing

Caratteristica	Definizione
On demand self-service	L'utente ha la facoltà, unilaterale, di approvvigionarsi di risorse computazionali, come ad esempio tempo macchina e storage di rete, automaticamente, senza che ci sia la necessità di una interazione umana con i fornitori del servizio.
Broad network access	Le risorse sono accessibili via rete attraverso meccanismi standard che promuovono l'uso di piattaforme client eterogenee (ad esempio smartphone, laptop, PDA, ecc.)
Resource pooling	Le risorse computazionali del fornitore sono messe in comune per servire molteplici utenti, usando uno schema multi-cliente, che gestisce risorse fisiche e virtuali dinamicamente assegnate e riassegnate, in accordo con le indicazioni degli utenti. Gli utenti, in alcuni casi, possono avere la facoltà di indicare la locazione fisica delle risorse, ma solo a un elevato livello di astrazione (ad esempio Stato o data center). Per risorse si intendono: lo storage, le capacità elaborative, la memoria, le capacità di rete e le macchine virtuali.
Rapid elasticity	Le risorse sono in grado di essere allocate rapidamente ed elasticamente, in alcuni casi automaticamente, per soddisfare, in maniera veloce, le maggiori o minori richieste degli utenti. Gli utenti hanno l'impressione che le risorse disponibili siano illimitate e che possano essere acquistate in qualsiasi quantità e in qualsiasi momento.
Measured service	I sistemi cloud controllano automaticamente e ottimizzano l'utilizzo delle risorse tramite strumenti di misura basati su adeguati livelli di astrazione (ad esempio storage, capacità elaborativa, banda, e account utente attivi). L'utilizzo delle risorse può essere monitorato, controllato ed elaborato, in piena trasparenza sia per il provider sia per l'utente del servizio.

1.1.2 I "Service model"

Iaas, PaaS e SaaS sono tre acronimi entrati a far parte del linguaggio dei servizi IT per indicare i possibili modelli di erogazione dei servizi cloud. Per questi modelli il NIST ha fornito le definizioni mostrate nella tabella seguente.

Tabella 2 – I "Service model"

Service model	Definizione
Iaas – Cloud Infrastructure as a Service	I clienti possono rifornirsi di capacità elaborativa, storage, reti e altre risorse IT di base. Su queste risorse, i clienti possono caricare ed eseguire software di base e applicativo. I clienti però non gestiscono o controllano l'infrastruttura cloud ma si limitano alla gestione dei sistemi operativi, dello storage, delle applicazioni caricate e, a volte, di un insieme predeterminato di risorse di rete.
PaaS – Cloud Platform as a Service	I clienti hanno la possibilità di sviluppare in proprio applicazioni cloud basate su strumenti e linguaggi di programmazione supportati dal fornitore o utilizzare applicazioni di mercato compatibili. I clienti non gestiscono l'infrastruttura cloud né le componenti di rete, i server, i sistemi operativi o lo storage ma hanno il controllo sulle applicazioni utilizzate e, alcune volte, sulle configurazioni degli ambienti di hosting.
SaaS – Cloud Software as a Service	I clienti possono utilizzare le applicazioni messe a disposizione dal fornitore nell'infrastruttura cloud. Le applicazioni sono accessibili da varie tipologie di apparati attraverso l'interfaccia tipica del dispositivo che stanno utilizzando, ad esempio un browser nel caso di un "thin client" o una "App" nel caso di un tablet o di uno smatphone. I clienti non gestiscono l'infrastruttura cloud né le componenti di rete, i server, i sistemi operativi, lo storage o le capacità dell'applicazione. Alcune possibili eccezioni sono limitate a specifiche configurazioni dell'applicazione legate all'utente.

1.1.3 I modelli di erogazione

Quando si parla di servizi cloud, ci si riferisce generalmente al modello di erogazione di tipo "Public Cloud" che è solo una delle possibili soluzioni che possono essere adottate, come mostra la tabella dei modelli di erogazione delle cloud defniti dal NIST.

Tabella 3 – I modelli di erogazione

Caratteristica	Definizione
Private cloud	L'infrastruttura cloud è dedicata a una sola organizzazione. Una cloud privata può essere gestita dall'organizzazione stessa o da un outsourcer e può essere fisicamente collocata in strutture interne o esterne all'organizzazione.
Community cloud	L'infrastruttura cloud è condivisa da molteplici organizzazioni e supporta una specifica community che condivide alcuni assunti di base come ad esempio la mission, i requisiti di sicurezza, le policy e gli approcci per la compliance. Può essere gestita direttamente dalle organizzazioni o da un outsourcer e può essere fisicamente collocata in strutture interne o esterne all'organizzazione.
Public Cloud	L'infrastruttura cloud è resa disponibile al pubblico o a vasti settori privati ed è di proprietà di un'organizzazione che vende servizi cloud.
Hybrid cloud	L'infrastruttura cloud è composta da due o più modelli di erogazione diversi, che, pur rimanendo entità a sé stanti, sono collegati tra loro da tecnologie - proprietarie o standard – che consentono la portabilità dei dati e delle applicazioni.

La seguente Figura mostra alcune tra le possibili casistiche che si possono verificare con i vari "Service Model" delle cloud. Queste quattro casistiche sono quelle che saranno approfondite nel presente documento.

Tabella 4 - Matrice delle casistiche dei Modelli di Erogazione

	Infrastruttura gestita da un Provider	Infrastruttura posseduta da un Provider	Infrastruttura Ubicata
Public Cloud	Esterno	Esterno	Esternamente
Community Cloud Est	Esterno	Esterno	Esternamente
Community Cloud Int	Interno	Interno	Internamente
Private Cloud	Interno	Interno	Internamente

1.2 Gli attori

Per il modello cloud, il NIST definisce anche gli "attori" coinvolti nell'erogazione e nell'utilizzo del sevizio. Si tratta della rivisitazione dei ruoli degli attori IT in chiave cloud. per avere una corretta rappresentazione delle dinamiche presenti in tale contesto, Secondo il NIST[2] gli attori da considerare sono:

- **Cloud Service Provider** (CSP), fornisce i servizi ai Cloud Service Consumer a costi e livelli di servizio concordati. Il provider gestisce l'infrastruttura tecnica necessaria per l'erogazione dei servizi e produce i dati e la reportistica prevista per la fatturazione; è il nuovo ruolo del fornitore di servizi IT;
- **Cloud Service Consumer** (CSC). è una organizzazione o un individuo che ha sottoscritto un contratto per l'erogazione di servizi con un Cloud Service Provider. Al CSC restano in capo sia le responsabilità legate alla definizione dei requisiti dei servizi e alla verifica della loro rispondenza alle esigenze, sia quelle relative all'esecuzione delle attività di amministrazione per la fruizione dei servizi stessi (quali ad esempio la gestione delle identità dei propri utenti); si rileva che questo nuovo ruolo dell'utente è molto più ampio di quello tradizionale; il NIST osserva che, in alcuni casi, il CSC può acquisire servizi da un CSP per integrarli e poi offrirli a terzi, assumendo così anche il ruolo di CSP;

- **Cloud Service Developer**, è la figura che si occupa della progettazione e dell'implementazione delle componenti di un servizio cloud. Il Cloud Service Developer descrive il servizio e quindi interagisce con il CSP per implementare le varie componenti definite, sulla base del template adottato. Il CSP può, in alcuni casi, personalizzare i servizi prima di renderli disponibili; corrisponde ad una sorta di "mediatore" tra CSP e CSC;
- **Cloud Service Distributor**, si occupa di fornire connettività e trasporto per applicazioni e servizi tra i fornitori di servizi cloud e i consumatori.

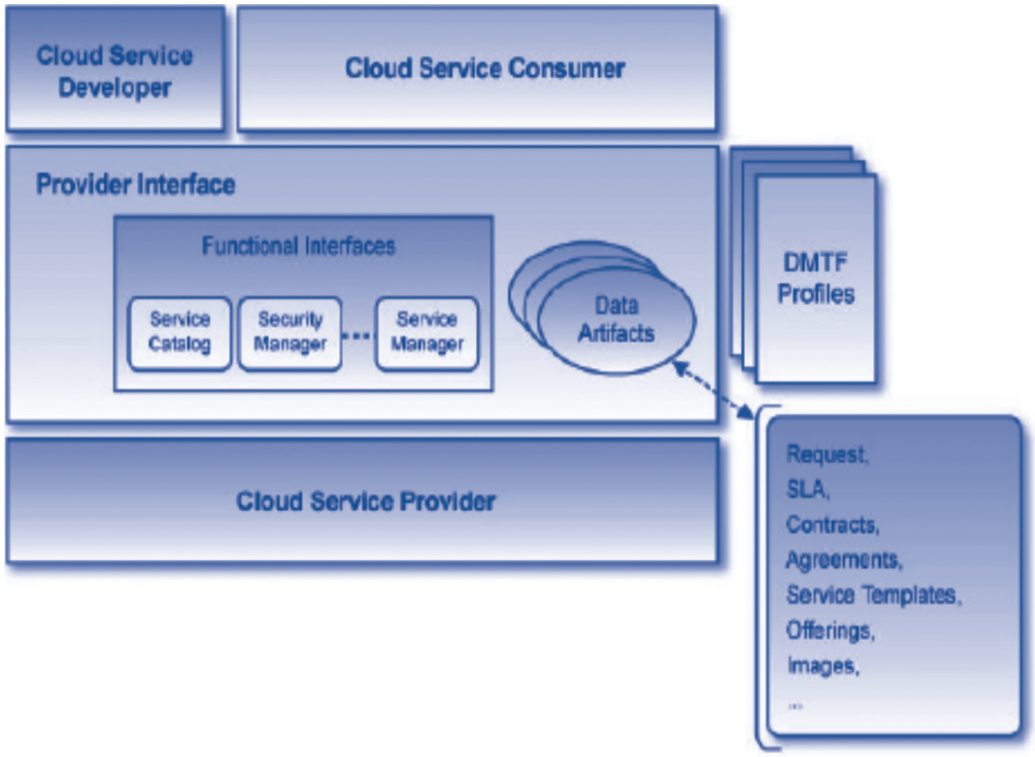
Nel caso di una cloud privata, CSC e CSP possono essere espressi da in un unico soggetto che tramite una propria articolazione (tipicamente la struttura organizzativa che si occupa di ICT) fornisce servizi cloud a clienti interni (le altre strutture aziendali). Nel caso più ampio di una cloud di community o di una cloud pubblica, invece, CSC e CSP sono rappresentati da entità differenti. Data questa indeterminazione, nel testo, qualora non altrimenti specificato, le figure di CSC e CSP devono essere intese nell'accezione più ampia possibile, focalizzando l'attenzione sulla funzione svolta e non sul soggetto reale che la svolge.

1.3 Il modello architetturale di riferimento

È utile schematizzare in un modello di riferimento le relazioni fra le componenti dei servizi cloud e i principali attori. A questo scopo si descrivono brevemente i modelli prodotti dalla "Distributed Management Task Force" (DMTF), gruppo nato per lo sviluppo di standard internazionali di interoperabilità, e quello della Cloud Security Alliance (CSA), organizzazione no profit nata per promuovere le "best practice" di sicurezza nel mondo del cloud computing.

Fig. *1 – DMTF Cloud Service Reference Architecture*

Distributed Management Task Force (DMTF): Cloud Service Reference Architecture



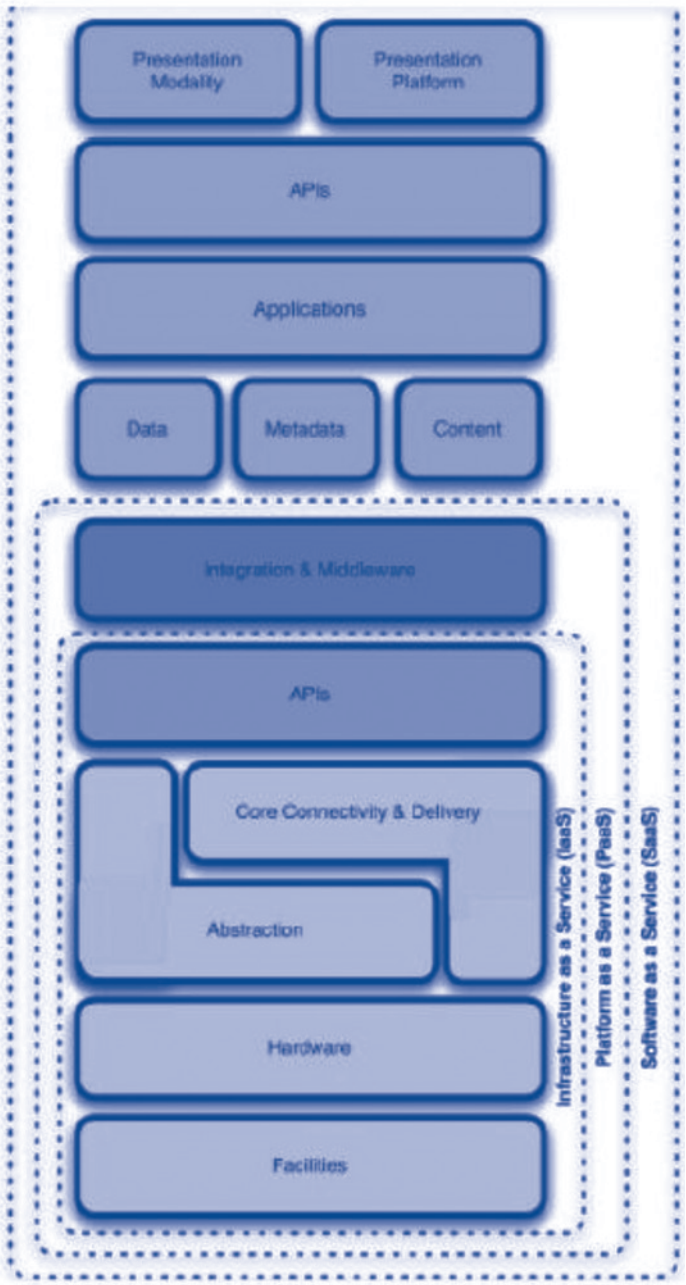
Il modello della DMTF è particolarmente utile per focalizzare alcuni fattori chiave come ad esempio gli attori, le interfacce, i dati e i profili. Nella figura 1 sono evidenziati, secondo la visione della DMTF, i tre principali attori – Cloud Service Provider, Cloud Service Consumer e Cloud Service Developer – e le relazioni che li legano ai profili e ai dati attraverso le interfacce messe a disposizione dal Provider.

Come si può vedere, il Cloud Service Developer è un attore che si posiziona tra il CSP e il CSC per effettuare un'attività di progettazione, realizzazione e monitoraggio dei servizi che vengono erogati.

Ogni organizzazione può, a seconda delle situazioni, assumere ognuno dei tre ruoli previsti dal modello.

Le interfacce funzionali sono rappresentazioni delle API fornite ai Consumer e ai Developer per richiedere, distribuire, amministrare e infine utilizzare i servizi cloud. Infine i "DMTF profile" sono profili specializzati delle interfacce che vengono messi a disposizione di specifiche figure (ad esempio, del security manager o del responsabile dell'esecuzione contrattuale) per avere un accesso dedicato alle funzioni di interesse.

Fig. *2 – CSA Cloud Reference Model*



Il modello della CSA, nasce con lo scopo di mettere in evidenza le dipendenze delle funzioni di sicurezza e i possibili rischi nei tre "Service Model". Come mostra la figura 2, la CSA vede il modello IaaS come il fondamento di tutti i servizi cloud, con gli altri modelli PaaS e SaaS che vengono ad essere costruiti sopra il primo.
Questo modello evidenzia che il modello SaaS fornisce le funzionalità più integrate e le minori possibilità da parte degli utenti di modificare il servizio, mentre gli altri modelli consentono maggiori gradi di libertà nella costruzione delle caratteristiche desiderate dal cliente.

Ovviamente, a maggiori gradi di libertà corrispondono maggiori oneri di gestione per il cliente stesso che, ad esempio, nel caso dello IaaS dovrà occuparsi di gestire tutta la pila del software, a partire dal sistema operativo, comprese le relative componenti di sicurezza[2].

1.4 I possibili scenari

L'Open Cloud Manifesto e il Cloud Computing Use Case Discussion Group[3] hanno sviluppato un documento(3) che, tra le altre cose, mette in evidenza i possibili scenari di utilizzo delle cloud. Tra questi, i più pertinenti alla presente trattazione sono:

1. **Enterprise to Cloud**, questo scenario vede l'utilizzo di servizi cloud da parte di un soggetto privato o pubblico per i propri processi interni. Questo utilizzo potrebbe essere il più comune nelle fasi iniziali di approccio al mondo cloud proprio per la maggiore semplicità che implica rispetto agli altri scenari. In linea di massima i possibili utilizzi delle cloud in questo scenario sono:
   - Storage as a Service;
   - Provisioning di risorse elaborative per la gestione dei picchi di richieste;
   - Software as a Service;
   - Provisioning di DB nell'ambito di un processo elaborativo;

[2] Per approfondire le relazioni di responsabilità che legano i CSP e i CSC nei vari "service model", può essere utile fare riferimento al capitolo 6 "Reccomendations and key messages", paragrafo "Division of responsibilities" del documento "Cloud Computing – Benfits, risks and reccomendations for information security" prodotto da ENISA

[3] Questi due gruppi annoverano alcuni tra i maggiori player internazionali (pubblici, privati e accademici) del mondo cloud e perseguono le finalità di creare le condizioni affinché i servizi cloud siano "open" al pari degli altri servizi IT.

2. **Enterprise to Cloud to End User**, questo scenario vede l'utilizzo delle cloud da parte di un soggetto privato o pubblico per fornire dati o servizi agli utenti finali. Gli utenti finali possono essere interni o esterni al CSC[4];
3. **Enterprise to Cloud to Enterprise**, questo scenario vede l'interazione di due soggetti privati o pubblici che utilizzano la stessa cloud per scopi comuni (ad esempio supply chain management);
4. **Private Cloud**, questo scenario sostanzialmente è composto dall'unione dei modelli di Private Cloud e Community Cloud definiti dal NIST. Viene normalmente adottato da grandi soggetti pubblici o privati che hanno processi caratterizzati da grandi picchi di richieste elaborative o grandi richieste di flessibilità e velocità nel deployment di nuovi servizi[5].

Vale la pena di notare che, per le finalità di questo Quaderno, tutti gli scenari riferiti alle Enterprise possono essere ritenuti applicabili al più generale concetto di ente, contenendo quindi anche tutte le PA centrali e locali.

[4] Un'interessante applicazione di questo concetto è stata realizzata nel 2009 dal Ministero dell'Economia, del Commercio e dell'Industria giapponese che ha prodotto una piattaforma SaaS (J-SaaS composta da circa 50 applicazioni in settori quali la gestione finanziaria, la tenuta dei libri contabili, la gestione degli adempimenti fiscali, ecc) dedicata alle piccole e medie imprese al fine di ridurre gli oneri legati ai costi operativi e agli investimenti per l'ICT.

[5] In quest'ambito deve essere ricordato il progetto di realizzazione di una cloud privata all'interno del Dipartimento del Tesoro (DT) del Ministero dell'Economia e Finanze. Questo progetto, curato dal DT-UCID in sinergia con Consip, presenta positive ricadute sull'efficienza del Dipartimento attraverso la realizzazione di: applicazioni cloud, infrastrutture (disponibili in modalità PaaS e IaaS) e nuovi processi. Inoltre si propone in quest'ambito come esperienza pilota per la PA italiana.

2. Il Cloud e il mercato

Attualmente, il mercato dell'offerta dei servizi ICT sta mettendo in campo molte risorse per far percepire ai possibili clienti i numerosi vantaggi che possono derivare dalla sottoscrizione di un servizio cloud.

Questi indubbi benefici sono da ascrivere fondamentalmente:

- ad aspetti di tipo economico-finanziario;
- al superamento di molte inerzie e dei conseguenti ritardi che accompagnano il rilascio di nuovi servizi;
- a una generale maggiore efficienza nella gestione e nella sicurezza dei servizi.

A fronte delle numerose ed efficaci campagne di marketing che accompagnano i cospicui investimenti e le aspettative di crescita dei fornitori, è necessario che i potenziali CSC siano preparati a cogliere queste opportunità e i conseguenti benefici, effettuando le analisi e assumendo le decisioni sulla base di una completa comparazione di tutti i pro e i contro delle possibili soluzioni.

Una ricerca(4) effettuata da ENISA sul modo in cui le piccole e medie imprese valutano i servizi cloud mostra chiaramente che le maggiori preoccupazioni per l'adozione di tali servizi sono legate alla sicurezza (perdite di riservatezza, disponibilità e integrità dei dati, perdita di controllo su dati e applicazioni), alle problematiche di rispetto della disciplina per la protezione dei dati personali ed alla disomogeneità dei requisiti legali che devono essere soddisfatti non solo all'esterno, ma anche all'interno, della stessa Unione Europea. Avere, quindi, una piena consapevolezza dei possibili punti deboli e delle maggiori problematiche di sicurezza e legali dei servizi cloud, consente di effettuare le migliori scelte, evitando i possibili rischi con l'adozione di efficaci contromisure[6].

[6] A questo proposito può essere utile consultare il documento "Security of Cloud Computing Providers Study" pubblicato dal Ponemon Insitute nell'aprile del 2011. Questo documento contiene un sondaggio sulle tematiche di sicurezza nel mondo cloud effettuato tra oltre 100 CSP americani e 24 europei.
http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf

2.1 Vantaggi e benefici

Come messo in evidenza anche dal documento "Moving to the Cloud"[5] a cura del Cloud Computing Use Case Discussion Group, l'adozione di servizi cloud comporta sensibili vantaggi economico-finanziari quali ad esempio:

- la capacità di diminuire i costi di start-up di un sistema;
- la possibilità di dimensionare sistemi e applicazioni sulla base dei normale carico di lavoro gestendo i picchi di carico tramite la capacità di scalare tipica delle infrastrutture cloud;
- la capacità di ottimizzare i costi sia in termini di risorse computazionali, sia in termini di risorse di esercizio (logistica, consumi elettrici, raffreddamento, ecc.), sia in termini di risorse umane di gestione;
- la possibilità di ridurre gli investimenti (CAPEX) a fronte di maggiori spese correnti (OPEX).

Inoltre si possono ottenere ulteriori vantaggi dal punto di vista operativo:

- la drastica riduzione dei tempi di realizzazione e di messa in esercizio di nuovi servizi;
- la rapida capacità di scalare le risorse rapidamente per venire incontro a nuove esigenze o a requisiti modificati;
- il rapido ed efficiente provisoning e deprovisioning delle risorse;
- l'ottimizzazione dei consumi energetici sia per le esigenze computazionali sia per le esigenze di refrigerazione dei centri di elaborazione.

Per l'obiettivo di questo Quaderno, però, è opportuno focalizzarsi sui benefici legati alla sicurezza. Da questo punto di vista, l'adozione di servizi cloud può portare a diversi benefici, tra i quali, la possibilità di fruire di:

- soluzioni di sicurezza superiori ai propri standard interni;
- organizzazioni di sicurezza difficilmente realizzabili nelle proprie realtà interne;
- servizi standard e aperti che superano gli approcci proprietari tipici delle soluzioni adottate in ambiti più ristretti.

Infatti, i fornitori di servizi cloud possono fare leva sulle economie di scala per riuscire a realizzare soluzioni molto più evolute e performanti rispetto a quelle che sono implementabili, a parità di investimenti, da più soggetti su una molteplicità di realizzazioni di minori dimensioni. Le caratteristiche che possono avere le soluzioni cloud sono, ad esempio: architetture ridondate e geograficamente distribuite, servizi di

monitoraggio ad elevata granularità e automazione, tempi molto ridotti di reazione agli incidenti, capacità di scalare risorse per rispondere a eventuali attacchi di tipo DDoS, migliori realizzazioni di sicurezza fisica e organizzativa, omogeneità e coerenza delle varie soluzioni di sicurezza.

Per quanto riguarda infine l'apertura delle soluzioni, i CSP, dovendo rivolgersi a molteplici soggetti diversi, hanno la necessità di orientare i propri servizi verso modalità di erogazione standard e, qualora possibile, aperte. Ciò comporta, dal punto di vista della sicurezza, una maggiore capacità di controllo diretto e indiretto sulle infrastrutture con indubbi riflessi positivi sulle capacità di esecuzione.

2.2 Problematiche e preoccupazioni

A fronte dei vantaggi e dei benefici descritti, i servizi cloud, presentano ancora alcuni problemi, nel campo della sicurezza e non solo. Una maggiore comprensione di queste problematiche può essere utile sia ai CSC (in atto o potenziali), che possono adottare opportune contromisure, sia ai CSP che, prendendone atto, possono lavorare per mitigarne gli effetti e migliorare in generale i servizi erogati.

La preoccupazione più diffusa in relazione all'utilizzo di servizi cloud è conosciuta come "lock-in" e si riferisce a tutti quei casi in cui una migrazione del servizio da un fornitore a un altro (o un successiva internalizzazione) risulta difficoltosa o, addirittura, impossibile. Questo rischio, che sarà analizzato più a fondo nei successivi paragrafi, è valutato da molti osservatori e dal mercato stesso come uno di quelli a maggiore probabilità e a impatto maggiore. Certamente, prima di sottoscrivere un qualsiasi contratto di servizio cloud, ogni potenziale cliente dovrebbe effettuare opportune verifiche per chiarire l'esatto impatto di questo rischio sul servizio che sta sottoscrivendo, definendo le modalità (tra le più importanti possono essere ricordate: il supporto fornito dal CSP, le tempistiche previste e gli eventuali costi) per riportare il servizio 'in house' (cd. 'Transfer Back') o migrarlo verso un altro fornitore.

Un'altra preoccupazione molto diffusa per i CSC riguarda la perdita di governance su dati e servizi. Il verificarsi di questa condizione può, in alcuni casi, comportare anche una perdita di conformità a standard come la ISO 27001 o la PCI-DSS. La perdita di governance sui dati e sulle applicazioni può altresì risultare in un significativo rischio di possibili violazioni della normativa per la protezione dei dati personali, con effetti di rilievo anche penale (ad esempio l'inappropriata adozione delle misure minime di sicurezza).

Le condizioni per le quali questa circostanza può verificarsi sono da ricercare nel fatto che i CSP, dovendo servire molteplici CSC, molto spesso scelgono di mettere a disposizione solamente un set minimo standard di strumenti di governo sulle funzionalità di sicurezza. A questa limitazione si aggiunge anche, in alcuni casi, l'impossibilità di effettuare audit e verifiche da parte del CSC. Quindi, nonostante le misure di sicurezza implementate dai fornitori siano generalmente di alto livello e in certi casi addirittura superiori a quelle che potrebbero essere realizzate dai singoli clienti, la carenza di governance sul proprio dominio si può trasformare in una mancanza di capacità di controllo e, in ultima analisi, di mantenimento di conformità a standard internazionali.

Infine, il cosiddetto "Multi-tenant model" pone un'altra serie di problematiche di riservatezza che devono essere prese in considerazione. Avere i propri dati in condivisione con altri clienti, oltre che con la struttura del fornitore, propone degli scenari abbastanza inediti dal punto di vista della sicurezza, tanto più che le separazioni di ambienti tra diversi clienti sono normalmente solamente "virtuali", rendendo quindi possibili, almeno in via teorica, attacchi - o errori di configurazione - che si propagano da un cliente all'altro dello stesso fornitore di servizi cloud. In questi ambienti "misti" una particolare attenzione va posta alla sicurezza dei dati che potrebbero essere più facilmente acceduti o modificati in maniera impropria o non consentita, con un impatto sulle responsabilità in materia di protezione dei dati personali già evidenziato nel paragrafo precedente.

3. Il Cloud e l'e-government

Gli enti governativi di tutto il mondo stanno riservando una grande attenzione ai servizi di cloud computing. Tale attenzione è dovuta, in massima parte, ai vantaggi che vengono percepiti anche dai CSC privati. Molti enti governativi che si occupano di verificare e governare i processi di sviluppo degli strumenti IT pubblici hanno quindi dedicato le loro analisi al cloud computing nel tentativo di stabilire le condizioni per le quali le Amministrazioni pubbliche possano accedere con profitto a queste tipologie di servizi. Tra le molte, vale la pena di ricordare le analisi statunitensi ed europee.

3.1 Gli approcci degli Stati Uniti e dell'Europa

Negli Stati Uniti, su un preciso impulso del Presidente Barack Obama, sono state redatte le strategie di sviluppo dei servizi cloud da mettere al servizio delle Agenzie federali allo scopo di aumentare l'efficienza e contenere i costi[7]. In quest'ottica, a novembre 2010, la GSA (Government Service Administration) ha messo a punto il programma FedRAMP(6) (Federal Risk and Authorization Management Program), programma governativo di valutazione di sicurezza, autorizzazione e monitoraggio continuo per i servizi di cloud computing delle Agenzie federali. Secondo gli obiettivi di questo programma, la decisione di adottare le tecnologie cloud deve essere basata, oltre che su elementi di natura economica, sulla valutazione del rischio e non su considerazioni di tipo tecnologico. Quindi, per il varo di una tale decisione, sono richiesti i contributi di tutte le parti interessate tra cui quelli del CIO (Chief Information Officer), del CISO (Chief Information Security Officer) e del responsabile della privacy. Una volta che la decisione è stata presa, gli enti governativi devono quindi determinare le modalità di implementazione più consone ai loro livelli di sicurezza.

L'approccio utilizzato nel programma FedRAMP fornisce un quadro di autorizzazione congiunta dei servizi di cloud computing e un modello comune di analisi e gestione del rischio riconosciuto dagli enti governativi federali. Questo modello unico di analisi e gestione del rischio, che prevede una "baseline" condivisa di sicurezza per le tecnologie cloud, consente di cogliere i benefici del cloud, rendendo consistenti tra loro le varie soluzioni realizzate all'interno delle strutture governative. Il modello di rischio comune permette, inoltre, alle strutture governative statunitensi approcci del tipo "*approve once and use often*" ottimizzando i benefici e garantendo al contempo l'uniformità delle soluzioni. In ultima analisi, FedRAMP consente alle

[7] Vivek Kundra, Chief Information Officer (CIO) dell'amministrazione pubblica statunitense, ha prodotto la "Federal Cloud Computing Strategy" in cui, tra le altre cose, viene ribadito che le nuove iniziative IT federali dovranno prendere in esame le soluzioni cloud based in via prioritaria rispetto ad ogni altra opzione. http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

Agenzie federali di giovarsi di:

- un approccio interdipartimentale controllato;
- un'applicazione coerente dei requisiti di sicurezza federali;
- una gestione del rischio consolidata;
- una maggiore efficienza e un consistente risparmio sui costi di gestione.

In Europa ENISA, a gennaio 2011, ha prodotto un documento[7] per guidare le Pubbliche Amministrazioni europee verso un'adozione "consapevole" dei servizi cloud. Questo documento ha il principale obiettivo di:

- evidenziare i pro e i contro, per quanto riguarda la sicurezza delle informazioni e la resilienza dei diversi "*Service Model*" in relazione ai differenti "modelli di erogazione";
- guidare gli enti pubblici nella definizione dei propri fabbisogni di sicurezza e resilienza rispetto ai servizi di cloud computing.

Inoltre, questa relazione fornisce un sostegno agli Stati membri dell'Unione Europea nella definizione della loro strategia di cloud nazionale per quanto riguarda la sicurezza e la resilienza. Nel documento viene sottolineata l'importanza della fase di raccolta dei requisiti, che viene considerata il fattore chiave per adottare la soluzione che meglio si adatta alle esigenze delle PA.

Inoltre, il documento di ENISA propone un utile modello decisionale, dedicato ai livelli dirigenziali delle Amministrazioni pubbliche, per l'approccio ai servizi di cloud computing. Questo modello sarà meglio analizzato nel successivo capitolo 6.

3.2 Vantaggi e preoccupazioni

Il cloud computing possiede il potenziale per offrire alle Amministrazioni pubbliche notevoli benefici e miglioramenti nella gestione dei servizi IT, tra cui:

- livelli di disponibilità e affidabilità dei servizi generalmente molto elevati;
- livelli di sicurezza potenzialmente maggiori;
- maggiore valore per gli investimenti.

Questi miglioramenti sono dovuti:

- all'infrastruttura tipica delle cloud (che consente di arginare i problemi dovuti a malfunzionamenti e a picchi di richieste);
- alla generale diffusione di maggiori competenze di sicurezza all'interno delle organizzazioni dei CSP;
- alle economie di scala ottenibili nelle forniture di servizi cloud.

Come messo in evidenza nella "Federal Cloud Computing Strategy"[8] in modo molto chiaro, nel settore pubblico i maggiori benefici sono relativi: all'efficienza, all'agilità e all'innovazione

Fig. *3 – Cloud Benefits (Fonte Federal Cloud Computing Strategy)*

EFFICIENCY	
Cloud Benefits	**Current Environment**
• Improved asset utilization (server utilization > 60-70%) • Aggregated demand and accelerated system consolidation (e.g., Federal Data Center Consolidation Initiative) • Improved productivity in application development, application management, network, and end-user	• Low asset utilization (server utilization < 30% typical) • Fragmented demand and duplicative systems • Difficult-to-manage systems
AGILITY	
Cloud Benefits	**Current Environment**
• Purchase "as-a-service" from trusted cloud providers • Near-instantaneous increases and reductions in capacity • More responsive to urgent agency needs	• Years required to build data centers for new services • Months required to increase capacity of existing services
INNOVATION	
Cloud Benefits	**Current Environment**
• Shift focus from asset ownership to service management • Tap into private sector innovation • Encourages entrepreneurial culture • Better linked to emerging technologies (e.g., devices)	• Burdened by asset management • De-coupled from private sector innovation engines • Risk-adverse culture

È però evidente che questi benefici possono essere raggiunti solamente in presenza di un livello soddisfacente di sicurezza e resilienza dei servizi cloud. Le condizioni minime per il raggiungimento di tale livello di sicurezza sono:

- la chiara identificazione dei requisiti per i servizi;
- la chiara definizione di livelli di servizio considerati "accettabili";
- il monitoraggio continuo dei parametri di sicurezza e resilienza;
- il coordinamento tra le funzioni dedicate al monitoraggio, alla gestione degli incidenti e alla gestione della continuità.

Per converso le maggiori preoccupazioni sono legate principalmente alla necessità di rinunciare (o nei casi più favorevoli, a contenere quanto più possibile) alle personalizzazioni dei servizi che, in un mondo dominato da grandi player internazionali, sono molto difficili da ottenere. Inoltre, con la fruizione dei servizi cloud, di norma, vi è una mancanza di governance e controllo sulle operazioni con conseguenti possibili difficoltà nella piena attuazione delle leggi e dei regolamenti in vigore a livello nazionale ed europeo, soprattutto quando i dati vengono conservati e trattati al di fuori dell›Unione Europea. Queste preoccupazioni sono certamente accentuate nelle cloud pubbliche che rappresentano la soluzione più rischiosa rispetto ad altri modelli di erogazione dei servizi cloud quali le cloud private o di community. I motivi per cui le cloud pubbliche sono da considerare maggiormente a rischio sono:

- i CSP sono spesso rappresentati da player internazionali che hanno logiche di organizzazione e gestione di sistemi che possono non essere compatibili con quelle dei CSC, questa considerazione assume una particolare valenza nel caso delle regole delle Amministrazioni pubbliche fruitrici dei servizi stessi;
- le cloud possono utilizzare infrastrutture localizzate fuori dell'Unione Europea;
- i CSP possono offrire un minor grado di trasparenza circa le misure di sicurezza e resilienza rispetto ai normali modelli di outsourcing oppure rispetto a soluzioni IT interne;
- i CSP possono avere interessi o obblighi di pubblicità degli incidenti di sicurezza incompatibili con le finalità e gli obiettivi perseguiti dalle Amministrazioni Pubbliche.

Altri due aspetti che devono essere tenuti in debita considerazione prima di sottoscrivere o di realizzare servizi cloud sono:

- la connettività Internet è un elemento fondamentale del modello di cloud, senza la quale non è ovviamente possibile accedere ai servizi. La qualità e le prestazioni delle reti (capacità, latenza, ecc.), spesso, non sono geograficamente omogenee e vi sono ancora ambiti territoriali in cui la qualità del

servizio potrebbe costituire un fattore fortemente limitante per la realizzazione di servizi cloud;

- la sottoscrizione di servizi cloud, come e più di altre forme di outsourcing può diminuire nel tempo il livello di competenza tecnica all'interno delle Amministrazioni. Questa preoccupazione, comune anche ad altre forme di outsourcing, è molto forte per i servizi cloud in quanto le competenze di base non sono normalmente presenti nelle Amministrazioni e gli ambiti sono in continua evoluzione. Una condizione di perdita di competenze interne potrebbe aggravare i rischi di "Lock-in" che sono particolarmente rilevanti in ambito governativo.

4. la gestione del rischio nel mondo cloud

Tra i molti approcci al cloud computing che sono stati proposti, tutti quelli che fanno riferimento alla sicurezza insistono su un concetto di base: "non è possibile ottenere servizi cloud sufficientemente sicuri senza partire da un'analisi dei rischi"[8].

Gli approcci specifici possono poi divergere e possono suggerire metodologie o modelli differenti, ma questo assunto di base rimane valido per tutti.

ENISA è certamente l'organismo che ha maggiormente puntato su questo approccio e ha sviluppato i modelli di valutazione più completi in questo campo. In particolare ENISA si è soffermata sulle prospettive delle Piccole e Medie Imprese(9) (PMI) e della Pubblica Amministrazione(op. cit.) con tre diversi scenari: una PA locale che vuole realizzare servizi di e-health tramite cloud, una PA locale che vuole erogare servizi innovativi ai propri cittadini e un'agenzia governativa che sta pianificando la realizzazione di una cloud per supportare l'innovazione e lo sviluppo del business.

È comunque da ricordare anche il contributo della Cloud Security Alliance (CSA) al tema del risk management applicato al cloud computing. La CSA ha infatti pubblicato il documento "Top Threats to Cloud Computing"(10) che contiene un'approfondita analisi delle principali minacce che incombono sul mondo delle cloud.

4.1 Risk assessment

I migliori approcci alla valutazione dei rischi sono quelli nei quali il perimetro e il livello di profondità dell'analisi sono commisurati alla criticità dei dati e dei servizi che si pensa di trasferire "on the cloud".

La Cloud Security Alliance, nella propria Security Guidance(11), propone ad esempio che, nei casi meno critici, venga adottato per lo meno un metodo semplificato per la valutazione dei rischi connessi all'utilizzo di servizi cloud e per la conseguente individuazione delle relative contromisure.

[8] Un contributo sul tema della valutazione dei rischi nel mondo cloud viene proposto nel documento di Booz&Co. "Cloud Computing an Information Security Perspective" in cui sono presentati alcuni interessanti schemi riassuntivi e delle considerazioni sulla governance di sicurezza per le cloud. http://www.booz.com/media/uploads/BoozCo-Cloud-Computing.pdf

In particolare questo metodo di valutazione del rischio prevede un primo passo di censimento degli asset oggetto del trasferimento su servizi cloud che riguardi i processi, le funzioni, le applicazioni e i dati.

Questo primo passo, comune a tutte le metodologie di valutazione dei rischi, è però particolarmente importante in ambienti cloud perché i dati e le applicazioni possono essere separati e quindi si potrebbero creare situazioni dove solo una parte dei dati o delle applicazioni sono oggetto di trasferimento "on the cloud". Si deve quindi determinare esattamente il perimetro dell'operazione per essere in grado di individuare le contromisure più adeguate.

In seguito al censimento si deve procedere con la valutazione vera e propria. Anche su questo la CSA fornisce le domande minimali per poter almeno abbozzare un quadro dei rischi.

Quindi, al fine di valutare, a grandi linee, i requisiti di riservatezza, disponibilità e integrità, per ogni asset si deve rispondere ad almeno questa serie di domande:
Che tipo di danno si verrebbe a creare se:

1. l'asset in valutazione diventasse di pubblico dominio?
2. un dipendente del fornitore di servizi cloud avesse accesso all'asset in valutazione?
3. il processo o la funzione fossero fraudolentemente manipolati da un attaccante esterno?
4. il processo o la funzione non fornissero i risultati attesi?
5. le informazioni/i dati fossero modificati in maniera non autorizzata?
6. l'asset in valutazione non fosse disponibile per un dato periodo di tempo?

CSA suggerisce infine, tramite l'analisi di questa serie di risposte, di procedere nella consapevole individuazione del "Modello di erogazione" più adatto alle nostre esigenze e solo DOPO cominciare a cercare un eventuale fornitore che possa soddisfare i requisiti individuati.

4.2 I principali rischi delle cloud

Al fine di facilitare l'analisi del rischio nel contesto del cloud computing, si è ritenuto utile identificare e descrivere quelli che appaiono come i 10 principali rischi[9] legati all'utilizzo di servizi erogati tramite cloud. La tabella seguente elenca i 10 rischi individuati e ne specifica la rilevanza a seconda del modello di erogazione adottato (si veda paragrafo 1.1.2).

Tabella 5 - Matrice della rilevanza dei rischi nei vari Service Model

Rischio	Public	Commun. EXT	Commun. INT	Private
Contrattualistica non sempre adeguata	A	M	B	B
Impossibilità di negoziare termini contrattuali	A	M	M	B
Legge applicabile e foro competente	A	B	B	B
Mancato rispetto normativa sulla privacy	A	A	A	M
Riflessi di azioni giudiziarie su altri clienti	A	A	A	A
Perdita di governance	A	M	B	B
Lock-in	A	A	A	A
Indisponibilità di un servizio o di un provider	A	A	A	A
Compromissione delle caratteristiche di sicurezza dei dati	A	A	A	A
Compromissione della sicurezza di rete	A	A	A	A

Legenda

A=Molto rilevante

M=Mediamente rilevante

B=Poco rilevante

Community-INT= Community Cloud posseduta, ubicata e gestita internamente

Community-EXT= Community Cloud posseduta, ubicata e gestita da terzi

4.2.1 Rischio 1 –Contrattualistica non sempre adeguata

Il mercato cloud è ancora un mercato giovane e i provider che offrono servizi cloud pubblici, non hanno ancora compiutamente sviluppato offerte differenziate per tipologia di mercato e di cliente. Nella maggioranza dei casi, i fornitori propongono l'adesione a contratti standard applicabili a tutti i loro

[9] La comunità che si riconosce nel "Open Web Application Security Project" (OWASP) sta proponendo un progetto chiamato "OWASP Top 10 Security Risks". Questa lista, che è classificata come un progetto ancora nella fase alpha, è fondamentalmente puntata ai rischi delle cloud pubbliche o ibride che erogano servizi SaaS.
https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project

clienti. Spesso questi contratti, proprio per favorire la semplicità di approccio, non vengono incontro ai diversi requisiti e si attestano verso "approcci base" che, come anche messo in evidenza da una ricerca di Gartner(12), si traducono in clausole che non sempre garantiscono le tipologie di clientela che hanno requisiti di sicurezza più elevati. In particolare, molti contratti di questo tipo sono carenti nella descrizione delle responsabilità imputabili al provider, risultando quindi poco adeguati ai requisiti legali delle realtà di tipo "enterprise" o, ancor più, delle Pubbliche Amministrazioni.

Infine, a volte, alcuni contratti, anche per aspetti rilevanti, rimandano a termini, clausole o SLA che sono specificati in maniera poco puntuale o che fanno riferimento a elementi esterni che ne specificano il dettaglio (ad esempio pagine Web che per loro natura sono, nel tempo, soggette a modifiche e che non garantiscono certezze ai clienti). Quindi, i casi precedentemente evidenziati costituiscono una problematica seria che deve essere affrontata sin dalle fasi iniziali della predisposizione degli accordi tra CSC e CSP[10]. Più precisamente, le condizioni generali di servizio devono essere analizzate accuratamente al fine di valutare la piena compatibilità con le esigenze del CSC. In caso negativo, andranno negoziati i punti critici (ipotesi spesso impercorribile – come spiegato subito di seguito) o dovrà essere scelta un'altra offerta cloud.

4.2.2 Rischio 2 – Impossibilità di negoziare i termini contrattuali

I CSP, allo scopo di realizzare le economie di scala che rappresentano il vero motore dell'economicità dell'approccio cloud, tendono a predisporre una contrattualistica standard, applicabile a tutti i CSC, con possibilità di negoziazione nulle o, qualora presenti, estremamente limitate.

Va detto che sono proprio alcune specificità dei servizi cloud pubblici che poco si prestano ad approcci "custom". Ad esempio, le caratteristiche di "multi-tenancy" delle cloud, ossia l'utilizzo di una singola istanza software per servire più clienti, non consentono o rendono arduo accogliere requisiti differenti provenienti dai diversi clienti.

Accade quindi abbastanza di frequente che si debba considerare di sottocrivere un servizio così come proposto dal CSP, dato che una effettiva negoziazione dei termini contrattuali non è realizzabile.

[10] Per approfondimenti il complesso tema della contrattualistica dei servizi cloud, si può fare riferimento all'interessante documento "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services" prodotto dalla Queen Mary University of London, School of Law. http://ssrn.com/abstract=1662374

4.2.3 Rischio 3 – Legge applicabile e foro competente

La legge applicabile alle eventuali controversie relative all'erogazione del servizio ed il foro competente sono generalmente indicati delle condizioni generali, e, quindi, come appena descritto nei due paragrafi precedenti, di fatto decisi dal CSP.

Discorso a parte merita la legge applicabile al trattamento dei dati personali, individuata da normativa speciale, non derogabile dalle parti. Analogamente, nei contratti "*business to consumer*" si applicherà invece, salvo eccezioni, la giurisdizione del luogo di residenza del consumatore.

Nei servizi erogati da cloud pubbliche, i dati e le applicazioni possono essere fisicamente allocati in una pluralità di data center distribuiti in vari paesi del mondo. I provider internazionali scelgono i Paesi dove realizzare i propri data center in base a criteri di natura economica (ad esempio in paesi con un costo ridotto del lavoro, agevolazioni finanziarie o fiscali), di natura geografica (ad esempio in paesi freddi in cui la refrigerazione dei data center presenta costi ridotti o in paesi distribuiti in modo da ottimizzare le risorse in base ai ritmi giornalieri di utilizzo delle risorse) e di natura tecnica (ad esempio in paesi con ampie disponibilità di skill adeguati). Questi criteri possono portare a scelte non adeguate per alcune tipologie di clienti che privilegiano scelte di garanzia con l'individuazione di Paesi con impianti giuiridico-normativi assimilabili a quelli di residenza. Infatti, se i data center del CSP sono stati realizzati in Paesi che hanno impianti normativi poco chiari o poco orientati alla certezza del diritto, i dati e le applicazioni dei clienti potrebbero, ad esempio, essere esposti a sequestri o restrizioni da parte delle forze dell'ordine o delle autorità giudiziarie con motivazioni e modalità del tutto inaccettabili.

Infine un punto che può presentare delle particolari criticità per i clienti è rappresentato dal foro competente. Alcuni provider possono avere dei vantaggi nella scelta, quale foro competente, di Paesi che sono ai margini dei normali circuiti internazionali. Nel caso di un confronto che dovesse sfociare in un contenzioso legale, riuscire a trovare una adeguata rappresentanza in questi Paesi potrebbe essere estremamente difficile e oneroso per il cliente.

4.2.4 Rischio 4 – Mancato rispetto della normativa in materia di protezione dei dati personali

Nel tempo, nei paesi occidentali e nell'Unione Europea in particolare, sono stati sviluppati dei sistemi legislativi di protezione e tutela dei dati personali che difficilmente trovano corrispondenza in altre tipologie di Paesi. In questa situazione, per un CSP può essere molto complesso riuscire a contemperare le esigenze

di rispetto della normativa in materia di protezione dei dati personali con la distribuzione geografica dei dati e delle applicazioni. Proprio al fine di riuscire a dare risposte a questo tipo di problematiche, alcuni CSP pubblici hanno elaborato delle offerte specifiche, che, anche a fronte di un maggior onere economico a carico del CSC, garantiscono che i dati e le applicazioni rimangano nell'ambito dell'Unione Europea o, al più, vengano trasferiti unicamente negli Stati Uniti a società che hanno adottato i cosiddetti "Safe Harbor Principles", ossia quelle disposizioni che garantiscono la compatibilità con le rigorose norme europee sulla protezione dei dati personali.

Inoltre, come messo in evidenza recentemente anche dall'Istituto Italiano Privacy (IIP)[11] esistono problematiche ancora non completamente indirizzate per quanto riguarda l'attribuzione dei ruoli privacy (Titolare e Responsabile del trattamento) e la filiera delle responsabilità che, allo stato attuale della normativa, mal si conforma alle modalità di gestione delle cloud. Queste disposizioni in materia di formalizzazione dei ruoli e delle responsabilità sono ulteriormente complicate nei casi di subfornitura o di gestione congiunta dei dati e delle infrastrutture.

Infine, allo scopo di adempiere correttamente alla normativa vigente, devono essere attentamente valutate le misure di sicurezza da riservare ai dati personali, verificandone in particolare gli aspetti di conformità.

Tutte queste casistiche meritano di essere attentamente vagliate e, nel caso, correttamente e accuratamente regolate a livello contrattuale.

4.2.5 Rischio 5 – Riflessi di azioni giudiziarie verso altri clienti

L'ambiente "multi-tenant" tipico delle cloud comporta numerose nuove problematiche. Tra queste risulta di particolare importanza la possibilità che il sequestro di dati o, più genericamente, l'acquisizione di materiale probatorio da parte delle forze dell'ordine, relativamente a un procedimento riguardante un CSC di una cloud, possa avere consistenti impatti anche sugli altri CSC della stessa cloud. Questa situazione potrebbe comportare una compromissione della riservatezza e possibili interruzioni del servizio. Per queste ragioni è particolarmente importante la valutazione delle modalità:

- di accesso delle forze dell'ordine ai dati e alle infrastrutture;
- di notifica ai CSC in caso di intervento delle forze dell'ordine.

[11] L'IIP è un centro studi dedicato alle tematiche della protezione dei dati personali e della cybersecurity nella società globale dell'ICT. L'Istituto, operando come think tank è un punto di riferimento per gli esperti e per i diversi player dei mercati ad elevato contenuto tecnologico. http://www.istitutoitalianoprivacy.it

4.2.6 Rischio 6 – Perdita di governance

Nell'ambito dei servizi erogati dai CSP, la perdita di governance è un rischio sempre presente. I fattori che influenzano questo fenomeno sono legati principalmente alle modalità di utilizzo proposte dal CSP, eventualmente formalizzate in apposite clausole, SLA e termini contrattuali. In generale è bene ricordare che alcune pratiche di sicurezza ormai considerate normali nei rapporti di outsourcing, quali ad esempio gli assessment (tecnici e procedurali) e gli audit, sono invece tipicamente escluse dai contratti di servizi nelle cloud. Inoltre, l'utilizzo di subfornitori da parte del cloud provider potrebbe portare a un ulteriore – e difficilmente valutabile – impatto per questa tipologia di rischio.

È bene ricordare che, per una corretta valutazione delle possibili conseguenze di questa problematica, si deve tenere conto anche dei requisiti di conformità a normative di settore, regolamenti, standard e best practice. Queste normative, infatti, potrebbero contenere dei requisiti legati al controllo e alla governance la cui compatibilità con le cloud risulta complicata se non addirittura impossibile da soddisfare.

4.2.7 Rischio 7 – Lock In

Questo rischio evidenzia l'attuale situazione di difficoltà per un CSC di poter cambiare CSP a seconda delle proprie esigenze contingenti. Un CSC, soprattutto se di tipo "enterprise" o governativo, dovrebbe infatti avere la garanzia di poter:

- cambiare il proprio CSP;
- riportare al proprio interno il servizio se gestito da un CSP esterno;
- affidare a un CSP esterno un servizio gestito internamente nella propria cloud privata.

Il tutto dovrebbe avvenire senza particolari problematiche.

Tutto ciò si deve tradurre in chiare clausole contrattuali che specifichino in modo completo ed esaustivo tutte le condizioni e le modalità operative di uscita dal servizio (cd. Transfer-Back), con particolare riferimento a:

- le modalità con le quali vengono forniti i dati e, se del caso, il codice applicativo;
- le modalità di erogazione del supporto alla migrazione;
- i tempi, gli effort previsti e gli eventuali step transitori.

Al riguardo, sarebbe altresì utile lo sviluppo e l'emanazione di best practice e di standard internazionalmente riconosciuti che rendano realmente fattibile ed efficiente la migrazione di dati e applicazioni tra diverse cloud.

Come ricordato recentemente[13] dalla vice presidente della Commissione Europea, Neelie Kroes, l'interoperabilità è essenziale nel settore delle cloud affinché questo nuovo mercato diventi equo, aperto e competitivo e quindi possa esprimere appieno il proprio potenziale.

4.2.8 Rischio 8- Indisponibilità di un servizio o di un provider

Gli SLA proposti dai CSP per la disponibilità dei servizi sono normalmente molto sfidanti. Non è inusuale infatti trovare percentuali di "uptime" superiori al 99,5%. Questi SLA devono però essere opportunamente valutati nel contesto del contratto in relazione ai periodi di osservazione e a eventuali intervalli di tempo definiti, al di sotto dei quali il disservizio non viene considerato. Ad esempio, se l'intervallo definito è pari a 15 minuti, un'interruzione del servizio per 14 minuti non contribuirà al calcolo delle percentuali di "uptime". I rischi di indisponibilità dei servizi erogati dalle cloud sono quindi da considerare molto attentamente, soprattutto nel caso in cui vengano utilizzati per dati e applicazioni critici. Infatti, nonostante l'adozione di tecnologie evolute a garanzia della continuità di servizio e la conseguente proposizione di appositi SLA da parte dei CSP, i CSC non devono pensare che tutte le possibili problematiche siano state risolte. Non ci sono infatti reali ragioni tecnologiche per confidare in un cambiamento di scenario tale da far considerare superati i principi di base per la disponibilità e l'affidabilità che, in passato, hanno guidato la progettazione e la gestione delle applicazioni. I concetti di ridondanza delle risorse e l'utilizzo di copie di emergenza hanno ancora una fondamentale importanza anche nel mondo del cloud computing. I CSC devono quindi porre particolare attenzione nella scelta di clausole contrattuali e di contromisure che diano delle effettive garanzie di ridondanza, eventualmente anche scegliendo di suddividere il servizio tra diversi CSP.

Una variante di questo rischio, è legata a possibili fallimenti o chiusure di CSP o di servizi. Come precedentemente ricordato, infatti, il mercato del cloud è molto giovane e quindi è probabile che, nel corso del tempo, la "selezione naturale" dei vari competitor conduca a fallimenti, chiusure, fusioni e riorganizzazioni in una misura maggiore rispetto a quella riscontrabile in altri settori più consolidati. Inoltre, dati i rischi di "Lock in" anch'essi precedentemente analizzati, per un cliente potrebbe essere estremamente difficoltoso e oneroso, qualora possibile, trovare soluzioni alternative se il proprio CSP decidesse o fosse costretto a interrompere l'erogazione dei propri servizi, con possibili gravi conseguenze dal punto di

vista della disponibilità e del recupero dei dati, della riservatezza e dell'integrità dei medesimi, ma anche con riferimento alla responsabilità del CSC in merito al rispetto della disciplina sulla protezione dei dati personali.

4.2.9 Rischio 9 – Compromissione delle caratteristiche di sicurezza dei dati

In questo rischio confluiscono gli aspetti più tipicamente tecnici che possono portare alla perdita delle principali caratteristiche di sicurezza quali: la riservatezza, l'integrità e la disponibilità dei dati. Ad esempio, l'isolamento tra le risorse computazionali condivise tra i vari CSC è una problematica che, a seguito della maturazione delle tecniche di virtualizzazione, viene ormai considerata come un dato di fatto non più in discussione. È però bene ricordare che potrebbero verificarsi delle condizioni, legate ad esempio alla scoperta di nuove vulnerabilità, che potrebbero mettere a repentaglio questo approccio. Inoltre, altre problematiche quali la compromissione delle interfacce di management, la reale cancellazione dei dati, la gestione delle identità, ecc. sono esempi tipici di rischi che devono essere attentamente valutati nell'ottica delle tipologie di servizio cloud che si intendono sottoscrivere.

In generale tutte le problematiche tecnologiche legate a possibili compromissioni della sicurezza dei dati e delle applicazioni "on the cloud" dovrebbero essere oggetto di approfondita analisi al fine di comprenderne appieno i rischi.

Questa tematica, infine, esprime anche delle implicazioni di carattere legale, poiché, come recentemente affermato anche dalla European Privacy Association (EPA)[12], un problema di sicurezza in ambito cloud può tradursi in un danno diretto nei confronti di molti clienti che troverà un completo risarcimento nei successivi procedimenti legali solo qualora sussistano tutti i presupposti normativi e legali. È quindi molto importante verificare accuratamente le clausole contrattuali dedicate:

- alla riservatezza (cd. "*Confidentiality Clause*");
- alla proprietà intellettuale;
- alle modalità di trasferimento, conservazione, elaborazione, accesso e custodia delle informazioni dei clienti;
- al foro competente e alla giurisdizione applicabile.

[12] L'EPA è una rete pan-europea di esperti di sicurezza e di privacy con sede a Bruxelles che lavora a stretto contatto con le istituzioni europee, in particolare con il Parlamento europeo, con il mondo accademico, la società civile e l'industria per portare avanti nuove idee e affrontare i pressanti problemi di privacy che l'Europa sta affrontando.
http://www.europeanprivacyassociation.eu/

4.2.10 Rischio 10 – Compromissione della sicurezza della rete

L'architettura delle cloud è di tipo altamente distribuito e quindi basata su servizi di rete che devono garantire la piena interoperabilità delle varie parti, oltre all'accesso riservato ai clienti verso le risorse, i dati e le applicazioni. Ciò implica chiaramente che tutti gli aspetti di sicurezza della rete costituiscano un elemento centrale per il corretto funzionamento delle cloud.

Ad esempio, l'adozione di contromisure come la cifratura, l'autenticazione forte e la realizzazione di attente politiche di garanzia della qualità dei servizi di rete, costituiscono alcuni degli elementi fondamentali per l'erogazione di servizi cloud con livelli di riservatezza, integrità e disponibilità definiti. Inoltre, essendo il cloud costituito da servizi di tipo "end-to-end", per garantire la disponibilità dei dati, deve essere verificata l'effettiva possibilità di usufruire di infrastrutture di rete affidabili e ridondate sia a livello geografico (nazionale e regionale) sia a livello delle scelte del fornitore di servizi cloud.

Anche in questo caso, tutte le contromisure di tipo tecnologico, devono essere presenti e specificate in clausole contrattuali che regolano la materia in maniera chiara e comprensibile anche dal punto di vista dell'allocazione delle responsabilità.

5. Cloud Security: gli aspetti più rilevanti

Esaminati i principali rischi da analizzare prima di adottare servizi cloud, è opportuno approfondire gli aspetti di sicurezza[13] che devono essere affrontati e risolti. Al riguardo è utile ricordare le definizioni di sicurezza e resilienza proposte da ENISA(op. cit.).

Sicurezza *è la capacità di proteggere le informazioni e il sistema da accessi, utilizzi, comunicazioni, modifiche o distruzioni non autorizzati e di gestire la risposta e il recupero in caso di guasti o incidenti.*

Resilienza *è la capacità di un sistema (rete, servizio, infrastruttura, ecc.) di fornire e di mantenere un accettabile livello di servizio rispetto a vari incidenti e problemi che possono avvenire nel corso delle normali operazioni.*

Inoltre, ENISA precisa che i parametri di sicurezza e resilienza devono essere considerati nel quadro dei livelli di servizio concordati e quindi un dato servizio può essere considerato sicuro e resiliente quando rispetta le relative specifiche dei livelli di servizio.

5.1 Il sistema di governo e le policy di sicurezza

Come osservato nel paragrafo dedicato all'analisi dei rischi, l'utilizzo delle cloud può produrre una perdita delle capacità di governo sui servizi fruiti. Questa perdita della capacità di governo si accompagna al mantenimento, in tutto o in parte, della responsabilità nei confronti dei terzi. In questo contesto è evidente la necessità di recuperare, almeno in parte e in forma diversa da quella tradizionale, il governo dei servizi.

L'obiettivo è di realizzare un sistema di governo delle strutture/processi tale da garantire:

- il mantenimento di un effettivo governo della sicurezza;
- l'implementazione di un sistema di risk management;
- la conformità a leggi, regolamenti e best practice;
- un adeguato controllo sulla sicurezza dei dati e delle applicazioni.

[13] Come precedentemente ricordato, la Cloud Security Alliance ha prodotto la "Security Guidance for Critical Areas of Focus in Cloud Computing"(op. cit.), uno dei documenti di riferimento nel mondo della sicurezza del cloud computing. In questo documento il tema è affrontato in modo complessivo, individuando 13 domini concettuali, logicamente suddivisi in aree afferenti al governo e all'operatività delle cloud. Questo documento, che peraltro sarà aggiornato a breve, deve rappresentare certamente una fonte primaria per chi si accinge a effettuare delle valutazioni di sicurezza sui servizi erogati nell'ambito delle cloud.

È particolarmente importante che il CSP sia dotato di un chiaro e definito Piano della sicurezza rispondente alle esigenze del CSC. Il CSC non solo non dovrà rinunciare a definire il proprio Piano di Sicurezza ma dovrà anche verificare che il proprio piano sia coerente con quello del CSP. La coerenza dovrà almeno riguardare:

- l'individuazione delle minacce;
- le misure per il risk management;
- la struttura responsabile della sicurezza;
- le modalità per il mantenimento della conformità alle normative vigenti in materia con particolare riferimento alla disciplina in materia di protezione dei dati personali;
- le modalità per il mantenimento della conformità ad altre normative e standard applicabili al caso di specie;
- le metriche e gli standard di misurazione dei valori relativi alla sicurezza;
- le metodologie di assessment, la frequenza degli stessi e l'eventuale coinvolgimento di terze parti fidate;
- l'approccio agli audit e il relativo piano attuativo;
- la descrizione, ad alto livello, delle misure di protezione fisica, logica e organizzativa;
- le interazioni tra cliente e fornitore nella gestione corrente e nella gestione delle anomalie e degli incidenti.

Nel caso di significative discrepanze tra il Piano di Sicurezza del CSC e quello del CSP, il cliente dovrà verificare le possibilità di adeguamento di quest'ultimo.

Nel frequente caso di impossibilità nell'esercizio di un controllo diretto sulle infrastrutture soprattutto con i CSP pubblici, il controllo sugli aspetti di sicurezza sarà affrontato attraverso la definizione di opportuni SLA ed adeguate garanzie da parte del CSP sui livelli di sicurezza applicati.

Quindi è bene che la struttura che si occupa di sicurezza per il cliente sia coinvolta, sin dalle fasi iniziali, nell'analisi delle relative sezioni delle condizioni generali di servizio o, nel caso vi sia la possibilità di negoziare, nella definizione delle clausole contrattuali.

5.2 Audit e compliance

Nell'ambito del cloud computing le problematiche di conformità e, di conseguenza, quelle dell'audit assumono una particolare importanza. La compliance riguarda anzitutto i temi legati alla protezione dei dati personali e alle difficoltà legate al mantenimento delle certificazioni di sicurezza.

Il pieno rispetto degli obblighi imposti dalla normativa in materia di protezione dei dati personali è un tema molto complesso e dibattuto (si veda il paragrafo 4.2.4). La condizione minima per adempiere agli obblighi privacy è che il CSP abbia un piano di gestione degli adempimenti e sia disponibile a ricevere tutte le eventuali nomine formali del caso, gli obblighi connessi e le relative responsabilità. Inoltre, il CSC deve preventivamente effettuare un censimento e un'approfondita ricognizione dei dati personali e dei relativi trattamenti oggetto di trasferimento "on the cloud", verificando che tutti i necessari presupposti siano effettivamente in essere. Infine, il CSC dovrà modificare la documentazione ufficiale relativa alla privacy (Documento programmatico della sicurezza, in primis) in modo da rappresentare correttamente la situazione aggiornata e dare conto delle scelte effettuate.

Al fine di avere le maggiori possibilità di trattare la complessa materia in modo completo ed efficace è necessario che, sin dalle prime fasi della definizione degli accordi o del contratto, i responsabili degli adempimenti privacy per il CSC ne verifichino i punti rilevanti ed eventualmente si interfaccino con l'omologa componente del CSP per chiarire e risolvere tutte le possibili problematiche[14].

Allargando la portata di questa verifica è opportuno che venga effettuato anche un censimento completo di tutte le leggi e normative nazionali e internazionali ritenute applicabili in questo contesto, con particolare riferimento agli eventuali trasferimenti ed elaborazioni di dati all'estero. Lo stesso esercizio va esteso alla ricognizione delle specifiche normative di settore applicabili al caso concreto (ad esempio le normative applicabili nel mondo sanitario).

Per quanto riguarda invece le certificazioni che devono essere mantenute dal cliente è importante avere ben chiaro che, nella maggior parte dei casi, queste certificazioni non sono state concepite avendo come

[14] A questo proposito può essere utile fare riferimento al concetto di 'Privacy Level Agreement' (PLA) elaborato nello studio "Il cloud computing nella disciplina italiana" pubblicato dall'Istituto Italiano Privacy (IIP) a giugno 2011.

riferimento il mondo del cloud computing. È opportuno che il CSC affronti con il fornitore, in maniera preventiva, alcuni aspetti quali ad esempio quelli relativi alla definizione del perimetro e alle suddivisioni di responsabilità, alle registrazioni di sistema e alle verifiche. Il tema delle verifiche è particolarmente critico in quanto i fornitori di servizi cloud, normalmente, oppongono resistenze nel concedere la possibilità ai propri clienti di effettuare audit. Qualora questi accessi fossero necessari per il mantenimento della conformità a normative o a standard, il cliente deve riuscire a trovare preventivamente una soluzione tecnica e contrattuale adeguata alle sue esigenze.

Un aspetto da non sottovalutare, infine, è la produzione di certificazioni di sicurezza da parte del fornitore di servizi. In particolare la certificazione ISO 27001 o altre certificazioni che attestino in maniera indipendente il rispetto delle migliori pratiche di sicurezza è da considerare un mezzo per i clienti per assicurarsi la conformità alle normative vigenti.

5.3 La definizione e la gestione dell'infrastruttura

L'architettura dei sistemi per l'erogazione di servizi cloud è un elemento chiave da esaminare ai fini del rispetto dei requisiti di sicurezza.

Le cloud, come messo in evidenza della definizione del NIST (si veda paragrafo 1.1.1), si basano fondamentalmente sulla messa in comune di risorse e sul modello "multi-tenant". In questo contesto tutti gli sforzi per mettere in sicurezza i dati e i servizi devono essere orientati a creare dei perimetri, dei "compartimenti", all'interno dei quali i clienti possano essere confidenti dei livelli di sicurezza erogati.

Questo principio di "compartimentazione" deve essere declinato per i vari aspetti dell'architettura:

1. **Rete**. La compartimentazione di rete prevede al minimo:
   - la scelta di un'adeguata topologia di rete;
   - l'applicazione dei concetti di "Defence in depth";
   - la segmentazione attraverso apparati di sicurezza;
   - la documentazione delle scelte effettuate;
   - la revisione periodica o su base necessità dell'intero progetto.

2. **Accessi**. La compartimentazione degli accessi prevede al minimo:
   - la classificazione delle tipologie di accesso;
   - l'individuazione di ruoli da assegnare alle risorse con particolare attenzione nell'assegnazione dei privilegi di amministrazione e di accesso alle interfacce di gestione;
   - la definizione delle caratteristiche di sicurezza delle diverse tipologie di canali di comunicazione;
   - l'utilizzazione di protocolli sicuri di comunicazione;
   - l'applicazione del principio di "least privilege";
   - la definizione di standard per la gestione degli accessi basati sul ruolo.
3. **Servizi**. La compartimentazione dei servizi prevede al minimo:
   - l'individuazione delle tipologie di risorse;
   - l'individuazione dei servizi che devono essere attivi su ogni tipologia di risorsa;
   - lo hardening standard delle risorse;
   - la realizzazione di un Patch Management Program;
   - l'utilizzo di strumenti automatizzati di discovery;
   - l'effettuazione di Vulnerability Assessment periodici.
4. **Virtualizzazione**. La compartimentazione degli elementi virtuali prevede al minimo:
   - l'utilizzo di componenti integrativi di sicurezza;
   - l'utilizzo di controlli di sicurezza esterni per la protezione delle interfacce di amministrazione;
   - l'utilizzo dei controlli di sicurezza delle piattaforme di virtualizzazione per la gestione del traffico che attraversa i "backplane";
   - la creazione di zone sicure basate sul tipo di utilizzo delle risorse.
5. **Spazi fisici**. La compartimentazione degli spazi fisici prevede al minimo:
   - la definizione di un piano di sicurezza fisica;
   - la definizione di aree a diversa criticità;
   - l'implementazione di contromisure fisiche per la prevenzione di accessi non autorizzati;
   - l'adeguata gestione degli accessi del personale esterno;
   - l'adeguata protezione da minacce di natura fisica.
6. **Personale**. La compartimentazione del personale prevede al minimo:
   - la puntuale definizione dei ruoli anche in relazione ai temi relativi alla protezione dei dati personali;
   - l'applicazione dei concetti di "need to know";
   - la definizione delle procedure operative da applicare;
   - l'adeguata formazione di tutte le figure previste;
   - la realizzazione di un piano di audit.

Esistono poi delle tematiche trasversali che riguardano principalmente la realizzazione di un Piano di Business Continuity e di un Piano di Disaster Recovery. Da questo punto di vista è fondamentale non ritenere che un'infrastruttura cloud sia robusta e resiliente "di per sé". Senza un'adeguata progettazione e pianificazione, gli SLA contrattualizzati saranno certamente irrealizzabili.

Infine, sono da privilegiare gli approcci alla sicurezza che contemplano certificazioni e metodi di miglioramento continuo.

5.4 L'utilizzo della cifratura

Tenuto conto della condivisione di risorse prevista nelle cloud, l'utilizzo di strumenti di cifratura dei dati assume un'importanza centrale nella valutazione delle misure di sicurezza implementate. La cifratura dovrebbe essere estensivamente utilizzata, ad esempio cifrando i dati:

- in transito all'interno e all'esterno della cloud;
- conservati all'interno dei database;
- archiviati sui supporti di backup.

È opportuno valutare anche la possibilità di utilizzare un ulteriore livello di cifratura per i dati in memoria, al fine di ridurre al minimo le possibili perdite di controllo sulla riservatezza dei dati stessi.

La cifratura, inoltre, può essere un valido strumento in due situazioni molto critiche del mondo cloud: il furto di dati e la cancellazione dei dati. In riferimento al primo caso, è da sottolineare che nel caso di molte legislazioni, un furto di dati cifrati non è soggetto agli obblighi di pubblicità che altrimenti dovrebbero essere svolti se i dati fossero in chiaro[15]. Per queste legislazioni, se i dati sono cifrati, è come se il furto di dati non fosse avvenuto.

[15] L'Amministrazione Obama, a maggio 2011, ha proposto una nuova normativa sugli obblighi di notifica degli incidenti che comportano la perdita o il furto di dati personali. Tale proposta di "Data Breach Notification" parte dalla considerazione che l'utilizzo della cifratura sui dati rubati rende nullo il rischio e quindi conclude con la non applicabilità delle norme di garanzia tra cui l'obbligo di notifica. http://democrats.senate.gov/pdfs/WH-cyber-breach-notice.pdf

Per quanto riguarda la cancellazione dei dati, invece, la cifratura consente di rendere estremamente rapido e affidabile un processo che normalmente crea grandi difficoltà a chi lo deve portare a termine. La garanzia di cancellazione definitiva di dati, infatti, è materia molto complessa che prevede numerosi passaggi ed è quindi onerosa sia dal punto di vista dei tempi sia delle risorse utilizzate. Se i dati sono memorizzati in forma cifrata, la distruzione della chiave associata e una procedura di cancellazione dei dati "leggera" possono portare a risultati superiori con minori sforzi.

Però, per non incorrere in inutili rischi, si ricorda che si devono assicurare i migliori criteri di gestione delle chiavi che devono essere conservate in maniera sicura. Inoltre gli accessi alle chiavi devono essere opportunamente regolati e devono essere realizzate e applicate chiare ed efficaci procedure di backup e recovery delle chiavi stesse.

5.5 La gestione delle identità

Un'altra caratteristica cruciale per la gestione della sicurezza delle cloud è rappresentata dalla corretta gestione delle identità. Da questo punto di vista devono essere presi in esame almeno quattro aspetti:

- la gestione delle utenze;
- l'autenticazione;
- l'autorizzazione;
- la federazione tra sistemi di gestione delle identità.

Tra gli aspetti appena citati, le problematiche legate alla federazione dei sistemi di gestione delle identità tra il CSC e il CSP risulta centrale. Infatti, nel caso siano presenti sistemi di gestione delle identità da parte del CSC, questi devono essere interconnessi con quelli del fornitore dei servizi cloud. Questa indicazione pone dei requisiti di standardizzazione e di flessibilità dei sistemi del CSP (e in parte anche per il sistema dei CSC). Inoltre devono essere valutate attentamente le modalità di integrazione dei sistemi al fine di non inserire possibili vulnerabilità o punti di debolezza nei sistemi stessi. In questo particolare ambito si colloca il tema della protezione delle "API Key", ovvero delle "stringhe di dati" che, in alcune tipologie di infrastruttura, consentono di realizzare soluzioni di federazione dei sistemi di gestione delle identità. Le API Key devono essere protette in modo molto stringente poiché sono legate con degli appositi automatismi al sistema di "billing" del CSP e perché sono utilizzate come veri e propri "lasciapassare" per i servizi erogati al CSC a cui sono assegnate.

5.6 La sicurezza delle applicazioni

La maggioranza degli attacchi ai sistemi si concentra ormai sullo strato applicativo. L'importanza della sicurezza applicativa è ancora maggiore negli ambienti cloud based, in quanto, questi, sono ambienti multi-cliente e costituiscono di conseguenza una grande attrattiva per i criminali. Riuscire a trovare una vulnerabilità applicativa che consente di accedere ai dati (ad esempio tramite un attacco di tipo SQL-Injection) in un ambiente cloud può consentire all'attaccante un accesso privilegiato ai dati di tutti i clienti del fornitore di servizi cloud.

Per riuscire a realizzare un adeguato sistema di sicurezza per le applicazioni cloud, oltre a implementare tutte le misure di sicurezza normalmente previste per le applicazioni che sono eseguite in ambienti tradizionali, devono essere realizzate anche una serie di misure pensate specificamente per gli ambienti cloud.

La costruzione di un framework che copre tutti gli aspetti dell'intero ciclo di vita delle applicazioni è un presupposto necessario per garantire adeguati livelli di sicurezza[16]. Devono essere adeguatamente trattati i delicati temi: della validazione delle applicazioni, del change management e della separazione degli ambienti di sviluppo, test e collaudo da quelli di produzione.

Al fine di mantenere il controllo della sicurezza delle applicazioni è opportuno introdurre metriche per la misura "oggettiva" di alcuni parametri chiave quali ad esempio i risultati di test di vulnerabilità o i tempi di risoluzione delle problematiche di sicurezza del codice.

Come anticipato al paragrafo 1.3, si osserva che il tema della sicurezza delle applicazioni riguarda tutti i "Service model" IaaS, PaaS e SaaS e che, nei tre casi, attribuisce le responsabilità sia al CSP che al CSC, anche se ripartite in modo differente. Ad esempio, nel modello IaaS sarà principalmente il CSC a doversi porre il problema di utilizzare adeguate tecniche e metodologie di sicurezza applicativa mentre nel modello SaaS il CSP dovrà assicurare che le tecniche e le metodologie da lui adottate nel campo della sicurezza applicativa garantiscano i dati dei CSC.

[16] In questo contesto il progetto open source Open Web Application Security Project (OWASP) è certamente un riferimento da tenere presente. http://www.owasp.org

6. Un approccio consapevole ai servizi cloud

La scelta di usufruire di servizi cloud è dunque una scelta molto complessa che investe numerose competenze e che prevede molte considerazioni inerenti a domini diversi. Riuscire a cogliere i vantaggi del cloud significa saper sfruttare al meglio le possibilità che questo paradigma di erogazione dei servizi sa dare, senza correre rischi eccessivi o, peggio ancora, non conosciuti.

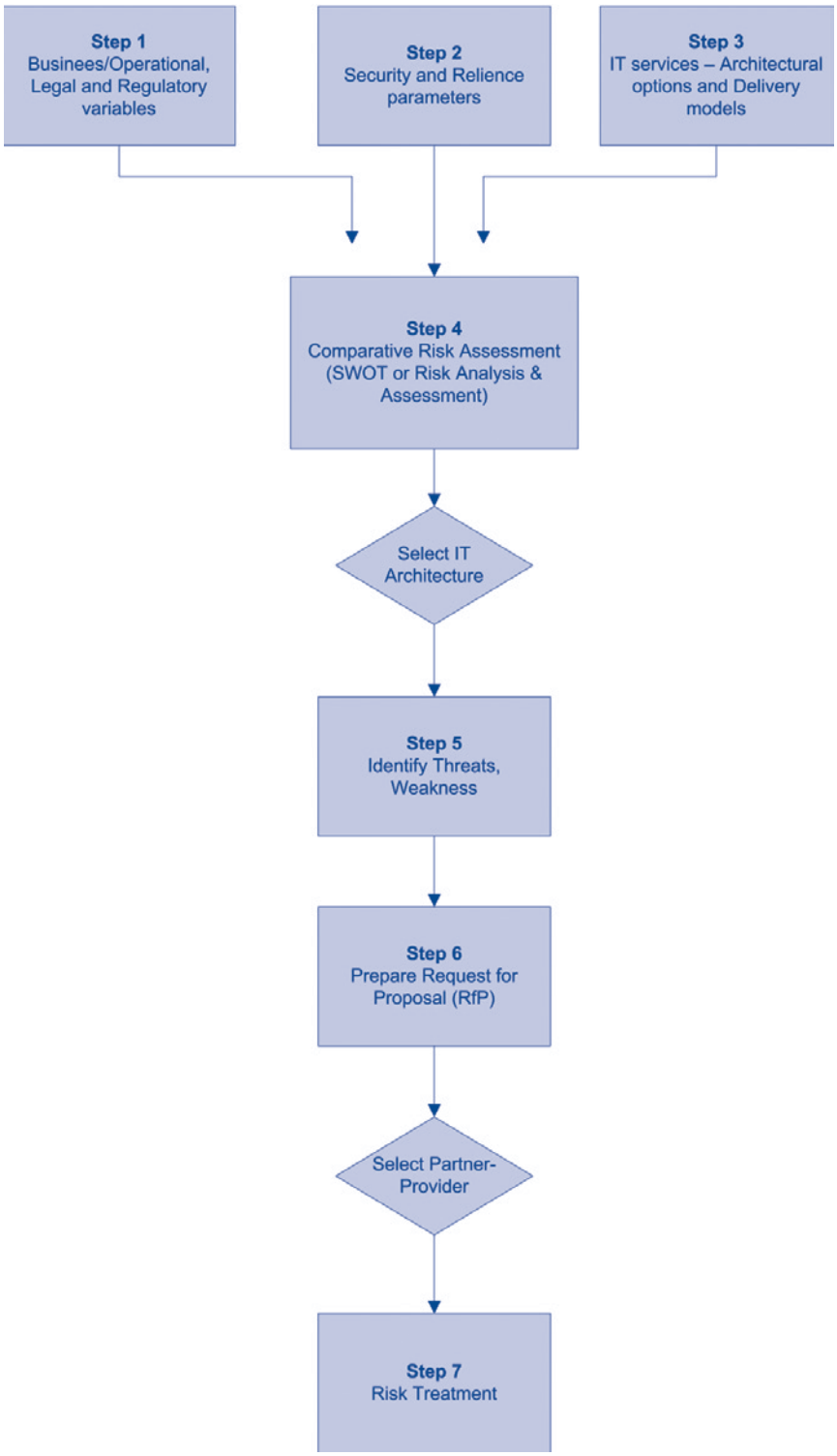
Tutto ciò richiede che le strutture ICT dei CSC sviluppino e maturino delle nuove competenze tali da consentire scelte corrette e di interagire in maniera efficace ed efficiente con le strutture tecniche e organizzative del CSP.

Un approccio di tipo metodologico alla scelta delle caratteristiche dei servizi e del CSP che li erogherà[17] assume quindi una grande importanza e a tal fine ENISA ha sviluppato un modello decisionale(op. cit.) pensato per il settore governativo ma applicabile a una grande varietà di contesti.

Il modello proposto da ENISA è rappresentato nella seguente figura 4 e prevede alcuni passaggi analitici per selezionare la soluzione cloud che meglio si adatta alle esigenze espresse.

[17] Nella fase di selezione della soluzione, è possibile avvalersi anche della metodologia maturata all'interno dell'esperienza CAMM (Common Assurance Maturity Model) che sta sviluppando dei controlli di sicurezza in grado di misurare e valutare i profili operativi dei CSP. Attraverso l'approccio proposto da CAMM, sarà quindi possibile avere una visione "top-down" delle capacità dei CSP nei settori della sicurezza, della governance e della compliance. http://common-assurance.com/

Fig. *4 – ENISA Model for decision-makers*



Questo modello intende definire un percorso che guidi le Amministrazioni pubbliche:

- nell'identificazione e nella raccolta dei requisiti di business e degli obblighi di conformità a leggi e regolamenti;
- nella definizione degli opportuni livelli di servizio in materia di sicurezza e resilienza
- nell'applicazione di una metodologia di analisi (SWOT analysis[18]) per la scelta della soluzione cloud che meglio risponde alle esigenze espresse;
- nella preparazione della "richiesta di servizio".

Per una descrizione dettagliata del modello ENISA si rimanda al documento già citato.

Allo scopo di semplificare l'approccio ai progetti di cloud computing, nel seguito si propone una selezione di raccomandazioni ritenute fondamentali - sia con espresso riferimento alla sicurezza dei servizi sia di carattere più generale -.

6.1 La definizione di una strategia

Tutta la letteratura in materia di cloud computing è concorde nel sottolineare la necessità di evitare scelte isolate e determinate da esigenze specifiche, privilegiando invece la definizione di una strategia complessiva di approccio al mondo cloud. Ogni potenziale CSC dovrebbe pensare a un proprio approccio che definisca correttamente i passi da compiere e le scelte da effettuare in modo progressivo, partendo da progetti semplici con impatti minimi sui "processi core" per poi evolvere verso applicazioni e sistemi a complessità e criticità crescente.

Ogni CSC dovrebbe quindi sviluppare una strategia di approccio al cloud che fissi le principali tappe di evoluzione nell'utilizzo del cloud, indicando in maniera chiara e inequivocabile i vincoli ritenuti fondamentali per procedere in sicurezza verso le condizioni che consentono di beneficiare dei vantaggi ad esso connessi.

Il documento di strategia deve riguardare:

- la definizione degli SLA di sicurezza e resilienza;

[18] La SWOT analysis è uno strumento di pianificazione strategica usato per valutare i punti di forza (Strengths), debolezza (Weaknesses), le opportunità (Opportunities) e le minacce (Threats) di un progetto o in un'impresa o in ogni altra situazione in cui un'organizzazione o un individuo deve prendere una decisione per raggiungere un obiettivo.

- la definizione di specifiche clausole per assicurare la conformità alla normativa attraverso una corretta distribuzione dei ruoli, delle responsabilità e dei rischi privacy;
- la gestione delle identità;
- l'utilizzo della cifratura;
- la sicurezza delle applicazioni;
- la gestione degli incidenti.

È di fondamentale importanza che si individui un percorso di attuazione degli adempimenti per il rispetto delle normative vigenti, non solo con riferimento alla protezione dei dati personali, ma anche delle eventuali normative di settore applicabili al caso concreto.

L'attribuzione di specifiche responsabilità in merito all'attuazione di tutto quanto disposto è certamente un'opzione che fornisce le migliori garanzie per una corretta realizzazione dei vari passi previsti e sarebbe opportuno che venisse nominato uno "Steering Committee" con lo scopo di monitorare e armonizzare tutte le varie fasi di attuazione della strategia.

6.2 La definizione dei requisiti

Per la valutazione dei servizi cloud, si ribadisce l'importanza di iniziare dalla raccolta e dall'analisi dei propri requisiti.

I CSP tendono a pensare i propri servizi in modo da evitare, per quanto possibile, le personalizzazioni, proponendo "pacchetti di servizi" normalmente chiusi e poco modificabili. Per confrontare questi "pacchetti di servizi" proposti dai vari CSP si dovrà disporre di un insieme di requisiti che rappresenti i "desiderata" del CSC. Solo mettendo a confronto ogni "pacchetto" con tali requisiti si potrà capire quanto ogni offerta sia vicina a bisogni espressi e valutare correttamente la gestione degli eventuali scostamenti.

6.3 La valutazione degli SLA

Il cloud computing propone uno schema di erogazione dei servizi che presuppone una perdita di controllo sui dati e sulle applicazioni da parte del relativo owner. In questo scenario è di fondamentale importanza che l'accordo o il contratto che fissa gli impegni delle parti sia il più chiaro possibile e non dia adito a possibili interpretazioni diversificate. È necessaria quindi un'attenta valutazione preventiva delle proposte di accordo che i vari CSP hanno elaborato.

I punti contrattuali che sono a maggiore impatto sui servizi erogati sono quelli che regolano gli SLA (Service Level Agreement) che devono essere sottoposti a un'attenta verifica del CSC rispetto ai requisiti espressi e ogni punto non risolto deve essere opportunamente trattato in via preventiva rispetto alla formalizzazione dell'accordo stesso.

Gli SLA costituiscono una precisazione fondamentale dell'oggetto di ogni accordo di servizio nel mondo cloud e devono essere espressi in modo comprensibile, chiaro e univoco. Un utile esercizio al fine della verifica dell'adeguatezza degli SLA è rappresentato dalla valutazione della loro rilevanza per la rappresentazione delle caratteristiche chiave dei servizi. Se gli SLA consentono di rappresentare correttamente l'andamento delle caratteristiche chiave dei servizi ed esprimono dei valori soglia ritenuti compatibili con i requisiti, si è in presenza di un accordo di soddisfazione sia per il CSC che per il CSP.

È opportuno inoltre che si verifichino gli algoritmi di misura degli SLA proposti dal CSP, comprovando l'effettiva misurabilità delle metriche nel contesto delle prestazioni erogate. Infine è bene che vi siano dei meccanismi di revisione degli SLA che possano essere attivati su richiesta del CSC o su base periodica.

6.4 Il Piano della Sicurezza

Il Piano della Sicurezza è il documento nel quale vengono indirizzate tutte le tematiche relative agli aspetti di sicurezza nell'utilizzo delle cloud. Come già detto al paragrafo 5.1, le migliori condizioni si verificano quando sia il CSC che il CSP hanno un proprio Piano della Sicurezza e, in fase di definizione degli accordi, procedono alle opportune verifiche di compatibilità operando tutte quelle modifiche che si rendano necessarie per armonizzare gli approcci.

Nella eventuale fase di scelta del CSP, la verifica del Piano della Sicurezza dei potenziali fornitori è molto importante per determinarne la compatibilità con la propria strategia di approccio e con le proprie scelte di sicurezza.

Il Piano della Sicurezza, per consentire un'effettiva valutazione e una integrazione delle scelte, deve trattare, al minimo, i seguenti punti:

- criteri e modalità di esecuzione delle tematiche di sicurezza fisica;
- criteri e modalità di esecuzione delle tematiche di sicurezza logica;
- criteri e modalità di esecuzione delle tematiche di sicurezza organizzativa;
- scelte in merito alla continuità operativa e al Disaster Recovery;
- indicazioni e procedure relative alla prevenzione e gestione degli incidenti,
- criteri di gestione degli aspetti di conformità alle leggi, agli standard e alle best practice.

Infine, dal punto di vista del CSC, il Piano della Sicurezza rappresenta una delle logiche conseguenze della Strategia di approccio al cloud e quindi dovrebbe contenere gli approfondimenti e i criteri di attuazione delle tematiche di sicurezza trattate in quel contesto.

6.5 La continuità dei servizi

Gli aspetti di continuità dei servizi sono particolarmente rilevanti nel mondo cloud e meritano un focus particolare. Data la perdita di controllo diretto sui dati e sulle applicazioni da parte del CSC e data la impossibilità di conoscere con esattezza la dislocazione fisica delle risorse assegnate, si determina una condizione per la quale gli aspetti di archiviazione dei dati, di disponibilità e di continuità dei servizi sono svolti dal CSP.

Nelle cloud, errori umani, malfunzionamenti di alcune componenti hardware o deliberati attacchi, hanno delle enormi potenzialità di impatto su moltissimi CSC. In questi casi la garanzia di poter accedere a copie dei dati opportunamente archiviate in sicurezza è il necessario presupposto per fruire dei servizi cloud. Inoltre, anche se la struttura stessa delle cloud è orientata alla resilienza, anche dal punto di vista della disponibilità dei servizi sono presenti grandi rischi dovuti alla distribuzione geografica e alla complicazione dei sistemi.

I CSP quindi devono curare con grande attenzione: la predisposizione delle misure di sicurezza a garanzia della disponibilità dei dati e dei servizi e la indispensabile descrizione formale delle stesse in modo da impegnarsi in obiettivi misurabili che possano essere effettivamente verificati dai CSC.

6.6 La gestione degli incidenti

Nel campo della gestione degli incidenti di sicurezza, le cloud pongono dei grandi interrogativi ai CSC. Infatti, la gestione dell'evento ricade interamente nella sfera di competenza del CSP pur essendo i dati, e in alcuni casi anche i servizi, di proprietà dei CSC. Questo intreccio di interessi può portare a situazioni molto difficili da gestire. Ad esempio, in presenza di commissione di reati, oltre alla ordinaria complessità di gestione si aggiungono anche le difficoltà legate all'intervento delle forze dell'ordine che, applicando le proprie procedure, superano le prassi concordate tra le parti.

È molto importante che, per quanto riguarda gli eventi rilevanti che possono avere degli impatti sull'operatività o sull'immagine dei CSC, vengano definite delle chiare modalità di comunicazione tra tutti i soggetti coinvolti e tra questi e i media. I CSP all'interno delle proprie proposizioni contrattuali dovranno inserire delle opportune clausole che fissino chiaramente gli obblighi e i limiti delle comunicazioni in merito alla gestione degli incidenti, consentendo ai potenziali CSC di valutare compiutamente e in via preventiva la compatibilità degli approcci proposti con le proprie esigenze e i propri requisiti.

7. Le sfide per il futuro

Sembra ormai generalmente accettato che il cloud computing avrà un ruolo fondamentale nel futuro dell'ICT. La crescita dell'offerta di mercato è stata rapida e ha superato anche ostacoli apparentemente insormontabili. È però ancora necessario consolidare le posizioni e creare quel clima di fiducia e di affidabilità che è il presupposto concreto per il raggiungimento degli ambiziosi obiettivi correlati alla diffusione di questo paradigma di erogazione dei servizi.

I temi che meritano attenzione e approfondimenti sono stati quindi indicati da politici, esperti e professionisti come fattori determinanti per lo sviluppo del cloud computing[19]. In questo capitolo sono elencate cinque "sfide" che, se rapidamente raccolte e indirizzate, abiliterebbero e faciliterebbero la diffusione del cloud computing all'interno delle Pubbliche Amministrazioni e in altri settori del mercato. È auspicabile che tutti gli *stakeholder* dell'ICT pubblica siano partecipi e allineati nella risoluzione di queste "sfide per il futuro".

7.1 Sfida 1: l'evoluzione normativa

Il cloud computing potrebbe avere un effetto dirompente, oltre che sul mercato, anche sulle normative in tema di trattamento dei dati. Infatti il modello cloud, pur non essendo in completo contrasto con le leggi in vigore, esaspera i limiti dell'attuale normativa nazionale ed europea in materia di protezione dei dati personali, soprattutto per quanto riguarda l'attribuzione di responsabilità e le tradizionali modalità di adempimento agli obblighi normativi.

Questo paradigma di erogazione di servizi sta però forzando molte resistenze e il cloud, di fatto, si sta diffondendo nel panorama ICT mondiale. Tutto ciò spiazza sia le Autorità garanti della protezione dei dati personali europee sia le componenti legali dei CSC che, dopo un primo momento di rigetto, stanno ora valutando correttivi da inserire negli accordi tra le parti.

[19] In particolare il documento "The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010" propone una via europea al miglioramento e allo sviluppo del cloud. In questo documento, partendo da una SWOT analysis, sono tratteggiate le specifiche possibilità di sviluppo che si aprono per l'Europa.
http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

Ad oggi, questi sforzi hanno soltanto portato a delle soluzioni parziali. Quindi nei Paesi maggiormente sviluppati, si sta facendo strada l'idea di dare vita a un nuovo approccio normativo che, pur mantenendo inalterati gli attuali principi ispiratori, sia reso compatibile con il cloud computing. Ad esempio a livello europeo la Commissione sta lavorando alla predisposizione di una "Strategia Europea per il cloud computing"[20] che ha come primo obiettivo la predisposizione di un nuovo impianto normativo che sappia coniugare: i diritti degli utenti, la protezione dei dati e la privacy, pur tenendo presente le connotazioni tipiche dei servizi "globali" erogati nel mondo del cloud computing.

La realizzazione di un nuovo set di regole consentirebbe di operare in un regime di maggiore certezza sia dal lato dei CSC sia dal lato dei CSP, favorendo quindi la realizzazione di servizi cloud a sempre maggiore valore aggiunto.

7.2 Sfida 2: la lotta al cyber crime

Il mondo cloud incontra il cyber crime almeno secondo due modalità: le grandi cloud pubbliche sono percepite dai cyber criminali come bersagli di valore e il cloud computing fornisce nuove possibilità e nuovi strumenti a chi ha deciso di percorrere la strada della criminalità informatica.

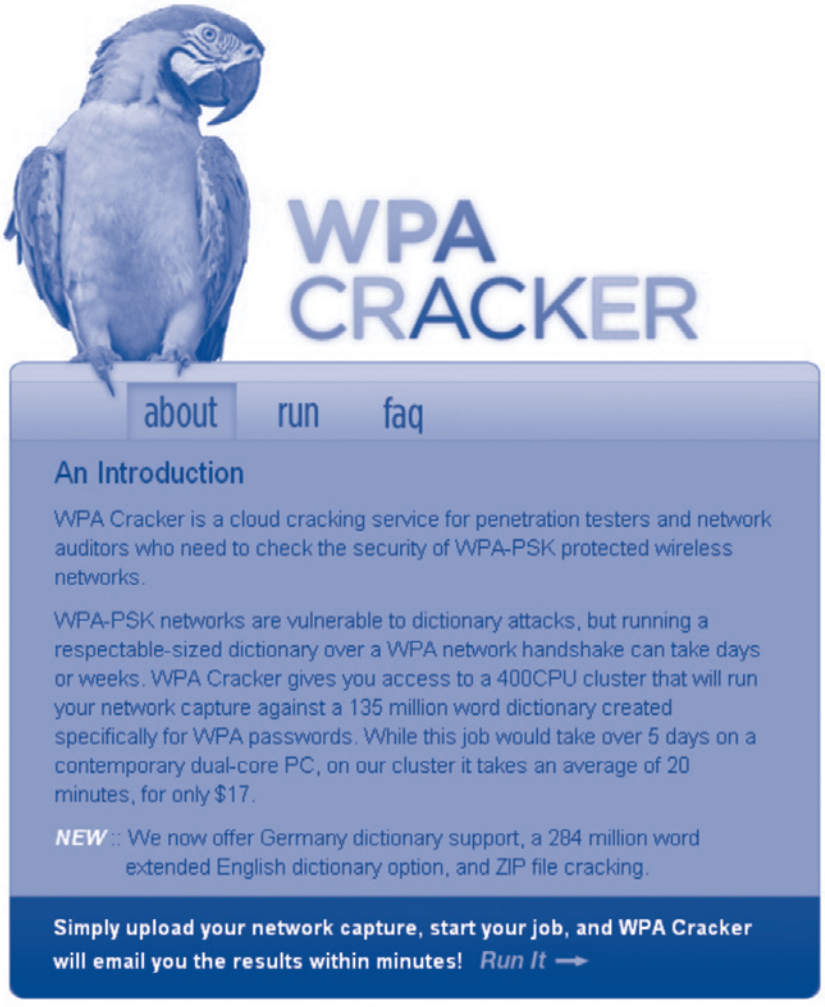
Prendendo in esame il caso in cui le cloud fungono da bersaglio dei cyber criminali, si possono mettere in evidenza molte motivazioni, tra cui:

1. le cloud pubbliche sono degli accentratori di grandi quantità di dati provenienti da molti clienti diversi (multi-tenant model);
2. una singola vulnerabilità o un singolo errore di configurazione possono comportare una grande superficie d'attacco per i criminali;
3. le successive indagini delle forze dell'ordine sono tecnicamente molto complesse;
4. la natura transnazionale delle cloud pubbliche complica ulteriormente la scena del crimine;
5. in caso di giudizio non ci sono ancora precedenti consolidati sul reperimento e sull'introduzione nel relativo procedimento giudiziale (produzione) delle prove a carico del trasgressore.

[20] La Commissione Europea si è impegnata a pubblicare la "European Cloud Computing Strategy" entro il 2012. A questo proposito, a maggio 2011, ha avviato una raccolta di pareri ed opinioni sulle modalità con le quali possono essere sfruttati al meglio i servizi di cloud computing in Europa.
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/575&format=HTML&aged=0&language=IT

Prendendo invece in esame il caso in cui le cloud fungono da strumento per realizzare crimini, si può partire dalla considerazione che una comune modalità di misura della robustezza di molti meccanismi di sicurezza è data dal tempo necessario per comprometterne il corretto funzionamento con i normali strumenti messi a disposizione dal mercato. Per cui molti meccanismi di sicurezza sono considerati sufficientemente robusti perché garantiscono di resistere per tempi considerati adeguati.

Il cloud computing sta mettendo seriamente in discussione questo approccio poiché, con estrema facilità e velocità, si possono realizzare (e poi successivamente dismettere) infrastrutture ICT capaci di grandi performance computazionali. Questa caratteristica, permettendo di superare le difficoltà economico-organizzative connesse alla realizzazione di sistemi ICT particolarmente performanti, può essere sfruttata dai criminali per portare attacchi altrimenti impossibili.



A dimostrazione delle reali potenzialità di questo tipo di approccio si riporta la home page di un sito che offre a "penetration tester and network auditors" la possibilità di sfruttare un "cloud cracking service" che mette a disposizione un cluster di 400 CPU per l'ottimizzazione della procedura di individuazione delle password di reti WiFi protette con algoritmo WPA.

Come si può leggere nel testo proposto dal sito, il tempo di calcolo richiesto per questa operazione passa da circa 5 giorni a 20 minuti e i costi sono di soli 17 dollari.

Inoltre, data la difficoltà nello svolgere indagini e individuare e assumere le prove nelle cloud, i crimini commessi sfruttando i servizi offerti dalle cloud sono, attualmente, di difficile approccio e risoluzione.

Devono essere predisposte misure di contrasto a questi fenomeni che consentano la crescita del mercato delle cloud, limitando al massimo gli impatti di questi fenomeni.

Quanto prima dovranno essere pubblicati standard di sicurezza collegati a relativi schemi di certificazione che, tenendo conto delle peculiarità delle cloud, contribuiscano a limitare gli "effetti collaterali" della natura condivisa di questi ambienti. Standard e certificazioni concorreranno ad aumentare i livelli di sicurezza e forniranno garanzie ai CSC su come la sicurezza viene affrontata dai vari CSP.

Dovrà essere fatto un grande sforzo a livello di standardizzazione delle procedure e degli strumenti di "forensic" nel mondo cloud in modo che le forze dell'ordine abbiano la possibilità di acquisire in modo efficiente, certo e affidabile le prove di quanto eventualmente accaduto.

Come sarà ribadito nel paragrafo 7.4, è auspicabile che siano promulgate normative omogenee e armoniche tra i vari Stati che consentano di minimizzare le limitazioni di intervento connaturate alla distribuzione internazionale dei data center che possono essere parte di una cloud. Queste normative costituiscono il presupposto necessario per riuscire a contrastare efficacemente il fenomeno del cyber crime, soprattutto nel mondo del cloud.

Infine, i codici di comportamento dei CSP dovranno essere e armonizzati e standardizzati in modo che gli utilizzi consentiti per le risorse siano strettamente limitati e sottoposti ad adeguati controlli. Ciò consentirebbe, tra l'altro, ai CSC di avere delle garanzie sull'utilizzo che viene fatto dagli altri clienti della cloud in modo da limitare al massimo i rischi di riflessi di azioni giudiziarie verso altri CSC (si veda paragrafo 4.2.5).

7.3 Sfida 3: la portabilità dei dati e delle applicazioni

Una delle maggiori preoccupazioni per l'adozione di servizi cloud è legata al rischio di "Lock-in" (si veda paragrafo 4.2.7). Trovare adeguate soluzioni a questa seria problematica è una delle priorità per superare gli impedimenti a una più ampia diffusione di questi servizi. Da questo punto di vista l'obiettivo è avere la possibilità di scegliere tra molteplici offerte che consentono successivi cambi e trasferimenti di dati e servizi in funzione della convenienza e dell'opportunità. L'interoperabilità è quindi essenziale affinché il mercato delle cloud sia equo, aperto e competitivo.

Gli sforzi devono quindi essere concentrati sull'eliminazione di tutte le barriere tecniche che tendono a vincolare i CSC a un dato CSP. In quest'ambito, nel cruciale contesto della definizione dei requisiti di sicurezza e compliance, un ruolo fondamentale sarà giocato proprio dal settore pubblico. Ad esempio, a livello nazionale, sarebbe utile disporre di una lista di requisiti considerati accettabili per la PA italiana, che fissi ad esempio:

- le tipologie di API e "data format";
- i controlli di sicurezza da introdurre;
- gli standard di servizio attesi per le varie tipologie di applicazione.

In questo modo, le forniture di servizi cloud per la PA potrebbero avere caratteristiche standard favorendo la portabilità del servizio e creando modelli riutilizzabili dagli altri attori del mercato, prime tra tutte le piccole e medie imprese (PMI). Gli sforzi internazionali per la standardizzazione[21], recependo in parte le istanze nazionali, avranno un ulteriore benefico impatto sul cloud computing. La definizione di standard consentirà la creazione di un fiorente mercato costituito da attori impegnati in una sana competizione con vantaggi equamente distribuiti tra i CSC e i CSP. Inoltre, con la realizzazione di una piena interoperabilità e portabilità di dati e servizi, anche gli altri attori del cloud computing, quali ad esempio i Cloud Service Developer e i Cloud Service Distributor, avranno dei benefici in termini di efficienza e di riuso delle soluzioni che sapranno realizzare, a tutto vantaggio della solidità del mercato stesso.

Parafrasando i concetti espressi dalla Responsabile della Digital Agenda Europea, la vice presidente della Commissione Europea Neelie Kroes(op. cit.), se saranno individuate adeguate soluzioni al problema dell'interoperabilità e della portabilità dei dati, cogliendo tutti i requisiti provenienti dagli attori coinvolti, il cloud computing potrà diventare un mezzo per i governi e le Amministrazioni Pubbliche per fornire servizi più efficienti ed economici a cittadini e imprese.

7.4 Sfida 4: l'approccio transnazionale

Le cloud, soprattutto se di tipo pubblico, sono costituite da un'infrastruttura di datacenter fisicamente distribuiti in molte parti del mondo. Maggiori sono le dimensioni delle cloud, maggiore è la distribuzione geografica dei data center e maggiori sono i vantaggi di esercizio per i CSP.

Tra le implicazioni principali che la distribuzione geografica comporta, si devono annoverare i possibili impatti sui servizi erogati dalle cloud a causa delle diverse legislazioni nazionali che regolano le attività ICT nei Paesi dove sono distribuiti CSP, CSC e i data center. Ogni attore di questa catena, facendo leva su una legge nazionale, potrebbe causare impatti anche rilevanti sui servizi erogati. Questi impatti, inoltre, sarebbero di difficile risoluzione da parte degli altri attori coinvolti proprio per il loro carattere transnazionale.

[21] In questo specifico campo, la Commissione Europea ha varato numerosi progetti e proposte tra cui vale la pena di ricordare SIENA (Standards and Interoperability for eInfrastructure ImplemeNtation InitiAtive 2010-2012), che è un'iniziativa concepita per contribuire alla definizione di una roadmap per le future infrastrutture europee con particolare attenzione all'interoperabilità e agli standard, attraverso la definizione di scenari, l'identificazione delle tendenze e l'analisi dei possibili impatti del cloud computing.
http://cordis.europa.eu/fp7/ict/e-infrastructure/docs/siena.pdf

Un'altra implicazione importante per le cloud è legata alla modalità di accesso ai dati e ai servizi che, tipicamente, avviene attraverso la rete Internet. Alcuni accadimenti internazionali, hanno messo in evidenza che, in alcune situazioni, come estrema misura, i governi nazionali possono decidere il completo isolamento di un paese dalla rete Internet. Questa condizione, nel caso di un paese che ospita un data center di una cloud, avrebbe un impatto difficilmente arginabile dal CSP sui servizi erogati.

È evidente quindi che, per consentire di diffondere il paradigma cloud anche per applicazioni "mission critical" o per i servizi erogati da enti governativi, è necessario che siano introdotte a livello internazionale delle misure volte a contrastare i fenomeni sopra ricordati.

In particolare deve essere trovata una modalità di armonizzazione delle legislazioni nazionali che regolano la materia ICT, trovando definizioni comuni di ciò che è consentito e vietato e individuando opportune modalità di approccio comune. Inoltre, in maniera analoga alla Corte Internazionale di Giustizia, che si occupa di dirimere le dispute fra Stati membri dell'ONU che hanno accettato la sua giurisdizione, dovrebbero essere determinati i soggetti e le sedi internazionali deputate all'individuazione di possibili soluzioni legate all'interpretazione e all'applicazione degli accordi internazionali sulle cloud.

Le problematiche affrontate rimandano a temi più generali su cui la comunità internazionale si sta interrogando per trovare soluzioni condivise su:

- la natura di Internet;
- le modalità con le quali possono essere affrontati possibili attacchi, statuali e non, che fanno uso della rete;
- la liceità della realizzazione e dell'utilizzo del cosiddetto "Internet Kill Switch" che permette di isolare completamente alcuni Stati, se non il mondo intero, dalla rete Internet.

7.5 Sfida 5: le best practice e le certificazioni

Parte delll'immaturità del mercato cloud dipende anche dall'attuale mancanza di standard certi e ampiamente riconosciuti dal mercato. Soprattutto nel campo della gestione della sicurezza si percepisce una mancanza di riferimenti certi a cui possono guardare i CSC per valutare gli approcci proposti dai CSP.

Inoltre, uno dei principali rischi per il cloud computing è legato alla perdita di governance e controllo su dati e applicazioni (si veda paragrafo 4.2.6) e in parte è determinato dalla impossibilità per i CSC di eseguire audit e assessment. Questa impossibilità di accesso diretto, al momento, si traduce inevitabilmente per il CSC in una passiva accettazione di quanto dichiarato dal CSP a proposito dei propri approcci e delle proprie procedure di sicurezza.

In generale, in tutte le casistiche in cui gli audit di seconda parte sono considerati inattuabili, il mercato ha proposto una valida soluzione alternativa attraverso l'introduzione di normative, standard e best practice associate a un sistema di verifiche di terza parte con produzione di certificazioni ampiamente riconosciute.

Questa evoluzione deve essere ancora compiutamente realizzata nel mondo cloud, sarà perciò una grande sfida per il futuro riuscire ad assistere a un percorso di mutuo riconoscimento da parte dei vari CSP delle migliori pratiche corredato da un iter evolutivo finalizzato all'implementazione di questi nuovi standard.

La presenza di un forte sistema di controlli e certificazioni di terza parte sarà quindi uno degli indicatori che mostreranno l'avvenuta maturazione del mercato dei servizi cloud.

Ringraziamenti

Molte persone hanno contribuito alla stesura di questo documento fornendo preziose indicazioni e utili suggerimenti. In particolare devono essere menzionati i colleghi Massimo Fedeli e Gabriele Mezzacapo che hanno formato il team di supporto alla redazione del documento. Inoltre, una fondamentale funzione di guida e indirizzo è stata svolta da Gaetano Santucci che ha indicato gli obiettivi e le mete verso cui puntare. Altri colleghi come Alessandro Grilli, Domenico Fumarola e Luana Angelone hanno contribuito alla revisione e al miglioramento di questo Quaderno.

Infine, un caloroso ringraziamento va a Paolo Balboni (partner di ICT Legal Consulting) per la revisione ed integrazione degli aspetti legali e a Daniele Catteddu (ENISA) per i numerosi approfondimenti proposti. Il loro contributo, le loro idee e la loro attiva partecipazione hanno consentito di pubblicare un Quaderno migliore e più completo.

Referenze

	Ente	Titolo	Codice	Data pubblicazione
1	NIST	The NIST Definition of Cloud Computing (Draft)	SP 800-145	Gennaio 2011
2	NIST	Cloud Computing Taxonomy	Preliminary Draft	Gennaio 2011
3	Cloud Computing Use Case Group	Cloud Computing Use Case	Version 4.0	Luglio 2010
4	ENISA	An SME perspective on Cloud Computing	-	Novembre 2009
5	Cloud Computing Use Case Group	Moving to the Cloud	Version 1.0	Febbraio 2011
6	GSA	Proposed Security Assessment & Authorization for US Government Cloud Computing	Draft version 0.96	Novembre 2010
7	ENISA	Security & Resilience in Governmental Clouds – Making an informed decision	-	Gennaio 2011
8	US Chief Information Officer	Federal Cloud Computing Strategy	-	Febbraio 2011
9	ENISA	Cloud Computing – Benefits, risks and recommendations for information security	-	Novembre 2009
10	Cloud Security Alliance	Top Threats to Cloud Computing	Version 1.0	Marzo 2010
11	Cloud Security Alliance	Security Guidance for Critical Areas of Focus in Cloud Computing	Cer 2.1	Dicemrbe 2009
12	Gartner	Four Risky issues when contracting for cloud services	G00210385	Febbraio 2011
13	EU Commission	European Cloud Computing Strategy needs to aim high	Speech/11/199	Marzo 2011

Design:
Crea Identity Srl
www.creaidentity.com