

CARATTERIZZAZIONE DEI SISTEMI CLOUD PER LA PUBBLICA AMMINISTRAZIONE

versione 1.0



AGENZIA PER L'ITALIA DIGITALE

INDICE

PREFAZIONE	4
1. IL CLOUD COMPUTING NELLA PUBBLICA AMMINISTRAZIONE	5
1.1 Servizi Cloud di interesse strategico per la PA	8
1.2 Scenari di adozione	10
1.3 Architetture da adottare per i nuovi servizi di e-Government.....	12
1.4 Ruoli della PA nel Cloud Computing	14
1.5 OpenStack	15
2. MODALITÀ DI EROGAZIONE DI SERVIZI CLOUD	17
2.1 Servizi IaaS in gare “infrastrutturali” e “applicative”	18
2.1.1 Servizi di Datacenter basati su Cloud Computing	18
2.1.2 Macchine virtuali off-the-shelf per servizi di piattaforma	19
2.2 Servizi PaaS in gare “applicative”	20
2.3 Servizi SaaS in gare “applicative”	21
3. REQUISITI NON-FUNZIONALI DEI DATA CENTER	23
3.1 Caratteristiche generali dei Data Center.....	23
3.2 Categorie di servizi di Datacenter	25
3.3 Classificazione dei Data Center secondo l'affidabilità.....	26
3.4 Green Computing	28
4. REQUISITI NON-FUNZIONALI DEI SERVIZI CLOUD	30
4.1. Aree di controllo dei requisiti.....	30
4.1.1. Conformità	31
4.1.2. Interoperabilità	32
4.1.3. Governance dei dati	33
4.1.4. Sicurezza	34
4.1.5. Gestione	34
4.1.6. Resilienza	35
4.2. Specifiche trasversali ai servizi.....	35
4.2.1. Requisiti di conformità	36
4.2.2. Requisiti di interoperabilità	37
4.2.3. Requisiti di governance dei dati	38
4.2.4. Requisiti di sicurezza	40
4.2.5. Requisiti di gestione	53
4.2.6. Requisiti di resilienza	55
4.3. Classi di servizio	60



4.3.1.	Classi di servizi IaaS	60
4.3.2.	Classi di servizi PaaS	60
4.3.3.	Classi di servizi SaaS	60
4.3.4.	Tabella dei requisiti per classi di servizio	61

BIBLIOGRAFIA	63
---------------------	-----------



PREFAZIONE

Il presente documento ha lo scopo di orientare le soluzioni di sistemi di Cloud Computing in ambito SPC ed è pertanto diretto ai datacenter delle Pa che vorranno seguire una logica di razionalizzazione e integrazione, al mercato interessato alle prossime gare SPC (compresa quella appena bandita alla data di uscita del presente documento), ai privati interessati a qualificare la propria offerta secondo i bisogni della PA e le linee di indirizzo dell'Agenzia, ai nuovi datacenter che verranno realizzati. Il documento intende inoltre essere una prima linea di indirizzo per la certificazione delle soluzioni cloud per la PA, in attuazione delle regole tecniche per la qualificazione dei fornitori SPC e della certificazione dei servizi in corso di emanazione.

L'Agenzia persegue un piano di integrazione a livello europeo e segue i gruppi di lavoro UE ed i relativi progetti al fine di determinare condizioni di interoperabilità non solo a livello nazionale ma anche europeo, in linea con gli indirizzi dell'agenda digitale europea. In particolare l'Agenzia porterà in Europa l'esperienza nazionale in questo settore, così come in altri, e recepirà le indicazioni che perverranno dalla Commissione UE, in maniera da favorire la competitività degli investimenti che in questo settore verranno fatti in Italia.



1. IL CLOUD COMPUTING NELLA PUBBLICA AMMINISTRAZIONE

La Pubblica Amministrazione, come del resto il settore privato, sta valutando da qualche anno l'adozione del Cloud Computing per la gestione delle proprie infrastrutture e l'erogazione dei propri servizi ICT. Per ottenere una concreta utilità, è indispensabile che le scelte verso questa direzione siano calate all'interno delle specifiche esigenze della PA. La messa a punto di un quadro strategico ampio e chiaro è indispensabile e presuppone la conoscenza dei concetti fondamentali e delle principali criticità del Cloud Computing, per un approfondimento dei quali si rimanda al lavoro di cui in [2].

Vediamo nel seguito, brevemente e solo a scopo introduttivo, gli elementi fondanti del Cloud Computing.

Virtualizzazione

E' il procedimento di astrazione delle componenti fisiche degli elaboratori (cioè dell'hardware) eseguito allo scopo di renderle disponibili in forma di risorsa virtuale al software soprastante. Attraverso la virtualizzazione è possibile, quindi, installare sistemi operativi e relative applicazioni su macchine virtuali, costituite dall'insieme di componenti hardware virtuali, quali dischi rigidi, memoria, processore, interfacce di rete, che non sono mappate identicamente su componenti fisiche.

Architetture Orientate al Servizio

Sono architetture software pensate per l'erogazione di servizi web che consentono l'interoperabilità tra diversi sistemi. Le singole applicazioni diventano componenti di un processo di business generale, ovvero non dipendente da un particolare sistema. E' possibile così soddisfare le richieste degli utenti in modo integrato (cioè avvalendosi della composizione dei servizi di più sistemi) e trasparente (ossia senza introdurre evidenze di tale composizione).

Sistemi distribuiti

Si tratta di un insieme di calcolatori, interconnessi tra loro da una rete, che condividono risorse. I calcolatori possono essere eterogenei, possono avere diverse funzioni e possono essere connessi da reti di vario tipo e dimensione, scambiandosi messaggi basati su diversi protocolli.

Reti a banda larga



Sono basate su interconnessioni veloci alla rete Internet, realizzate ad esempio tramite fibre ottiche, ma anche con sistemi mobili di telecomunicazioni di terza e quarta generazione (3G, 4G), seppur caratterizzate da un'ampiezza di banda notevolmente inferiore rispetto ai sistemi cablati in fibra ottica. L'evoluzione dei sistemi cablati viaggia ora verso la cosiddetta banda ultralarga grazie all'avvento delle Next Generation Network.

Browser as a platform

Si riferisce alla possibilità di sostituire gli applicativi desktop, con servizi fruibili direttamente online attraverso un browser, con il vantaggio dell'ubiquità e dell'accesso trasparente da sistemi eterogenei.

Autonomic System

L'Autonomic Computing ha lo scopo di fornire ai computer gli strumenti necessari per autogestirsi senza l'intervento umano. In un sistema autoamministrato, l'operatore umano non deve controllare il sistema direttamente. Piuttosto, egli definisce politiche generali a regole date in input al processo di autogestione, le cui aree funzionali sono: autoconfigurazione, autoguarigione, autoottimizzazione, autoprotezione.

Web 2.0

E' lo stato di evoluzione del World Wide Web, che fa capo all'insieme di tutte quelle applicazioni online che permettono un elevato livello di interazione tra il sito web e l'utente, come i blog, i forum, le chat, i wiki, le piattaforme di condivisione di media, i social network.

Framework per applicazioni web

Framework software progettati per supportare lo sviluppo di siti web dinamici, applicazioni e servizi web, aventi per scopo l'alleggerimento del lavoro associato allo sviluppo delle attività più comuni di un'applicazione web e l'adozione di tecniche di riuso di codice.

Service Level Agreement

Accordo sul livello del servizio, ovvero strumenti contrattuali attraverso i quali si definiscono le metriche di servizio (es. qualità del servizio) che devono essere rispettate da un fornitore di servizi (provider) nei confronti dei propri clienti/utenti.

Modelli di servizio Cloud

- Cloud Software as a Service (SaaS)



- Uso delle applicazioni del provider sulla piattaforma Cloud
- Cloud Platform as a Service (PaaS)
 - Deployment di applicazioni custom sulla piattaforma Cloud, sfruttando i servizi PaaS disponibili
- Cloud Infrastructure as a Service (IaaS)
 - Affitto di storage, risorse computazionali, capacità di rete e altre risorse sulla piattaforma Cloud – le risorse computazionali possono essere fornite in macchine virtuali di varie taglie, oppure possono essere rese disponibili in *bundle* di risorse opportunamente bilanciati tra le diverse tipologie, a partire dai quali costruire macchine virtuali alla bisogna.

Modelli di deployment

- Cloud privata
 - Posseduta (o in affitto) dalla PA
- Cloud di comunità
 - Infrastruttura condivisa per una specifica comunità
- Cloud pubblica
 - Posseduta dal fornitore e aperta al pubblico
- Cloud ibrida
 - Composizione di due o più Cloud
- Posizionamento della Cloud On/Off-premises

Per una strategia della PA nel Cloud, occorre innanzi tutto tenere presente che l'IaaS è un punto di transizione naturale dai Datacenter tradizionali. I servizi di base offerti dall'IaaS, in forma quantizzata e su richiesta, sono la computazione (CPU e RAM), la memorizzazione e la rete. Le macchine virtuali garantiscono la piena fungibilità delle risorse che costituiscono i servizi. **Le barriere più critiche per l'adozione di soluzioni Cloud risultano essere quelle determinate dall'interoperabilità, dalla sicurezza e dalla privacy.** Per quanto concerne l'interoperabilità delle soluzioni intesa come comparabilità e flessibilità di passaggio tra diverse soluzioni il presente documento intende fornire, allo stato attuale della tecnologia, dei ragionevoli indirizzi. Per la parte di sicurezza e privacy l'adozione dello scenario SPC, la sottomissione alle regole e alle procedure di sicurezza rappresentano una garanzia per le PA.



1.1 Servizi Cloud di interesse strategico per la PA

La Figura 1 mostra il diagramma logico di Sam Johnston, che raffigura i servizi Cloud per tipologia (content, collaboration, communication, identity, runtime, compute, storage, ecc.) e livello (applicativo, di piattaforma e infrastrutturale) e con le principali modalità di accesso.

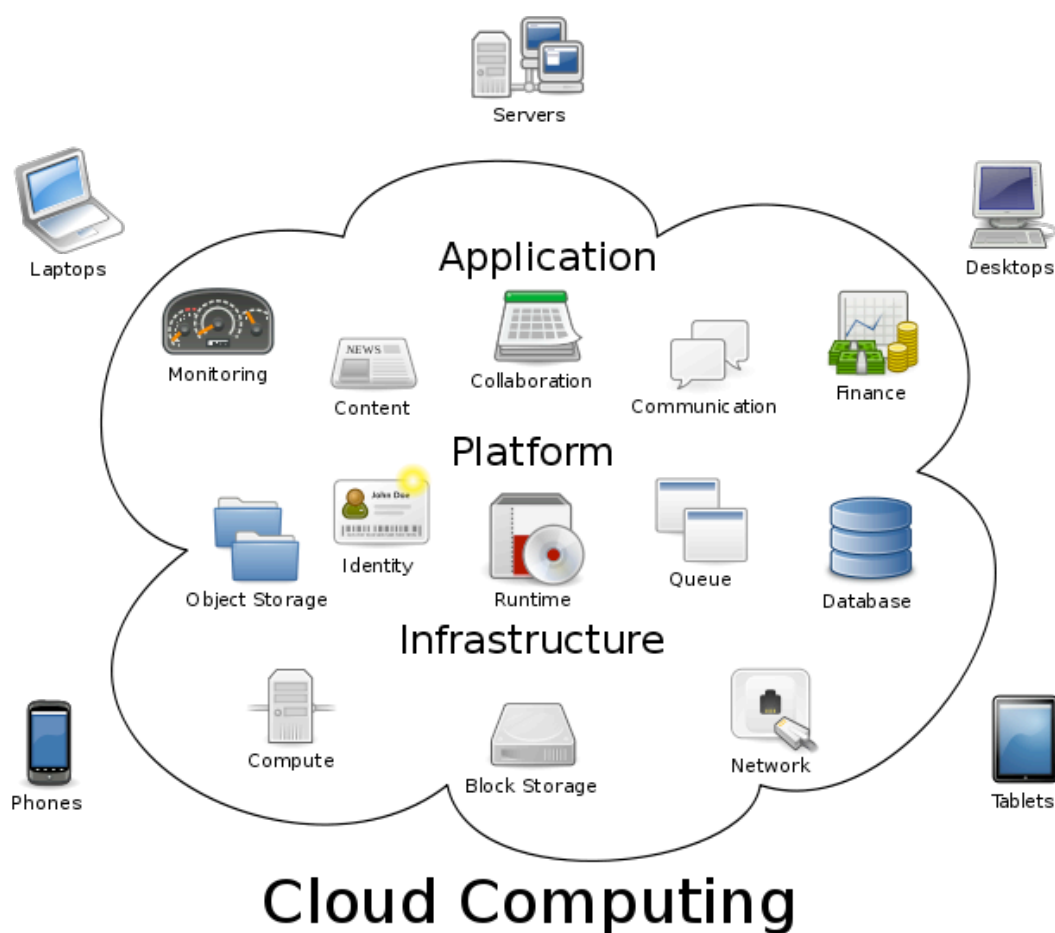


Figura 1



La Figura 2, invece, presenta nello specifico alcuni servizi di interesse strategico per la PA, all'interno di una categorizzazione architetturale e non funzionale, che non esclude, ovviamente, la domanda o l'offerta di altri servizi di varie tipologie e a vari livelli.

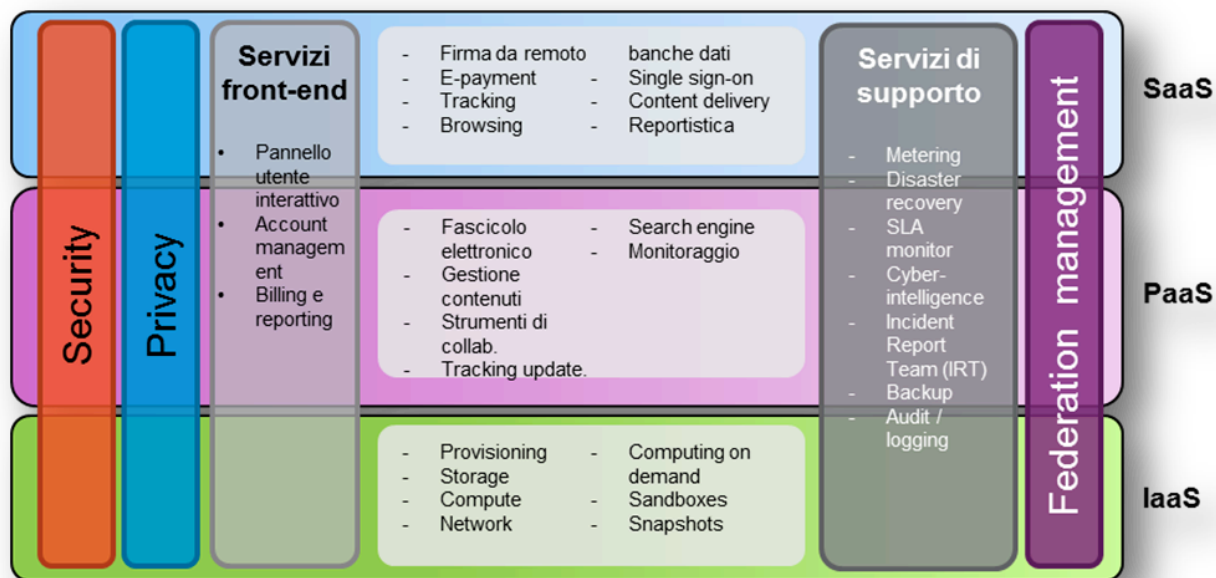


Figura 2

Vediamo in particolare le tipologie di servizio individuate suddivise per livelli e ambiti.

Servizi infrastrutturali:

- Risorse elaborative: compute
- Risorse memorizzazione: storage (object e block)
- Risorse di rete
- Funzionalità di backup e restore
- Disaster Recovery con “availability zones”
- Content delivery: CDN
- Identity management

Servizi di piattaforma:



AGENZIA PER L'ITALIA DIGITALE

- Application hosting
- DB as a Service
- Web hosting
- Media Hosting
- Strumenti di collaborazione (Collaboration service)
- Strumenti di comunicazione (Unified communication)
- Search engines
- CMS (gestione contenuti)
- Single Sign-on (SSO) e identità federate
- Data visualization e infografica di banche dati

Servizi software:

- E-Payment
- Reportistica
- Firma digitale
- Strumenti di qualificazione e certificazione
- Fascicolo elettronico
- Protocollo
- Document management

Servizi di sicurezza:

- Cyber-intelligence
- SIEM: security information and event management
- Security Intelligence and Risk Management

1.2 Scenari di adozione



- Le PA possono usare Cloud ibride (pubbliche-private).
- Il Datacenter di una PA grande può evolvere e diventare una Cloud privata, da condividere con altre PA.
- Una PA piccola può usare SaaS su Cloud pubbliche o private di grandi PA e minimizzare così la crescita di data center.
- I fornitori di Cloud pubbliche e private possono essere spinti ad usare standard per lavorare con le PA.

Un possibile percorso di avvicinamento è illustrato nel seguito:

- Sviluppo di cloud private:
 - Costruzione di una cloud privata
 - Ottenimento di una virtual private cloud
 - Consolidamento e migrazione dei data center a cloud private (completamente virtualizzati)
- Costruzione o ottenimento di cloud di community:
 - Disaster recovery per le cloud private
 - Realizzazione di PaaS su IaaS
- Uso di tecnologie per cloud ibride:
 - Portabilità del carico tra diverse cloud

Ovviamente la portabilità e l'interoperabilità partono dal presupposto di stabilire e adottare degli standard relativi a:

- Formato delle VM utilizzate - non essendo possibile imporre un singolo formato è necessario che i vari vendor di soluzioni di virtualizzazione siano in grado di importare VM che hanno formati di altri vendor (VMDK, VHD, QCOW2, ecc.)
- Interfaccia API dello IaaS basate su standard

A tale proposito e come vedremo anche nel seguito (par. 1.5), si ritiene che OpenStack abbia la maturità e la diffusione tale da poter essere considerato come standard di riferimento.

Infine una nota sul Disaster Recovery. Un modello di base di DR può essere l'utilizzo nella Community Cloud delle "availability zones" (presenza di più di un Datacenter su cui è basata l'infrastruttura della piattaforma cloud) con mirroring automatico e costante delle risorse storage e delle immagini delle risorse compute. Questo sistema rende possibili maggiori garanzie di disponibilità dei servizi.



1.3 Architetture da adottare per i nuovi servizi di e-Government

Nel modello SPC, saranno contemplate solo le architetture di modelli di servizio che prevedono la presenza di tutti i modelli di servizio, dall'IaaS in su, ovvero le architetture velate di rosso in Figura 3.

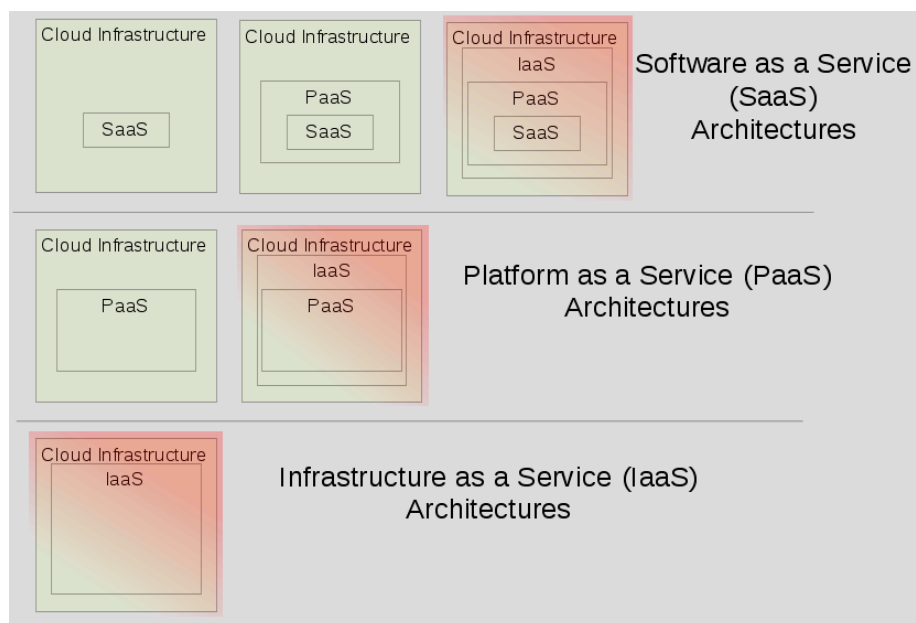


Figura 3

Gli obiettivi che si intende cogliere con il nuovo modello SPC sono, infatti, i seguenti:

- **Eliminare soluzioni legacy** e per questo si richiede, anche nel caso di fornitura di servizi PaaS, che lo strato su cui poggiano sia IaaS standard). L'adozione di uno specifico modello a larga diffusione e basato su interfacce aperte è dunque raccomandabile.
- **Abilitare misurazioni trasparenti** che consentano di controllare il rispetto degli accordi sul livello di servizio in modo strutturato e conferme al modello Cloud, garantendo efficienza e risparmio, oltre a fornire strumenti puntuali per la valutazione della riduzione degli sprechi.
- **Introdurre architetture standard** nell'interesse delle PA (modularità e riuso), del mercato (concorrenza) e nel rispetto delle normative europee in materia di concorrenza.
- **Integrare fornitori diversi** riducendo drasticamente il rischio di lock-in.



A tal proposito si riporta quanto ha dichiarato il commissario europeo Neelie Kroes: “Gli utenti devono essere in grado di cambiare il proprio cloud provider il più rapidamente e facilmente possibile come la modifica del fornitore Internet o Mobile lo è diventata in molti posti”.

Questo comporta l'adozione di uno standard di interoperabilità per i modelli di servizio, in particolare per lo IaaS che di fatto costituisce le fondamenta dell'architettura a strati descritta sopra. La varietà di software e piattaforme Cloud disponibili, anche a livello PaaS e SaaS, presenta una grande sfida nelle scelte che la PA dovrà operare. Da un lato si devono offrire pari opportunità a tutti i player di mercato, dall'altro occorre garantire il massimo livello di interoperabilità tra sistemi e amministrazioni, evitando gli sprechi derivanti da scelte parziali. Per queste ragioni è necessario adottare specifiche aperte, come quelle offerte dal gruppo di lavoro OGF *Open Cloud Computing Interface* e incoraggiare tutti i fornitori che intendano giocare un ruolo nella partita a supportare quello standard [8].

Resta inoltre assolutamente necessario che le soluzioni basate sul Cloud Computing garantiscano il massimo della visibilità e del controllo, siano pienamente documentate e si attengano agli standard internazionali, anche tenendo conto delle questioni sollevate in tema di Privacy dal Garante della Protezione dei Dati Personali: "La direttiva UE sulla privacy è obsoleta, bisogna rivederla con un accordo internazionale. E, nell'attesa, sarebbe opportuno che i fornitori "notificassero" (cioè sottoponessero) i propri servizi cloud ai Garanti europei”.

Al fine di garantire il pieno controllo sull'intero stack Cloud, anche nel rispetto delle disposizioni in materia di tutela della privacy, la fornitura di servizi PaaS e SaaS deve poter offrire e garantire anche servizi IaaS di base. In questo caso è consigliabile, ai fini di una maggiore efficienza tecnologica e commerciale, l'adozione di soluzioni ad-hoc a taglie prestabilite di IaaS (descritte nella sezione 4.1.2), dal momento che il fornitore ha il pieno controllo su tutto il progetto del sistema. Ciò non esclude, in ogni caso, la possibilità di adottare servizi IaaS di granularità fine (descritte nella sezione 4.1.1), sui quali costruire successivamente (ed eventualmente) altri servizi di livello PaaS e SaaS anche di altri fornitori. In ognuno di questi casi, è opportuno che tutti i livelli siano sfilabili ed erogabili da altri fornitori, cosa che presuppone, ripetiamo, l'adozione di standard universalmente riconosciuti ed accessibili.

Viene dunque richiesto a chi offre servizi PaaS di poter fornire, opzionalmente, una propria piattaforma IaaS. In particolare, nell'ambito di bandi di tipo “Infrastrutturale” dovrebbero essere previsti servizi IaaS di base a granularità fine, mentre per bandi di tipo “Applicativo” le soluzioni PaaS/SaaS richieste dovranno appoggiarsi su servizi IaaS già in dotazione o su altri a taglie prestabilite predisposti ad-hoc.

A maggior supporto a tale indicazione, è opportuno ricordare anche che il contenimento dei costi, l'integrazione e l'interconnessione sono previsti dal Codice dei Contratti Pubblici. Inoltre nel nuovo CAD si parla esplicitamente di economicità, disaster recovery, continuità operativa, valutazione comparativa e riuso, tutti obiettivi perseguibili attraverso scelte che introducano modelli basati su sistemi Cloud e in particolare quelli strutturati sulla base di standard internazionali aperti. Si rammenta che l'opzione “cloud” è stata specificamente introdotta di recente proprio all'art. 68 del CAD tra le scelte oggetto di valutazione comparativa.



1.4 Ruoli della PA nel Cloud Computing

La Figura 4 illustra il modello concettuale di riferimento del Cloud Computing proposto dal NIST (National Institute of Standards and Technology) per quanto attiene agli attori e alle attività e funzioni da essi svolte.

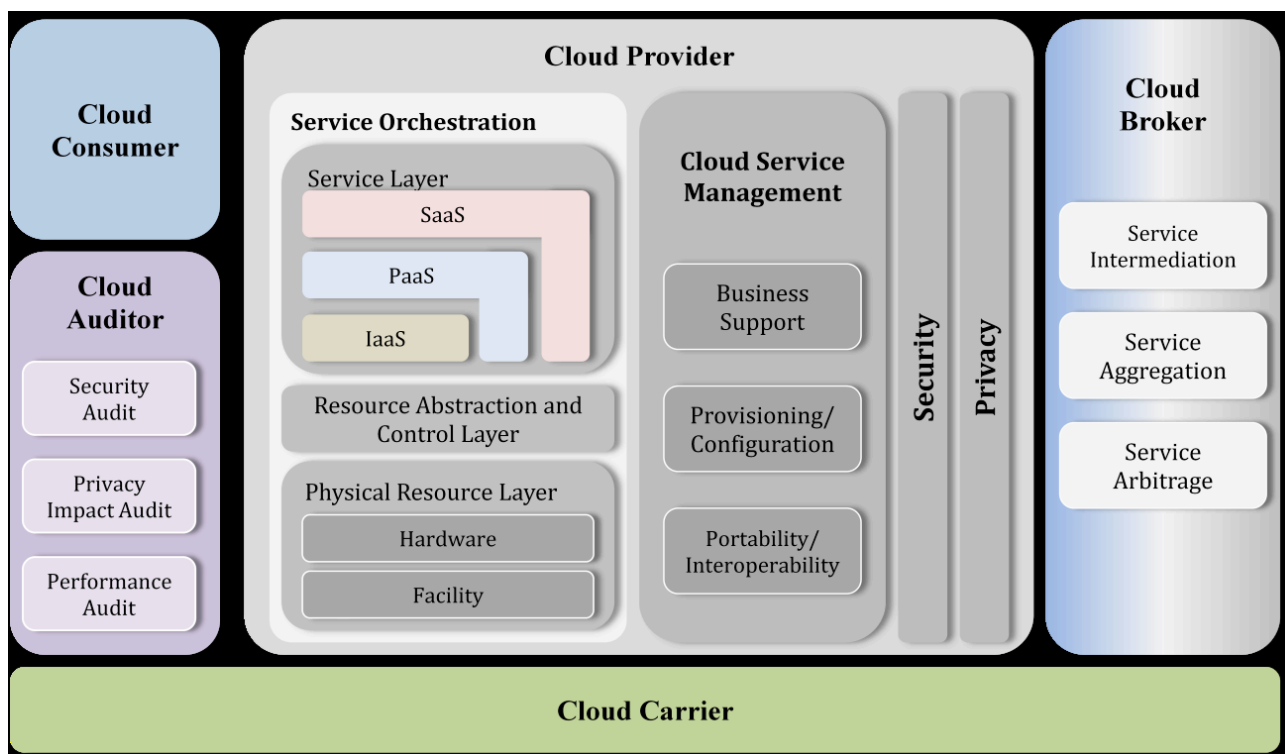


Figura 4

Con particolare riferimento alle infrastrutture Cloud dedicate alla PA, i ruoli che possono venire in rilievo sono:

- il **Cloud Provider**, che acquisisce e gestisce le infrastrutture elaborative necessarie a fornire i servizi, assicura l'esecuzione dei programmi che consentono i servizi, e le infrastrutture per erogare i servizi attraverso la rete;
- il **Cloud Consumer**, ossia l'utente o l'organizzazione che utilizza i servizi di cloud computing e che sottoscrive un contratto con il Cloud Provider. Il Cloud Consumer



esamina il catalogo dei servizi di un cloud provider, richiede specifici servizi e li utilizza. Il Cloud Consumer utilizza degli accordi sui livelli di servizio (Service Level Agreements, SLA) per specificare i requisiti sulle prestazioni tecniche che devono essere soddisfatti da un Cloud Provider;

- il **Cloud Auditor**, il soggetto che può eseguire un esame indipendente sui controlli effettuati sui servizi erogati da un Cloud Provider, con il fine di esprimere un parere ad esempio in merito alla sicurezza, all'impatto sulla privacy e al livello delle prestazioni [10].

Come evidenziato in [2], attualmente non esistono delle norme specifiche, nazionali o comunitarie, che disciplinino l'erogazione di servizi di Cloud Computing. Ma come descritto in [1], le pubbliche amministrazioni possono adottare il modello evolutivo di SPC sia in veste di fruitori di servizi, che di erogatori. Un'amministrazione potrebbe dotarsi solo di servizi di livello IaaS, per poter poi offrire in modo efficiente e conforme spazi per servizi di livello PaaS e SaaS, ad esempio a pubbliche amministrazioni non in grado di acquisire e gestire tutte le risorse necessarie per la messa in opera e il funzionamento di un proprio data center sul quale ospitare le proprie applicazioni. Alternativamente le pubbliche amministrazioni possono agire come fruitori o erogatori dei livelli PaaS e SaaS, concentrandosi solo sugli aspetti più funzionali della logica applicativa, oppure utilizzare tutti i servizi, di tutti i livelli, offerti da diversi erogatori. Questa flessibilità ha chiaramente un impatto sulle responsabilità che le diverse Pubbliche Amministrazioni possono assumersi.

1.5 OpenStack

Il gruppo di lavoro OGF succitato, l'*Open Cloud Computing Interface*, si occupa di specifiche di protocolli, di interfacce e di standard, anche se non entra troppo nel merito delle scelte tecnologiche, mantenendosi su un piano più astratto. A cambiare le cose è intervenuto l'annuncio di Rackspace, NASA ed altri leader industriali, avvenuto a metà del 2010, che ha lanciato il progetto OpenStack, uno stack Open Source di software per gestire sistemi Cloud di memorizzazione e computazione, derivato dalla piattaforma di computazione Nebula della NASA.

Anche se non pienamente rispondente ad OGF OCCI, si propone di implementare le API di Amazon AWS, che sono lo standard de facto del Cloud Computing. Altri fornitori, come Eucalyptus, già offrivano questa caratteristica. Ad ogni modo il sistema OpenStack promette una maggiore scalabilità e più funzionalità nel contesto del software licenziato GPL.

OpenStack è di estremo interesse per chi offre e per chi domanda servizi Cloud nel settore pubblico, per le seguenti motivazioni:

- La piattaforma è interamente Open Source;
- Gli standard sui quali si basa sono tutti ben noti e pubblicati;
- E' basata su hypervisor KVM, che supporta non solo piattaforme guest GNU/Linux, ma anche Windows;
- Vi è già una diffusa conoscenza e adozione delle specifiche delle API AWS;



- Lo sviluppo della piattaforma viene finanziato da diversi soggetti, tra cui gioca un ruolo determinante il governo statunitense.

In conclusione, OpenStack rappresenta una soluzione tecnologica concreta, a cui è possibile affidarsi con confidenza per i prossimi sviluppi nel campo di questo tipo di architetture. [12].



2. MODALITÀ DI EROGAZIONE DI SERVIZI CLOUD

Il livello IaaS offre il maggior grado di estendibilità in quanto costituisce il “primo mattone” sul quale poi ospitare i servizi di piattaforma e quelli di livello software per l'utilizzo da parte degli utenti finali. In particolare, sono possibili due modalità di erogazione: quella “a risorse” e quella “a macchina virtuale”.

La modalità “a risorse” prevede l'acquisto di risorse computazionali quali CPU, memoria, storage a stock di quantità qualunque. Le risorse acquisite verranno successivamente utilizzate per istanziare un certo numero di macchine virtuali, che determinate caratteristiche, variabili in base alle esigenze dell'utente.

La modalità “a macchina virtuale” prevede invece l'acquisto di un server virtualizzato in vari tagli già dimensionati, esposto su Internet o integrato in una VPN, per il periodo di tempo utile alle necessità specifiche (“pay per use”). Questa generalizzazione, nota come *commodization* (mercificazione), è una tendenza tipica del mercato dei beni di consumo e offre una maggiore praticità commerciale.

Bandi di gare di natura “Infrastrutturale” dovrebbero essere rivolti a servizi IaaS del primo tipo, che garantiscono più gradi di libertà all'utente, mentre bandi di gara di tipo “Applicativo” ben si adattano a servizi IaaS del secondo tipo (maggiori dettagli nel seguito). Sebbene l'offerta di servizi del primo tipo sia un pò esposta ad una maggiore difficoltà di comparazione dei prezzi, dovuta alla estrema varietà di tipi di offerte, un raffronto equo dei prezzi è comunque una sfida che chi si occupa di preparare le gare si troverà a dover affrontare, considerato che il mercato, anche nelle offerte a taglie predefinite, è tutt'altro che omogeneo.

Per le risorse di tipo memorizzazione (storage), l'acquisto può essere fatto in funzione dello spazio utile alle necessità specifiche. Normalmente c'è una unità minima con cui specificare lo spazio, generalmente pari a 1GB. Le risorse storage devono prevedere due modelli distinti: *block* e *object*.

Il primo, *block*, è la tipologia di storage adatta ad essere utilizzata dalle istanze di risorse di calcolo, montabile come filesystem ed in grado di esporre una interfaccia block-oriented con lettura e scrittura di blocchi dati di dimensioni fisse (tipicamente usato con le Storage Area Network). Il secondo, *object*, è un tipo di risorsa che tratta dati in contenitori di dimensioni flessibili e opera lettura e scrittura a livello di singolo contenitore (object). Da un punto di vista di implementazione si tratta di un distributed storage system per dati statici, come ad esempio le immagini delle macchine virtuali, foto, email, backup e archivi dati.

Questa suddivisione consente anche di differenziare più convenientemente il prezzo dello storage in funzione dell'utilizzo. Il *block storage* può essere usato solamente collegato alle istanze di risorse di calcolo, montandolo come filesystem, in base al sistema operativo che lo usa (non espone una interfaccia API). L'*object storage* deve essere accessibile a mezzo di API RESTful (HTTP/HTTPS).



Deve essere inoltre possibile effettuare *snapshot* delle immagini di macchina virtuale in container di *object storage*. Questo garantisce una elevata flessibilità di esportazione, importazione e backup delle immagini di sistemi operativi delle risorse di calcolo e del backup/restore di volumi di block storage.

La differenziazione tra object e block storage è contemplata in due dei principali standard di mercato IaaS: OpenStack (Cinder e Swift) e EC2 (EBS e S3).

2.1 Servizi IaaS in gare “infrastrutturali” e “applicative”

2.1.1 Servizi di Datacenter basati su Cloud Computing

Erogati in questa modalità, i servizi IaaS prevedono semplicemente l'acquisto di storage, risorse computazionali, capacità di rete e altre risorse sulla Cloud (resource pooling).

Si tratta di servizi IaaS gestiti automaticamente su infrastrutture *self-provisioned* e *self-managed*, alternative all'acquisto di hardware da mettere in co-location o nei propri data center. Ideale per test e sviluppo, può servire anche per applicazioni complesse. Le caratteristiche preminenti di questa modalità sono la flessibilità, un provisioning rapido, la possibilità di configurare e gestire in modo semplice e automatico le proprie macchine. Normalmente viene offerta la possibilità di installare sulle macchine sistemi operativi o middleware, all'interno di un catalogo prestabilito di opzioni. Ciò non esclude, ovviamente, la possibilità di installare liberamente sulle macchine sistemi custom. E' anche possibile richiedere al fornitore di abilitare una gestione della piattaforma che sia *partly-managed*, ossia che contempli la possibilità di richiedere l'intervento umano di assistenza, ad esempio a livello di sistema operativo e di gestione della sicurezza (è di fatto lo scenario più comune).

In questa modalità di IaaS, rete e capacità computazionale sono elastiche e on-demand, cioè gli utenti possono scalare in su e in giù la fornitura a richiesta, senza essere vincolati ad una capacità fissa. Le risorse possono essere dedicate o virtualizzate e la capacità può essere condivisa (è il caso ad esempio delle community cloud) o privata.

Una GUI e delle API devono essere fornite per una auto-amministrazione del Datacenter virtuale. È indispensabile la definizione di un modello di API standard unico, che abiliti scenari in cui agiscono molteplici provider. Anche in questo caso viene indicato il riferimento a OpenStack, in virtù della sua diffusione, della sua accessibilità (è basato su software Open Source) e dell'ottima copertura delle funzionalità di una piattaforma Cloud a livello IaaS.



2.1.2 Macchine virtuali off-the-shelf per servizi di piattaforma

Una possibile proposta di catalogo delle risorse di capacità computazionale a taglie, facente anche riferimento ad una modalità di classificazione della potenza elaborativa di una virtual CPU, può essere la seguente, presentata a solo scopo illustrativo:

VM Size	# Virtual CPU	RAM	System disk space	Cloud Compute Units
Extra Small	1	1G	30G	1
Small	2	2G	60G	2
Medium	2	4G	120G	4
Large	4	8G	240G	8
Extra Large	4	16G	480G	16
Double Extra Large	8	32G	960G	32

A solo a titolo esemplificativo, si riporta quanto segue a proposito dell'unità di misura Cloud Compute Unit: "Il CCU rappresenta l'ammontare di capacità elaborativa relative a un "virtual core". 4 CCU sono approssimativamente equivalenti alla potenza elaborativa minima di un core logico (un hardware hyper-thread) di una CPU Intel Xeon con clock a 2.67 Ghz o un AMD Opteron con clock a 2.4 Ghz".

Un altro approccio potrebbe essere quello di considerare la potenza elaborativa di un virtual core di Amazon AWS, meglio conosciuto come ECU (Elastic Compute Unit). Un EC2 Compute Unit (ECU) esprime la potenza elaborativa (capacità di calcolo della CPU) di una CPU equivalente a un processore fisico Opteron 2007 con clock a 1-1,2 Ghz. Per una maggiore consistenza tale processore fisico è stato misurato con il [Passmark score benchmark](#) ad un valore di 400. Quindi, in assenza di altri riferimenti, questo valore può essere usato come parametro di valutazione della capacità elaborativa di un virtual core di una VM parte del catalogo IaaS. Ovviamente si assume che non si faccia uso di overbooking delle CPU fisiche che ci sia la garanzia di accesso al 100% del core legato alla virtual CPU.

Ideale per il deployment di applicazioni custom sulla Cloud, questa modalità di erogazione di servizi IaaS è pensata principalmente per necessità di hosting web tradizionale, in particolare:

- **Utenti *mainstream*:** siti istituzionali, applicazioni dinamiche, strumenti collaborativi, gestione di processi di piccola scala.
- **Utenti di fascia alta:** applicazioni web ad alto tasso di richiesta, con alto grado di complessità e di aggiornamento, con necessità di alta scalabilità e flessibilità, gestione di processi complessi,



applicazioni SaaS “Web 2.0”.

L’hosting web può essere erogato nelle seguenti modalità:

- **Hosting dedicato:** infrastruttura e rete, più server dedicati;
- **Utility hosting:** infrastruttura e rete, più una piattaforma di utility computing, realizzata con sistemi di virtualizzazione, che offre capacità on-demand; può essere offerta insieme ad un’infrastruttura dedicata.

E’ possibile prevedere opzioni predeterminate per server virtuale, storage e banda aggiuntiva, nonché servizi opzionali professionali e di gestione. Alcuni esempi:

- Gestione del sistema operativo del server;
- Gestione dell’infrastruttura software (web server, application server, DB server);
- Gestione dello storage, incluso backup e recovery;
- Gestione della sicurezza;
- Gestione di altri dispositivi di rete, come application delivery controller (ADC);
- Servizi professionali associati all’hosting, come progettazione architettuale, pianificazione della capacità necessaria, test di performance, audit per la sicurezza e migrazioni del Datacenter

Tali servizi opzionali dovrebbero essere catalogati come *add-on* sul prezzo delle istanze di macchine virtuali. Inoltre i sistemi middleware e database ospitati sui sistemi operativi dovrebbero essere quotati sempre da catalogo e per singola istanza (di fatto ciò riguarda il livello PaaS di cui nel prossimo paragrafo).

2.2 Servizi PaaS in gare “applicative”

Il livello PaaS prevede l’impiego di tutte quelle piattaforme di sviluppo e ambienti *run-time* che consentono la progettazione ed esecuzione dei servizi del livello SaaS. A esse si aggiungono un insieme di servizi integrati con tali ambienti.

Questi servizi includono per esempio:

- AAA (Autenticazione, Autorizzazione, Accounting)
- Supporto al procedimento amministrativo
 - Piattaforma di firma digitale
 - Gestione documentale multicanale
 - Archiviazione/Conservazione dei documenti
 - Servizi di Comunicazione multicanale massiva



- PEC evoluta
 - Pagamenti/incassi elettronici
- Business Process Management System
- Governance
 - SLA monitoring
 - Business Intelligence
- Data visualization e infografica di banche dati
- Sicurezza e Privacy as a Service
- Supporto alla cooperazione applicativa
 - Accordi di servizio
 - Porta di dominio

Anche nel caso del Platform as a Service viene indicata la preferenza per sistemi aperti basati su standard Open Stack, che consentano di stare al passo con la molteplicità di linguaggi e la velocità di sviluppo e che consentano diverse soluzioni di deployment per la gestione di servizi su larga scala, escludendo *lock-in* tecnologici.

2.3 Servizi SaaS in gare “applicative”

A livello SaaS delle gare applicative si identificano tutti quei servizi che realizzano la vera e propria logica di business delle applicazioni della Pubblica Amministrazione. A tal riguardo, si distinguono due tipi di utenti finali ai quali tali servizi sono rivolti: i cittadini e le imprese, da un lato, e le Pubbliche Amministrazioni stesse, dall'altro. Le successive sottosezioni elencano esempi di servizi per le due tipologie di utenti.

2.3.1 Servizi ai cittadini e alle imprese

- Servizi web informativi
- Servizi web evoluti
 - Single Sign On (SSO)
 - form online
 - gestione documenti



- monitoraggio dell'evoluzione del servizio
 - pagamenti online
 - assistente virtuale
- Servizi web pro-attivi (l'Amministrazione informa l'utente sull'insieme di adempimenti che deve effettuare)

Queste categorie di servizi possono essere offerte sotto forma di *mobile-apps* in modo da consentire agli utenti finali di utilizzare comodamente tutte le funzionalità descritte anche mediante l'uso di dispositivi mobili, quali smartphone e tablet. Le *mobile-apps* possono essere incluse per il download da parte del cittadino/impresa sui siti istituzionali delle amministrazioni. Devono inoltre essere disponibili per lo scaricamento in specifici *app-store* della PA, gestiti attraverso PaaS, che offrano servizi di *user rating*, feedback, ecc. tanto per piattaforma Android, quanto per le altre piattaforme maggiormente diffuse, con preferenza per i sistemi basati su tecnologie Open Source. E' auspicabile la realizzazione di un portale di accesso agli *app-store* della P.A. che garantisca un facile accesso e controllo. I temi relativi alla gestione delle app per le PA verranno affrontati in un successivo lavoro anche in accordo con le politiche di valorizzazione dei dati pubblici che l'Agenzia è chiamata a proporre.

2.3.2 Servizi alle PA

La logica di business dei processi amministrativi può essere definita sia all'interno di singole PA, sia nel contesto di uno scenario di federazione di PA che interagiscono tra loro per erogare prestazioni aggregate ai cittadini/imprese.

- Procedimento amministrativo
 - protocollo informatico (art. 40-bis del CAD)
 - fascicolo elettronico (raccolta dell'insieme degli atti, dei documenti e dei dati di un procedimento amministrativo (art. 41 del CAD))
 - accesso a banche dati in rete (secondo quanto previsto dall'art. 50 del CAD)
- Sistemi collaborativi: condividere idee, documenti, attività e calendari (attraverso interfacce web, GUI e *mobile-apps*).



3. REQUISITI NON-FUNZIONALI DEI DATA CENTER

Il Cloud Computing si basa sui Data Center (in Italiano, Centri Elaborazione Dati, ovvero CED), che centralizzano le attività di coordinamento e manutenzione delle apparecchiature e dei servizi di gestione dei dati. Nella Pubblica Amministrazione italiana sono presenti più di 1000 CED, di cui 92 centrali, 67 intermedi e 874 provinciali, una reale stima dei datacenter delle PA esistenti è in corso nel momento di pubblicazione del presente. Per una maggiore efficienza e risparmio, sarebbe auspicabile una loro riduzione in numero, con conseguente concentrazione delle funzionalità, in ottica sia di efficienza economica che tecnologica.

Poiché SPC sarà l'ambiente nel quale verrà realizzato il processo di riduzione dei Data Center, si intende presentare i requisiti affinché i Data Center siano SPC-compliant.

3.1 Caratteristiche generali dei Data Center

Questa sezione descrive le caratteristiche generali degli ambienti dove sono ospitate le infrastrutture tecnologiche per l'elaborazione dei dati e preposte a fornire le funzionalità attese dal servizio per soddisfare determinati obiettivi. I data center offrono accesso controllato alle seguenti risorse:

Risorse computazionali - Le macchine virtuali sono il cuore del pool delle risorse di elaborazione e mediante l'astrazione dall'hardware (CPU, memoria RAM, interfacce di comunicazione) consentono una: piena flessibilità operativa, maggiore supporto alla affidabilità dei servizi e riduzione indiretta dei costi (ottimizzazione di energia, spazio e complessità)

Risorse storage - Queste si presentano come un pool di oggetti-storage che comprende unità logiche convenzionali, dischi virtuali e sistemi storage specifici per determinate applicazioni. I servizi storage di base come il backup, la deduplicazione, gli snapshot, il thin-provisioning e così via, si devono poter applicare sia agli oggetti-storage virtuali sia alle risorse fisiche sottostanti. Con la distinzione tra object storage e block storage si può inoltre ottimizzare l'utilizzo delle risorse di memorizzazione in funzione delle necessità e consentire una maggiore flessibilità operativa.

Una piattaforma cloud utilizzando un "cloud operating system" consente di gestire in modo integrato tutte le funzionalità tipiche elencate nel precedente paragrafo e di controllarle anche in modo programmatico tramite un set ben definito di API (Application Programming Interface).

Risorse network - astrazione di un network virtuale allacciandolo ai componenti fisici delle reti. Possibilità di implementare soluzioni di networking basate su tecnologia SDN (Software Defined



Networking) che consente una ulteriore astrazione dagli apparati di networking semplificando la gestione degli apparati fisici.

Di seguito sono elencate alcune caratteristiche tipiche per valutare in modo oggettivo un data center.

Criticità: livello di disponibilità di sistema che deve essere raggiunto in termini di norme su standard industriali.

Capacità: Massimo carico di IT (in kW) che l'infrastruttura fisica del Datacenter può sopportare

Capacità di crescita: descrizione dello stato con requisiti di massima potenza

Efficienza: Obiettivo di efficienza energetica per i sistemi infrastrutturali – generalmente espresso in tempi più recenti come PUE (Power Usage Effectiveness) rappresentante il rapporto tra la potenza da un data center e l'effettiva potenza erogata ai sistemi IT (compute, storage, network).

Densità: la media e il picco di potenza a cui si prevede si attestino i dispositivi IT (kW/rack) e l'ammontare di spazio richiesto.

Classificazione delle metriche relative alle funzionalità delle infrastrutture IT di un data center:

- **Setup time:** tempi upfront necessari per essere operativi o tempo di messa in opera delle infrastrutture
- **Reaction time:** tempi di reazione ai cambiamenti richiesti
- Scalabilità dei sistemi
- Consumi energetici
- Utilizzo ottimale dei sistemi:
 - occupazione della capacità operativa (> 60%)
 - Occupazione dello spazio storage (riduzione della frammentazione > 80%)
- **Indicatori di GreenIT** (vedi dopo): oggi giorno espresso come PUE.
- **Disaster recovery e Continuità operativa:** ripristino dei servizi in situazioni di emergenza e garanzia delle funzionalità, anche in modalità ridotta in termini di capacità operativa, nel caso di occorrenze di disastri che impattano le strutture di erogazione dei servizi (Data center)- usualmente identificate con le metriche di RTO (Recovery Time Objective e RPO (Recovery Point Objective)
- **Fuori servizio:** riferito ad un DC Tier IV – secondo ANSI/TIA-942 e derivante dalla classificazione dell'Uptime Institute) – è realistico considerare una disponibilità generalizzata



(availability) pari a 99.95%, cioè 52:56 minuti di stallo su base annuale corrispondenti a 21:56 minuti su base mensile o 5:04 su base settimanale – per servizi business critical. Alcuni servizi considerati estremamente critici possono richiedere una disponibilità del 99.99% che generalmente, allo stato attuale, non è consigliabile ospitare su una infrastruttura IaaS.

3.2 Categorie di servizi di Datacenter

Le soluzioni per erogare servizi di infrastruttura on demand o IaaS (Infrastructure as a Service), in un contesto di cloud computing, includono funzionalità di:

- Compute (capacità computazionale) provisioning
 - Storage (memoria di massa) provisioning diversificata in object e block storage
 - Networking (interconnessioni LAN virtuali) provisioning
 - Sicurezza di rete e isolamento
 - Sicurezza degli edifici e perimetrale
 - Servizi di supporto (alimentazione, manutenzione, cabling, ecc.)
-
- Servizi di provisioning (hardware, software)
Ricostituzione rapida di servizi
Alta disponibilità
Datacenter multipli e istanze multiple
-
- Servizi di storage
Replicazione automatizzata
Cifratura a riposo e in transito
Conservazione dei dati automatizzata
Possibilità di fornitura per aree geografiche
-
- Servizi di infrastrutture di processamento
Snapshot di immagini



Isolamento dei processi

Sandboxes

- Servizi di supporto
 - Controlli di sicurezza On-Demand (autenticazione, logging, firewalling...)
 - Certificazione e accreditamento
 - IRT (incident response team)
 - Federation management
- Servizi di sicurezza di rete e isolamento
 - Protezione da DDoS
 - Sicurezza perimetrale (IDS, firewall, autenticazione)
 - VLAN
 - VPN

3.3 Classificazione dei Data Center secondo l'affidabilità

Business Continuity e Disaster Recovery. Si rimanda a [4] per un ulteriore approfondimento.

L'affidabilità di un Data Center è un fattore cruciale, in quanto si riverbera sull'affidabilità dei servizi erogati dallo stesso Data Center. I servizi informatici devono garantire affidabilità e sicurezza senza soluzione di continuità. In particolare, alcuni servizi come per esempio quelli di monitoraggio, videosorveglianza, finanza elettronica, ecc. devono poter contare su una rete internet affidabile 24 ore su 24.

Per comprendere l'importanza di un Data Center di ultima generazione che garantisce dunque continuità nell'offerta dei servizi (con una possibilità di stallo non superiore a 26 minuti complessivi l'anno contro le 29 ore dei modelli di I generazione) possiamo pensare all'impatto negativo su tutta la popolazione potrebbe avere l'arresto di sistemi gestionali complessi come quelli che amministrano i servizi di mailing o di hosting e housing. Un blocco, anche solo di qualche ora, del servizio mail paralizzerebbe il lavoro a migliaia di utenti, mentre l'oscuramento dei siti web avrebbe notevoli ripercussioni economiche in particolar modo per i siti di e-commerce ma anche per quelli della pubblica amministrazione che negherebbero ai propri cittadini il diritto di accesso ai documenti pubblici.

La Telecommunications Industry Association ha definito, attraverso lo standard ANSI/TIA-942, quattro livelli (detti Tier) per la classificazione delle infra-strutture Data Center:



Il modello di Data Center proposto in questa misura è il più avanzato (TIER IV) che presenta i criteri più elevati di affidabilità.

In [4] i Tier vengono ulteriormente specificati, passando ad un numero di 6, inclusi nei 4 e che meglio li specificano. Vediamoli nel seguito:

Tier 1 prevede l'esecuzione, il trasporto e la conservazione dei backup (di dati, applicazioni e "immagine del sistema") in un sito diverso dal primario e, per i casi in cui si renda necessario assicurare il ripristino, la disponibilità di un sito "vuoto" attrezzato, pronto a ricevere le componenti e configurazioni necessarie, ove fosse richiesto, per far fronte all'emergenza (on demand). I backup (dei dati, delle applicazioni e dell'"immagine del sistema") sono conservati presso il sito remoto. In tale sito deve essere prevista la disponibilità, in caso di emergenza, sia dello storage su disco, dove riversare i dati conservati, sia di un sistema elaborativo in grado di permettere il ripristino delle funzionalità IT.

Tier 2: la soluzione è simile a quella del Tier 1, vengono assicurate l'esecuzione, il trasporto, la conservazione dei backup (dei dati, delle applicazioni e dell'"immagine del sistema") e la disponibilità presso il sito dei sistemi e delle configurazioni da poter utilizzare per i casi in cui si renda necessario il ripristino, con la differenza che le risorse elaborative possono essere disponibili in tempi sensibilmente più brevi, viene garantito anche l'allineamento delle performance rispetto ai sistemi primari.

Tier 3: la soluzione è simile a quella del Tier 2, con la differenza che il trasferimento dei dati dal sito primario e quello di DR avviene attraverso un collegamento di rete tra i due siti. Questa soluzione, che può prevedere tempi di ripristino più veloci rispetto ai Tier precedenti, rende necessario dotarsi di collegamenti di rete con adeguati parametri di disponibilità, velocità di trasferimento e sicurezza (sia della linea, sia delle caratteristiche dipendenti dalla quantità di dati da trasportare).

Tier 4: la soluzione prevede che le risorse elaborative, garantite coerenti con quelle del centro primario, siano sempre disponibili, permettendo la ripartenza delle funzionalità in tempi rapidi. Le altre caratteristiche sono quelle del Tier 3, con la possibilità di aggiornamento dei dati (RPO) con frequenza molto alta, ma non bloccante per le attività transazionali del centro primario (aggiornamento asincrono).

Tier 5: la soluzione è analoga a quella del Tier 4, con la differenza che l'aggiornamento finale dei dati avviene solo quando entrambi i siti hanno eseguito e completato i rispettivi aggiornamenti. Allo stato attuale della tecnologia questa soluzione non può prescindere dalle caratteristiche della connettività sia in termini di distanza, sia in termini di latenza; ne consegue che tale modalità (sincronizzazione), nonché l'eventuale bilanciamento geografico del carico di lavoro, risulta difficile oltre significative distanze fisiche fra sito primario e secondario (ferma restando la necessità di non prescindere dallo specifico contesto applicativo).

Tier 6: la soluzione prevede che nel sito di DR le risorse elaborative, oltre ad essere sempre attive, siano funzionalmente "speculari" a quelle del sito primario, rendendo così possibile ripristinare l'operatività in tempi molto ristretti. Le altre caratteristiche sono uguali a quelle del Tier 5.



3.4 Green Computing

Sistema di gestione del Data Center che sia conforme alla strategia EU2020.

Legittimazione normativa presentata in base alla gerarchia delle fonti:

- 1) Direttiva 2004/18/CE e quindi nel DLgs.. 163/2006 , ove si prevede in materia di GPP che le specifiche tecniche “ogniquale volta sia possibile devono essere definite in modo da tener conto dei criteri di protezione ambientale” e che quando si procede ad affidamenti con il criterio dell’offerta economicamente più vantaggiosa, il bando di gara stabilisce fra i criteri di valutazione dell’offerta pertinenti alla natura, all’oggetto e alle caratteristiche del contratto, oltre al prezzo, alla qualità e al pregio tecnico, estetico e funzionale, anche “le caratteristiche ambientali ed il contenimento dei consumi energetici e delle risorse ambientali dell’opera o del prodotto”.
- 2) “strategia di Lisbona” per la crescita e l’occupazione che sin dal 2000 ha identificato nella sostenibilità ambientale uno dei pilastri della competitività europea, promuovendo misure per addivenire ad acquisti sostenibili;
- 3) Linee Guida emanate dalla Commissione Europea per la redazione di Piani d’azione nazionali sul Green Public Procurement con l’obiettivo di incoraggiare ”gli Stati membri della Comunità a dotarsi di piani d’azione per l’integrazione delle esigenze ambientali negli appalti pubblici”;
- 4) Pacchetto crescita (ottobre-dicembre 2012). Verrà integrato da un piano nazionale dell’energia (l’ultimo risale ad ormai 15 anni addietro). Al centro il sostegno della Green Economy, ricca di prospettive occupazionali e per lo sviluppo (anche tecnologico): gli obiettivi della direttiva europea “20-20-20”, che prevede la riduzione del 20% delle emissioni dei gas serra, del consumo di energia del 20% e l’aumento del 20% della quota di energia proveniente da fonti rinnovabili entro il 2020, dovranno essere raggiunti e, se possibile, superati tramite potenziamento di idroelettrico, fotovoltaico, geotermia, biomasse ed interventi di efficienza energetica.
- 5) Con il d.m. 7.3.2012, il Ministero dell’ambiente ha stabilito criteri ambientali per gli appalti nella pubblica amministrazione, ossia i criteri ambientali fondamentali da inserire nei capitolati di appalto e nelle determine a contrarre relativi ai bandi pubblicati dalla pubblica amministrazione, finalizzati all’acquisto di servizi energetici per gli edifici: gli appalti pubblici dovranno infatti attenersi alle regole stabilite dal d.m. 7 marzo 2012, che determina le caratteristiche base per far sì che i servizi di illuminazione e riscaldamento, come anche quelli di raffreddamento, siano definiti ecosostenibili.

- Impatto ambientale dei Data Center

11.8 milioni di server nei data center, usati al 15% delle loro capacità



800 miliardi di dollari all'anno per comprare e mantenere software enterprise

80% della spesa è in installazione e manutenzione

I data center consumano fino a 100 volte di più al mq rispetto agli edifici per uffici

L'IT produce il 2% delle emissioni globali di diossido di carbonio

- Consumi energetici

Il consumo medio per server è quadruplicato dal 2001 al 2006

Il numero di server è duplicato dal 2001 al 2006

I data center consumano l'1.5% dell'elettricità degli USA

nel mondo, 0.6% nel 2000 e 1% nel 2005

Le tecnologie Green possono ridurre i costi energetici del 50%

Consumo energetico (agenda digitale italiana 8.5)

- Potenza per le infrastrutture di supporto

Abbattimento della potenza per le infrastrutture di supporto (agenda digitale italiana 8.6)

Requisiti:

- Tool per l'efficienza energetica
- Illuminotecnica per bassi consumi
- Sistemi di risparmio energetico e spegnimento automatico
- Sistemi di raffreddamento Rack con raffreddamento ad acqua
- Sistemi di condizionamento free cooling e natural cooling
- Soluzioni di compartimentazione per la neutralizzazione dell'aria calda
- Sistemi UPS modulari ad alto rendimento



4. REQUISITI NON-FUNZIONALI DEI SERVIZI CLOUD

La caratterizzazione dei servizi basati sul Cloud Computing di interesse della PA è funzionale alla determinazione di regole per la certificazione degli stessi. Del resto, qualificare i servizi in base ai loro requisiti risente, almeno in parte, di una categorizzazione fatta per tipologia di servizi. Un primo prodotto del lavoro nel seguito presentato consiste, pertanto, nella definizione di classi di servizi. Vengono quindi fornite specifiche trasversali alle tipologie di servizio, da affiancare alle specifiche espresse in funzione della classe di servizio.

La definizione di una normativa abilitante per la fornitura di servizi Cloud-based deve tener conto di una molteplicità di aspetti, dai livelli di sicurezza, ai livelli di servizio, dalle clausole contrattuali, all'affidabilità del provider. Si è dunque pensato di definire aree di controllo dei requisiti, focalizzate sulle varie dimensioni di cui l'offerta di servizi Cloud deve tener conto. I requisiti trasversali ai servizi verranno pertanto articolati nelle diverse aree di controllo.

La qualificazione dell'offerta di servizi Cloud, l'obiettivo principale di questo documento, facilita di fatto il processo di standardizzazione attualmente in corso nel mondo del Cloud Computing, almeno per quanto attiene alle esigenze della PA. L'articolazione dei requisiti in classi di servizio e aree di controllo volge infatti ad una emanazione ragionata di regole di compatibilità e portabilità dei dati tra servizi equivalenti.

Infine, una nota sui requisiti. Saranno presentati i requisiti non funzionali. Un requisito funzionale descrive la funzionalità attesa dal servizio per soddisfare determinati obiettivi. Mentre i requisiti non funzionali definiscono la qualità richiesta al servizio relativamente a usabilità, prestazioni, sicurezza, vincolo sui tempi, e budget.

4.1. Aree di controllo dei requisiti

Le aree di controllo sono state individuate astraendole dai requisiti e partendo dal lavoro di cui in [5]. Il perseguimento di obiettivi e l'applicazione di tecniche volte al raggiungimento di determinati requisiti, possono così essere più facilmente misurati per ogni area. Alcune aree di controllo sono ulteriormente suddivise in sotto-aree.

Le aree di controllo definite sono le seguenti:

- A. Conformità
- B. Interoperabilità
- C. Governance dei dati
 - o Proprietà dei dati
 - o Garanzia sull'integrità dei dati



- Reversibilità

D. Sicurezza

- Sicurezza dei sistemi
- Sicurezza della struttura
- Sicurezza delle risorse umane
- Sicurezza delle informazioni

E. Gestione

- Gestione operativa
- Gestione del rischio
- Gestione degli aggiornamenti (rilasci)

F. Resilienza

Nella sezione 6.2, i requisiti vengono presentati all'interno di tali aree di controllo, nel seguito meglio specificate.

4.1.1. Conformità

La conformità dei sistemi riguarda la necessità di adesione a standard riconosciuti a livello internazionale:

- Interfacce di gestione standard
- Set-up, gestione e allocazione semplificate
- Installazioni standard
- Sistemi standard con applicazioni custom pronti a partire

Riguarda inoltre:

- Legalità
- Mappa della regolamentazione dei sistemi informativi
- Proprietà intellettuale
- Propagazione minima

La conformità deve garantire la piena e agevole migrabilità a/da sistemi e infrastrutture le più varie. Questo garantisce: apertura del mercato, trasparenza, intercambiabilità dei fornitori, possibilità di restare al passo con l'innovazione tecnologica.



La conformità deve inoltre essere mantenuta nel tempo. Poiché nell'arco di durata contrattuale di erogazione dei servizi il sistema software della piattaforma Cloud subisce una costante e continua evoluzione, è importante che sia previsto un processo di “*Continuous Integration*” e “*Continuous Deployment*”, atto a garantire un aggiornamento continuo della piattaforma e a fornire risoluzioni di problemi (fix), risoluzioni di problematiche di sicurezza (security patching), introduzione di miglioramenti ed innovazioni sul fronte tecnologico.

4.1.2. **Interoperabilità**

Adozione di soluzioni interoperabili.

- Servizi software comuni
- Multi-tenancy
- Logging
- Garanzie di QoS e SLA
- Gli utenti finali (cittadini e dipendenti) usano thin client o workstation leggere (no gestione locale, no software complicati)
- **IaaS**
 - Distribuzioni di immagini di Virtual Machine (VM) – i formati possono essere quelli usati dagli hypervisor più diffusi ma con la garanzia di piena funzionalità di importazione/conversione tra i vari formati (e.g., DMTF OVF, VHD, VMDK, QCOW2, VDI, HDD) – standard: ISO/IEC 17203:2011
 - Fornitura e controllo di VM (OpenStack API)
 - Scambio di VM inter-cloud (e.g., EC2-OpenStack)
 - Storage Persistente (e.g., S3, EBS, GFS, Atmos, Azure Storage, HP Cloud Object Storage)
 - SLA di VM che siano “*machine readable*” e che specifichino:
 - Uptime
 - Garanzia sulle risorse
 - Ridondanza di storage
 - ...

OVF è un formato per la descrizione di macchine virtuali e non è sufficiente a garantire una migrazione/portabilità in quanto bisogna considerare il formato dei dischi virtuali utilizzati come root filesystem delle VM. Ogni hypervisor ha un suo formato e deve essere specificato in modo chiaro i



possibili formati di disco virtuali supportabili quali ad esempio: VMDK (VMware), VDI (Virtualbox), VHD (Microsoft), qcow2 (KVM/Linux), EC2 (AMI).

A prescindere dal formato dei dischi virtuali ogni cloud provider deve garantire la possibilità esportare/importare le immagini dei dischi virtuali dai formati sopra elencati.

- **PaaS e SaaS**

- PaaS e SaaS più difficile per la natura proprietaria (Il lock-in aumenta spostandosi verso l'alto nello stack (IaaS → PaaS → SaaS))
- Gli standard per PaaS devono specificare:
 - Linguaggi di programmazione supportati
 - API per i servizi cloud
- Gli standard per SaaS devono specificare:
 - Autenticazione/autorizzazione SaaS-specifica
 - Formati per importare ed esportare i dati (e.g., schema XML)
 - Standard distinti per ogni campo applicativo

Ogni servizio PaaS deve rendere disponibile un set API calls in formato RESTful (HTTP/HTTPS) seguendo l'approccio OCCI e/o in modalità web services.

4.1.3. *Governance dei dati*

- Problemi
 - **Proprietà dei dati** (dati delocalizzati)
 - **Portabilità dei dati:**
 - Data Transfer Agreement (DTA)
 - Classificazione dei dati (dati visti come un asset di business)
 - Standard di trasferimento
 - Accesso ai dati da parte di organismi governativi e impatto dovuto alle norme giurisdizionali nazionali ed internazionali
 - **Conservazione dei dati** (data retention)
 - Dati personali identificanti (PII) e sensibili nella piattaforma Cloud, Risk management (assicurazione), responsabilità



- **Reversibilità:** piena possibilità di disconnettersi dai servizi cloud e recuperare pienamente i propri dati con la garanzia che questi ultimi siano effettivamente cancellati in modo permanente dai supporti di memoria utilizzati nell'infrastruttura fisica delle piattaforme cloud.
- **Soluzioni richieste**
 - Cifrare l'accesso all'interfaccia di controllo delle risorse della Cloud
 - Cifrare l'accesso da amministratore ai sistemi
 - Cifrare l'accesso alle applicazioni
 - Cifrare i dati “a riposo” (quando non sono usati da applicazioni)

4.1.4. Sicurezza

- Sicurezza dei sistemi
- Sicurezza della struttura
- Sicurezza delle attività delle risorse umane
- Sicurezza delle informazioni

Conformità alla normativa e ai regolamenti tecnici italiani o europei

4.1.5. Gestione

- Monitoraggio e statistiche (notifiche, ridimensionamento risorse, calcolo costi, cyber-intelligence...)
- Integrazione/riduzione di certificazione e accreditamento (cloud pre-accreditate)
- Semplificazione delle analisi di conformità
- Soluzioni economiche di Disaster Recovery e Data Storage
- Security team specializzato e dedicato
- Controlli di sicurezza On-Demand



4.1.6. Resilienza

- Scalabilità
- Flessibilità
- Efficienza
- Continuità operativa
- Elasticità
- Resistenza ai guasti, affidabilità
- Maggior resilienza
- Protezione contro attacchi di rete
- Rapida ricostituzione di servizi

4.2. Specifiche trasversali ai servizi

In [7] sono riassunte i principali requisiti che qualificano una offerta Cloud adeguata alla domanda della PA. Li elenchiamo nel seguito al fine di poterli successivamente articolare in metriche:

- Utilizzo di standard aperti
- Integrazione con il software già in uso
- Dati in sicurezza
- Continuità, persistenza dei dati e interoperabilità
- Giusto rapporto prezzo/prestazioni
- Trasparenza
- Facilità d'uso
- Tutela della privacy
- Accessibilità
- Non discriminazione verso nessuno
- Diversità (indipendenza da licenze o software specifici)

Presentiamo quindi i requisiti articolati per aree di controllo. Per ciascun requisito viene indicato qual è l'oggetto o gli oggetti a cui il requisito si riferisce da un punto di vista architetturale. Gli oggetti architetturali sono i seguenti:

1) FIS



AGENZIA PER L'ITALIA DIGITALE

Si riferisce a oggetti di natura fisica

2) NET

Si riferisce alla rete e alle sue caratteristiche prestazionali

3) COMP

Si riferisce alle risorse computazionali (CPU e memoria RAM)

4) STOR

Si riferisce alla capacità di memorizzazione (in inglese, storage)

5) APP

Si riferisce alle applicazioni.

6) DATA

Si riferisce ai dati.

4.2.1. Requisiti di conformità

ID requisito	Nome requisito	Specifiche requisito	Note	Oggetti architetture
A1	Adesione standard internazionali	Interfacce di gestione standard, set-up, gestione e allocazione semplificate, installazioni standard, sistemi standard con applicazioni custom pronti a partire		COMP, STOR, APP, DATA
A2	Legalità	Rispetto di leggi e regolamenti sui dati, sugli oggetti, sulle applicazioni, sull'infrastruttura e sull'hardware.	RNF	FIS, NET, COMP, STOR, APP, DATA
A3	Mappa della regolamentazione dei sistemi informativi	Dati, oggetti, applicazioni, infrastrutture ed hardware devono avere assegnato un riferimento normativo documentato e aggiornato.	RNF	FIS, NET, COMP, STOR, APP, DATA
A4	Proprietà	Le licenze (proprietarie o	RNF	APP, DATA



	intellettuale	libere) dei software e dei dati devono essere esplicitate ed applicate.		
A5	Propagazione minima	Limitazione dell'accesso, della duplicazione di dati, della dislocazione dei dati.	RNF	FIS, NET, COMP, STOR, APP, DATA

4.2.2. Requisiti di interoperabilità

ID requisito	Nome requisito	Specifiche requisito	Note	Oggetti architetturali
B1	Cooperazione	Fornitura e controllo di immagini di VM in formato standard (IaaS), API aperte per i servizi cloud (PaaS), sistemi standard di autenticazione e autorizzazione (SaaS). • OpenStack come standard di riferimento per IaaS • API RESTful (web API) per PaaS e SaaS – web services • Soluzioni erogabili in modalità PaaS e SaaS portabili in un contesto IaaS in cui si usi lo stesso standard di riferimento (OpenStack)	RNF	COMP, STOR, APP, DATA
B2	Riutilizzo	Possibilità di scambio di VM inter-cloud (IaaS), storage persistenti ed interoperabili (PaaS), adesione a standard	RNF	COMP, STOR, APP, DATA



		aperti per ogni campo applicativo, documentazione e disponibilità del codice sorgente (SaaS): - standard ISO/IEC 17203:2011 per macchine virtuali - Capacità di convertire tra i vari formati di dischi virtuali usati dalle maggiori piattaforme di virtualizzazione (VMDK, VHD, HDD, QCOW2, AMI, ecc.)		
B3	Portabilità	Distribuzioni di immagini di VM in formati standard (IaaS), specifica dei linguaggi di programmazione supportati (PaaS), adesione a formati aperti per importare ed esportare i dati (SaaS)	RNF	COMP, STOR, APP, DATA
B4	QoS e SLA comparabili	SLA di VM, piattaforme e applicazioni che siano “machine readable” e che specifichino: - Uptime - Garanzia sulle risorse - Ridondanza di storage -	RNF	NET, COMP, STOR, APP
B5	Compatibilità e portabilità dei dati	Formati dei dati standard, aperti e approvati a livello internazionale	RNF	DATA

4.2.3. Requisiti di governance dei dati

ID requisito	Nome requisito	Specifiche requisito	Note	Oggetti
--------------	----------------	----------------------	------	---------



				architetturali
C1	Responsabilità dell'amministratore	Ogni dato deve avere un amministratore con responsabilità ben definite, documentate e comunicate.	RNF	COMP, STOR, APP, DATA
C2	Classificazione	I dati e gli oggetti contenenti dati devono avere assegnata una classificazione basata sul tipo di dati, la giurisdizione di origine, la giurisdizione della attuale locazione, il contesto, i limiti legali, i limiti contrattuali, il valore, la sensibilità, la criticità per l'organizzazione e gli obblighi per le terze parti rispetto a retention e prevenzione di divulgazioni non autorizzate e uso improprio.	RNF	COMP, STOR, APP, DATA
C3	Maneggio, etichettatura e politiche di sicurezza	Politiche e procedure per l'etichettatura, il maneggio e la sicurezza dei dati e degli oggetti contenenti dati.	RNF	COMP, STOR, APP, DATA
C4	Politiche di ritenzione	Politiche e procedure per la conservazione dei dati devono essere stabilite e meccanismi di backup o ridondanza implementati per garantire il rispetto delle normative e dei requisiti contrattuali o commerciali. La verifica del ripristino da backup deve essere attuata ad intervalli pianificati.	RNF	COMP, STOR, APP, DATA
C5	Rimozione sicura dei dati	Politiche e procedure devono essere stabilite e meccanismi attuati, per la rimozione sicura e completa dei dati da tutti i supporti di memorizzazione, garantendo la non	RNF	COMP, STOR, APP, DATA



		recuperabilità da nessuna indagine forense.		
C6	Dati non in produzione	I dati in produzione non devono essere replicati o usati in ambienti non in produzione.	RNF	STOR, APP, DATA
C7	Dispersione di dati	Meccanismi di sicurezza per prevenire la dispersione di dati	RNF	COMP, STOR, APP, DATA
C8	Assessment del rischio	Ad intervalli pianificati per verificare: - Consapevolezza di dove sono collocati i dati sensibili e trasmessi attraverso database, applicazioni, server e infrastrutture di rete - Conformità con i periodi di ritenzione e fine vita - Classificazione dei dati e protezione da accessi, uso, perdita, distruzione, non autorizzati e falsificazioni.	RNF	COMP, STOR, APP, DATA

4.2.4. Requisiti di sicurezza

ID requisito	Nome requisito	Specifiche requisito	Note	Oggetti architetturali
D1	Sicurezza dei sistemi - Inventario	Un inventario completo dei beni di importanza critica deve essere mantenuto, con proprietà definite e documentate.	RNF	FIS
D2	Sicurezza dei sistemi - Procedure	Politiche e procedure per la protezione, la gestione patrimoniale, l'uso, la manutenzione e lo smaltimento sicuro delle	RNF	FIS



		attrezzature.		
D3	Sicurezza dei sistemi – Trasferimenti fuori sede	Il trasferimento di hardware, software o dati in un locale fuori sede può essere ottenuto previa autorizzazione.	RNF	FIS, NET, COMP, STOR
D4	Sicurezza della struttura – Ingresso e uscita	Punti di ingresso e di uscita, quali aree di servizio e altri punti in cui il personale non autorizzato può entrare nei locali, devono essere monitorati, controllati e, se possibile, isolati dagli impianti per la memorizzazione dei dati, onde evitare compromissione, corruzione o perdita degli stessi.	RNF	FIS, NET, COMP, STOR
D5	Sicurezza della struttura – Monitoraggio	Ingresso e di uscita alle aree protette deve essere limitato da meccanismi di controllo degli accessi fisici per garantire che solo al personale autorizzato sia consentito l'accesso.	RNF	FIS
D6	Sicurezza della struttura – Perimetro e protezioni	Sicurezza perimetrale (recinzioni, muri, barriere, protezioni, cancelli, sorveglianza elettronica, meccanismi di autenticazione fisici, servizi di accoglienza e pattuglie di sicurezza) per salvaguardare i dati e i sistemi informativi.	RNF	FIS
D7	Sicurezza della struttura – Accesso alle risorse	L'accesso fisico alle risorse informative e le funzioni da utenti e personale di supporto deve essere limitato.	RNF	FIS
D8	Sicurezza delle risorse umane - Normative	Ai sensi delle leggi, le norme, l'etica e dei vincoli contrattuali, tutti i lavoratori,	RNF	DATA



		appaltatori e terzi saranno oggetto di verifica, proporzionata alla criticità dei dati a cui possono accedere, ai requisiti di business e di rischio accettabile.		
D9	Sicurezza delle risorse umane – Ambiente di lavoro	Politiche e procedure sono stabilite per il mantenimento di un ambiente sicuro e protetto di lavoro in uffici, sale, strutture e aree protette.	RNF	FIS
D10	Sicurezza delle risorse umane – Autorizzazioni all'accesso	Prima di concedere al personale l'accesso fisico o logico agli impianti, sistemi o dati, i dipendenti, gli appaltatori, gli utenti e i clienti terzi devono sottoscrivere i termini e le condizioni del loro lavoro, che devono includere in modo esplicito la responsabilità per la sicurezza informatica.	RNF	FIS, NET, COMP, STOR, APP, DATA
D11	Sicurezza delle informazioni - Policy	Va sviluppato, documentato, approvato e attuato un programma di gestione della sicurezza che includa garanzie amministrative, tecniche e fisiche per proteggere i beni e i dati da perdite, uso improprio, accesso non autorizzato, divulgazione, alterazione e distruzione. Il programma di sicurezza dovrebbe affrontare almeno i seguenti ambiti, nella misura in cui si riferiscono alle caratteristiche della fornitura: • Gestione del rischio	RNF	FIS, NET, COMP, STOR, APP, DATA



		• Politiche di sicurezza • Organizzazione della sicurezza delle informazioni • Gestione del risparmio • Sicurezza delle risorse umane • Sicurezza fisica e ambientale • Comunicazione e gestione delle operazioni • Controllo degli accessi • Sistemi informativi di acquisizione, sviluppo e manutenzione		
D12	Sicurezza delle informazioni – Requisiti di base	Requisiti di sicurezza di base devono essere stabiliti ed applicati alla progettazione e realizzazione di applicazioni, database, sistemi e infrastrutture di rete e di elaborazione delle informazioni (sviluppati o acquistati), in modo che siano conformi alle politiche, gli standard e i requisiti normativi applicabili. La conformità ai requisiti di protezione di base devono essere riesaminati almeno una volta all'anno o dopo cambiamenti significativi.	RNF	FIS, NET, COMP, STOR, APP, DATA
D13	Sicurezza delle informazioni – Policy per l'accesso utente	Criteri e procedure di accesso degli utenti devono essere documentate, approvate ed applicati per la concessione e la revoca di accesso base e privilegiato alle applicazioni, database e server e all'infrastruttura di rete, in	RNF	FIS, NET, COMP, STOR, APP, DATA



		accordo con i requisiti di business, la sicurezza, la conformità e il contratto sul livello di servizio (SLA).		
D14	Sicurezza delle informazioni – Autorizzazioni e restrizione all'accesso utente	Accesso utente base e privilegiato alle applicazioni, i sistemi, i database, le configurazioni di rete, i dati sensibili e le funzioni sono limitati e approvati dal management prima di concedere l'accesso.	RNF	NET, COMP, STOR, APP, DATA
D15	Sicurezza delle informazioni – Revoca dei permessi di accesso	Deprovisioning tempestive, la revoca o la modifica di accesso degli utenti ai sistemi, alle informazioni e ai dati devono essere attuate dopo ogni cambiamento di status di dipendenti, collaboratori, clienti, partner commerciali o di terzi (cessazione del rapporto di lavoro, contratto o accordo, cambiamento di lavoro o di trasferimento all'interno dell'organizzazione).	RNF	FIS, NET, COMP, STOR, APP, DATA
D16	Sicurezza delle informazioni – Revisione dell'accesso utente	Tutti i livelli di accesso utente vanno riesaminati dal management ad intervalli pianificati e documentati.	RNF	FIS, NET, COMP, STOR, APP, DATA
D17	Sicurezza delle informazioni – Crittografia	Politiche e procedure sono stabilite e meccanismi attuati per la crittografia dei dati sensibili in storage (ad esempio, file server, database e workstation) e per i dati in trasmissione (ad esempio, sulle interfacce di sistema, su reti pubbliche, e di messaggistica elettronica).	RNF	NET, COMP, STOR, APP, DATA



D18	Sicurezza delle informazioni – Gestione della chiave di crittazione	Politiche e procedure sono stabilite e meccanismi attuati per un'efficace gestione delle chiavi per supportare la crittografia dei dati in storage e in trasmissione.	RNF	NET, STOR, APP, DATA
D19	Sicurezza delle informazioni – Vulnerabilità e gestione delle patch	Politiche e procedure sono stabilite e meccanismi implementati per la vulnerabilità e la gestione delle patch, assicurando che le vulnerabilità delle applicazioni, dei sistemi e dei dispositivi di rete siano valutate e le patch di sicurezza, fornite dal fornitore, siano applicate in modo tempestivo, con un approccio basato sul rischio a determinare le priorità delle patch.	RNF	NET, STOR, COMP, APP, DATA
D20	Sicurezza delle informazioni – Anti-Virus e software malevolo	Assicurarsi che tutti i programmi antivirus siano in grado di rilevare, rimuovere e proteggere da tutti i tipi di software malevolo o non autorizzato, con gli aggiornamenti delle firme antivirus fatte almeno ogni 12 ore.	RNF	NET, STOR, COMP, APP
D21	Sicurezza delle informazioni – Gestione degli incidenti	Politiche e procedure sono stabilite per scandagliare eventi relativi alla sicurezza e garantire una gestione degli incidenti tempestiva e approfondita, attraverso sistemi di reporting su canali di comunicazione predefiniti, in accordo con i regolamenti e i requisiti contrattuali.	RNF	FIS, NET, COMP, STOR, APP, DATA



D23	Sicurezza delle informazioni – Metriche per la risposta agli incidenti	Meccanismi devono essere messi in atto per monitorare e quantificare i tipi, i volumi, i costi degli incidenti di sicurezza informatica.	RNF	FIS, NET, COMP, STOR, APP, DATA
D24	Sicurezza delle informazioni – Transazioni eCommerce	I dati relativi al commercio elettronico (e-commerce), che attraversano reti pubbliche devono essere adeguatamente classificati e protetti da attività fraudolente, divulgazione non autorizzata o artefazione, in modo tale da evitare dispute contrattuali e danneggiamento di dati.	RNF	NET, DATA
D25	Sicurezza delle informazioni – Accesso agli strumenti per l'audit	L'accesso e l'uso di strumenti di controllo che interagiscono con i sistemi informativi delle organizzazioni devono essere opportunamente segmentati e limitati per evitare la compromissione e l'uso improprio dei dati di log.	RNF	FIS, NET, COMP, STOR, APP, DATA
D26	Sicurezza delle informazioni – Accesso alle porte di configurazione e di diagnostica	L'accesso degli utenti alle porte di diagnostica e configurazione è limitato alle persone e alle applicazioni autorizzate.	RNF	FIS, APP
D27	Sicurezza delle informazioni – Dispositivi mobili e portatili	Politiche e procedure sono stabilite e misure attuate per limitare l'accesso ai dati sensibili da dispositivi portatili e mobili, quali computer portatili, telefoni cellulari e personal digital assistant (PDA), che generalmente sono a rischio più elevato rispetto a quelli non-portatili (ad esempio, computer desktop presso le	RNF	FIS, NET, COMP, STOR, APP, DATA



		strutture dell'organizzazione).		
D28	Sicurezza architetturale – Requisiti per l'accesso degli utenti	Prima di concedere agli utenti l'accesso a dati, asset, e sistemi informativi, tutti i requisiti identificati per la sicurezza, contrattuali e normativi, devono essere stati affrontati e soddisfatti.	RNF	FIS, NET, COMP, STOR, APP, DATA
D29	Sicurezza architetturale - Credenziali utente	Credenziali utente e controlli delle password per le applicazioni, database e server e infrastrutture di rete, che richiedono i seguenti requisiti minimi: • verifica l'identità dell'utente prima della reimpostazione delle password. • Se la reimpostazione della password utente è eseguita da altro personale (ad esempio, amministratore), la password deve essere immediatamente modificata dall'utente al primo utilizzo. • revoca tempestiva dell'accesso per gli utenti disabilitati. • Rimuovere / disabilitare gli account utente inattivi almeno ogni 90 giorni. • ID utente univoci e disabilitare account e password di gruppo, condivisi o generici. • scadenza password almeno ogni 90 giorni. • Lunghezza minima password di almeno sette (7)	RNF	NET, COMP, STOR, APP



		caratteri. • Password complesse contenenti caratteri numerici e alfabetici. • Consenti riutilizzo password dopo altre quattro (4) password utilizzate. • Blocco ID utente dopo non più di sei (6) tentativi. • Durata di blocco di ID utente per un minimo di 30 minuti o fino a quando l'amministratore riabilita l'ID utente. • Inserire nuovamente la password per riattivare il terminale dopo un tempo di inattività per la sessione di più di 15 minuti. • Mantenere i log dell'attività degli utenti privilegiati o con accesso a dati sensibili.		
D30	Sicurezza architetture – Sicurezza e integrità dei dati	Politiche e procedure sono stabilite e meccanismi attuati per garantire la sicurezza (ad esempio, la crittografia, controlli di accesso, e la prevenzione delle diffusioni non autorizzate) e l'integrità dei dati, scambiati tra una o più interfacce di sistema, giurisdizioni, o con terzi fornitori di servizi condivisi, onde evitare la divulgazione impropria, l'alterazione o la distruzione conforme alle prescrizioni legislative, regolamentari e contrattuali.	RNF	NET, COMP., STOR, APP, DADA
D31	Sicurezza	Le applicazioni devono essere	RNF	NET,



	architetturale – Sicurezza delle applicazioni	progettate in conformità con gli standard di sicurezza del settore riconosciuti (ad esempio, OWASP per le applicazioni web) e devono essere conformi ai requisiti normativi e aziendali.		COMP, STOR, APP, DATA
D32	Sicurezza architetturale – Integrità dei dati	Le routine di integrità per l'inserimento dei dati e per la loro uscita (ad esempio i controlli di riconciliazione e di modifica) vengono implementate per le interfacce delle applicazioni e dei database, onde evitare errori di elaborazione manuale o sistematica o corruzione dei dati.	RNF	NET, COMP, STOR, APP, DATA
D33	Sicurezza architetturale – Ambienti in produzione e non in produzione	Ambienti in produzione e non in produzione devono essere separati per impedire l'accesso non autorizzato o modifiche alle risorse informative.	RNF	FIS, NET, COMP, STOR, APP, DATA
D34	Sicurezza architetturale – Sicurezza di rete	Gli ambienti di rete devono essere progettati e configurati in modo da limitare i collegamenti tra reti attendibili e non attendibili, e vanno rivisti ad intervalli pianificati. Devono documentare la giustificazione per l'uso di tutti i servizi, i protocolli e le porte consentite, compresi i controlli implementati per i protocolli considerati insicuri. I diagrammi dell'architettura di rete devono indicare chiaramente gli ambienti ad alto rischio e i flussi di dati	RNF	FIS, NET, COMP, STOR, APP, DATA



		che possono avere impatti in conformità alle normative.		
D35	Sicurezza architetturale - Compartimentazione	Ambienti di sistema e di rete devono essere separati da firewall, per garantire l'aderenza a: • Attività e richieste del cliente • Requisiti di sicurezza • Conformità alle prescrizioni legislative, regolamentari e contrattuali • Separazione degli ambienti di produzione e non di produzione • Conservare la protezione e l'isolamento dei dati sensibili	RNF	FIS, NET, COMP, STOR, APP, DATA
D36	Sicurezza architetturale – Sicurezza wireless	Politiche e procedure devono essere stabilite e meccanismi messi in atto per proteggere gli ambienti di rete wireless, tra cui le seguenti: • i firewall perimetrali vanno configurati in modo da limitare il traffico non autorizzato • Impostazioni di sicurezza attivata con la crittografia avanzata per l'autenticazione e la trasmissione, in sostituzione delle impostazioni di default del fornitore (ad esempio, chiavi di crittografia, password, stringhe di comunità SNMP, ecc.) • L'accesso logico e fisico degli utenti ai dispositivi di	RNF	FIS, NET, COMP, STOR, APP, DATA



		rete wireless va limitato al personale autorizzato • Capacità di rilevare la presenza di dispositivi di rete wireless non autorizzati, per una tempestiva disconnessione dalla rete		
D37	Sicurezza architetturale – Reti condivise	L'accesso ai sistemi con l'infrastruttura di rete condivisa è limitato al personale autorizzato, in accordo con le politiche di sicurezza, procedure e standard. Le reti condivise con enti esterni devono avere un piano documentato che specifichi i controlli compensativi utilizzati per separare il traffico di rete tra le organizzazioni.	RNF	FIS, NET, COMP, STOR, APP, DATA
D38	Sicurezza architetturale - Sincronizzazione dei clock	Una sorgente di temporizzazione esterna accurata (esternamente concordato) deve essere utilizzata per sincronizzare i clock di sistema di tutti i sistemi di elaborazione delle informazioni all'interno dell'organizzazione o di un dominio di sicurezza definito in modo esplicito al fine di facilitare la tracciabilità e la ricostituzione della temporizzazione delle attività.	RNF	NET, COMP, APP
D39	Sicurezza architetturale – Dispositivi di autenticazione	L'identificazione automatica dei dispositivi deve essere utilizzata come metodo di autenticazione della connessione. Tecnologie location-aware possono essere utilizzate per	RNF	FIS, NET, COMP, STOR, APP



		convalidare l'integrità dell'autenticazione della connessione, in base alla posizione nota delle apparecchiature.		
D40	Sicurezza architettuale – Intrusione detection	Log che registrano attività di accesso di utenti privilegiati, tentativi di accesso autorizzati e non autorizzati, eccezioni di sistema ed eventi legati alla sicurezza delle informazioni devono essere conservati, nel rispetto delle politiche e dei regolamenti applicabili. I log devono essere esaminati almeno quotidianamente e strumenti per l'integrità dei file e il rilevamento delle intrusioni di rete (IDS) vanno messi in atto per facilitare l'individuazione tempestiva, l'indagine mediante l'analisi delle cause e la risposta agli incidenti. L'accesso fisico e logico degli utenti ai log di controllo deve essere limitato al personale autorizzato.	RNF	FIS, NET, COMP, STOR, APP, DATA
D41	Sicurezza architettuale – Codice mobile	Il codice mobile (software che viene trasferito tra sistemi) deve essere autorizzato prima della sua installazione e utilizzo, e la configurazione deve garantire che il codice mobile autorizzato operi secondo una politica di sicurezza ben definita. Deve essere impedito l'esecuzione di tutto il codice mobile non autorizzato.	RNF	NET, COMP, APP, DATA



4.2.5. Requisiti di gestione

ID requisito	Nome requisito	Specifiche requisito	RF/RNF	Oggetti architetture
E1	Policy	Politiche e procedure sono stabilite e messe a disposizione per tutto il personale a sostenere adeguatamente le operazioni.	RNF	STOR, APP, DATA
E2	Documentazione	Documentazione relativa al sistema d'informazione (ad esempio guide, amministratore e utente, diagrammi di architettura, ecc), va messa a disposizione del personale preposto a garantire quanto segue: • Configurazione, installazione e il funzionamento del sistema di informazione • Efficacia utilizzando le funzioni di sicurezza del sistema	RNF	FIS, NET, COMP, STOR, APP, DATA
E3	Pianificazione delle risorse e della capacità	La disponibilità e la capacità delle risorse devono essere pianificate, preparate, e misurate, per fornire le prestazioni richieste al sistema, in conformità con i requisiti normativi, contrattuali e di business. Proiezioni di requisiti di capacità futuri vanno effettuati al fine di ridurre il rischio di sovraccarico del sistema.	RNF	NET, COMP, STOR, DATA
E4	Manutenzione dei dispositivi	Politiche e procedure sono stabilite per la manutenzione delle attrezzature, per garantire	RNF	FIS, NET, COMP, STOR, APP,



		la continuità operativa e la disponibilità dei servizi.		DATA
E5	Gestione degli aggiornamenti e degli acquisti	Politiche e procedure sono stabilite per l'autorizzazione allo sviluppo o all'acquisizione di nuove applicazioni, sistemi, database, infrastrutture, servizi, operazioni e servizi.	RNF	FIS, NET, COMP, STOR, APP, DATA
E6	Cambiamenti di produzione	Le modifiche all'ambiente di produzione devono essere documentate, testate e approvate prima della realizzazione. Modifiche software e hardware possono comprendere applicazioni, sistemi, database e dispositivi di rete che necessitano di patch, service pack e altri aggiornamenti e modifiche.	RNF	NET, COMP, STOR, APP, DATA
E7	Test di qualità del rilascio	Un programma per il monitoraggio e la valutazione sistematica, per assicurare che gli standard di qualità siano rispettati, è stabilito per tutti i software sviluppati dall'organizzazione. Criteri di valutazione di qualità e di collaudo dei sistemi di informazione, aggiornamenti e nuove versioni viene stabilito, documentato e test del sistema devono essere effettuati sia durante lo sviluppo, che prima dell'accettazione. Il prodotto finale viene certificato come adatto allo scopo e gli errori devono essere eliminati prima del rilascio.	RNF	NET, COMP, STOR, APP, DATA
E8	Sviluppo in outsourcing dei rilasci	Un programma per il monitoraggio e la valutazione sistematica, che assicuri che gli	RNF	NET, COMP, STOR, APP,



		standard di qualità siano rispettati, va stabilito per tutto lo sviluppo software in outsourcing. Lo sviluppo di tutti i software in outsourcing è oggetto di vigilanza e controllo da parte dell'organizzazione e deve includere i requisiti di sicurezza, revisioni di sicurezza indipendenti dall'ambiente in outsourcing eseguiti da una persona certificata, sugli sviluppatori e sul software. Certificazione ai fini di questo controllo deve essere definita come un ISO / IEC 17024, o in base alla certificazione di competenza legislativa dove l'organizzazione di outsourcing ha il proprio domicilio legale.		DATA
E9	Installazioni di software non autorizzate	Politiche e procedure sono stabilite e meccanismi attuati per limitare l'installazione di software non autorizzato.	RNF	NET, COMP, STOR, APP

4.2.6. Requisiti di resilienza

ID requisito	Nome requisito	Specifiche requisito	RF/RNF	Oggetti architetturali
F1	Programma di gestione	Policy, processo e procedure che definiscono business continuity e disaster recovery, devono essere messe in atto per ridurre al minimo l'impatto di un evento di rischio, e facilitare il recupero del	RNF	FIS, NET, COMP, STOR, APP, DATA



		patrimonio informativo (che può essere il risultato di, ad esempio, disastri naturali, incidenti, avarie delle attrezzature e le azioni deliberate), attraverso una combinazione di controlli preventivi e di recupero, in conformità con i requisiti normativi, legali, contrattuali, e coerenti con gli standard di settore. Il programma di gestione della resilienza deve essere comunicato a tutti i partecipanti organizzativi, con l'obbligo di conoscerli prima dell'adozione e devono essere pubblicati, ospitati, conservati, registrati e diffusi a strutture multiple che devono essere accessibili in caso di incidente.		
F2	Analisi di impatto	Ci sarà un metodo definito e documentato per determinare l'impatto di eventuali interruzioni per l'organizzazione, che deve includere quanto segue: • Identificare i prodotti e i servizi critici • Identificare tutte le dipendenze, inclusi i processi, applicazioni, business partner e fornitori di servizi terzi • Comprendere le minacce a prodotti e servizi critici • determinare gli impatti derivanti da interruzioni pianificate o impreviste e come queste variano nel tempo • Stabilire il periodo massimo	RNF	FIS, NET, COMP, STOR, APP, DATA



		tollerabile per l'interruzione • stabilire le priorità per il recupero • Stabilire obiettivi dei tempi di recupero per la ripresa di prodotti e servizi critici nel loro periodo massimo tollerabile di interruzione • Stimare le risorse necessarie per il ripristino		
F3	Pianificazione della continuità operativa	Un quadro coerente unificato per la pianificazione della continuità operativa e del piano di sviluppo deve essere formalizzato, documentato e adottato, per garantire che tutti i piani di business continuity siano coerenti con i requisiti di manutenzione e di sicurezza delle informazioni. I requisiti per piani di continuità operativa sono i seguenti: • scopo e campo di applicazione definiti, in linea con le dipendenze rilevanti • accessibili e comprensibili da parte di coloro che li utilizzano • di proprietà di una (o più) persone fisiche, che siano responsabili della loro revisione, aggiornamento e approvazione • Linee definite di comunicazione, ruoli e responsabilità • le procedure di recupero dettagliate, work-around	RNF	FIS, NET, COMP, STOR, APP, DATA



		manuali e informazioni di riferimento		
F4	Testing della continuità operativa	Piani di continuità operativa saranno oggetto di test a intervalli pianificati, oppure in base a importanti modifiche organizzative o ambientali, per poter garantire la continua efficacia.	RNF	FIS, NET, COMP, STOR, APP, DATA
F5	Rischi ambientali	La protezione fisica contro i danni da cause naturali e disastri, come pure gli attacchi deliberati, compresi gli incendi, inondazioni, scariche elettriche atmosferiche, tempeste solari geomagnetiche indotta, vento, terremoti, tsunami, esplosioni nucleari, contrattacco, attività vulcanica, rischio biologico, disordini civili, colate di fango, forme di attività tettonica, e altre catastrofi naturali o di origine umana, devono essere tenuti in considerazione, e contromisure idonee devono essere progettate e applicate.	RNF	FIS
F6	Collocazione dei sistemi	Per ridurre i rischi derivanti da minacce ambientali e da opportunità di accesso non autorizzato, le attrezzature devono essere collocate lontano dai luoghi soggetti a rischi elevati di calamità ambientali e ridondate con apparecchiature di riserva ad una distanza ragionevole.	RNF	FIS
F7	Guasti agli impianti di potenza	I meccanismi di sicurezza e ridondanza sono attuati per proteggere le apparecchiature dalle interruzioni di servizi di pubblica utilità (ad esempio,	RNF	FIS, NET, COMP



		mancanza di corrente, interruzioni di rete, ecc.)		
F8	Impianti di telecomunicazioni	Gli impianti di telecomunicazione, cablaggio e ricetrasmissione dati o servizi di supporto devono essere protetti da intercettazioni o danni e progettati con ridondanze, fonti di energia alternative e routing alternativi.	RNF	FIS, NET



4.3. Classi di servizio

In questa sezione vengono definite le classi di servizio a cui riferirsi per una pratica catalogazione dei servizi cloud, presentate nella suddivisione per modelli di servizio (IaaS, PaaS, SaaS). Tale classificazione può essere utile nel lavoro di specifica dei requisiti da effettuare nelle procedure di qualifica e certificazione. Viene infine presentata una tabella utile in tale lavoro, che consente di elencare gli ID dei requisiti, di cui nelle tabelle della sezione 4.2, alle diverse classi di servizio.

4.3.1. *Classi di servizi IaaS*

1. Fornitura di risorse
2. Memorizzazione
3. Macchine virtuali
4. Server
5. Bilanciamento di carico

4.3.2. *Classi di servizi PaaS*

1. Esecuzione di applicazioni
2. Strumenti di sviluppo
3. Ambienti per la consegna di applicazioni
4. Basi di dati
5. Server web
6. Piattaforme aperte

4.3.3. *Classi di servizi SaaS*

1. SSO
2. accounting



3. Billing
4. collaboration
5. CRM
6. MIS
7. ERP
8. HRM
9. CM
10. invoicing
11. service desk management
12. Personal Productivity
13. Project Management

4.3.4. *Tabella dei requisiti per classi di servizio*

Modelli di servizio	Classi di servizio	Requisiti
IaaS	Fornitura di risorse	
	Memorizzazione	
	macchine virtuali	
	Server	
	bilanciamento di carico	
PaaS	Esecuzione di applicazioni	
	Strumenti di sviluppo	
	Ambienti per la consegna di applicazioni	
	Basi di dati	
	Server web	
SaaS	Piattaforme aperte	
	SSO	
	accounting	
	Billing	
	collaboration	
	CRM	
	MIS	



ERP	
HRM	
CM	
invoicing	
service desk management	
Personal Productivity	
Project Management	



BIBLIOGRAFIA

- [1] GdL 4 – Commissione di Coordinamento SPC, “Contenuti delle gare s2 e s3”, novembre 2011.
- [2] Raccomandazioni e proposte sull'utilizzo del Cloud Computing nella Pubblica Amministrazione. Versione 2.0 del 28 giugno 2012
- [3] Tier Classification Define Site Infrastructure Performance, W. Pitt Turner IV et al.
- [4] I servizi minimi essenziali per l'adozione delle soluzioni di Disaster Recovery, in linea con l'art. 50-bis del CAD. Versione 2.4 del 30/07/2012
- [5] CCM (Cloud Control Matrix), Cloud Security Alliance, adept by FedRAMP (Government Cloud)
- [6] Agenda Digitale Italiana
- [7] Dal Cloud Computing al G-Cloud: rischi e opportunità per la PA. Flavia Marzano
- [8] An analysis of G-Cloud sales. Andy Powell, 29 Aprile 2013
- [9] Cloud Computing Portability and Interoperability. Open Group Guide, Aprile 2013
- [10] Cloud: vanno indicati ruoli e responsabilità, Andrea Lisi e Sarah Ungaro, Professioni & Imprese 24
- [11] NIST Cloud Computing Reference Architecture, September 2011
- [12] OpenStack, Open source software for building private and public clouds

