Il modello di Cloud della PA

italia

04 mar 2024

Indice

Questo documento è obsoleto

Il riferimento attuale è Strategia Cloud Italia[4].

La razionalizzazione del patrimonio ICT, il consolidamento dei data center e l'adozione progressiva del paradigma del "cloud computing" rappresentano specifiche azioni trasversali della Strategia per la Crescita digitale del Paese[5], documento approvato in versione definitiva nel giugno 2016.

La strategia, in linea con gli interventi dell'Unione europea, fornisce un quadro di riferimento per le politiche di digitalizzazione del Paese, mentre il Piano Triennale per l'Informatica[6] ha tradotto le indicazioni strategiche in azioni operative conseguibili nel periodo di riferimento.

In questo documento viene descritta la strategia per l'adozione del cloud computing nella Pubblica Amministrazione secondo quanto previsto dal Piano Triennale per l'Informatica 2019 - 2021[7]

[4] https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/
[5] http://www.agid.gov.it/agenda-digitale/agenda-digitale-italiana/crescita-digitale-banda-ultralarga
[6] https://pianotriennale-ict.italia.it/
[7] https://pianotriennale-ict.italia.it/

CAPITOLO 1

Cos'è il cloud

Questo documento è obsoleto

Il riferimento attuale è Strategia Cloud Italia[8].

Il cloud computing, più semplicemente cloud, è un modello di infrastrutture informatiche che consente di disporre, tramite internet, di un insieme di risorse di calcolo (ad es. reti, server, storage, applicazioni e servizi) che possono essere rapidamente erogate come un servizio.

Questo modello consente di semplificare drasticamente la gestione dei sistemi informativi, trasformando le infrastrutture fisiche in servizi virtuali fruibili in base al consumo di risorse.

Il modello Cloud introduce dei vantaggi significativi rispetto alle tradizionali soluzioni hardware, che consentono di:

- effettuare in maniera continua gli aggiornamenti dell'infrastruttura e delle applicazioni;
- usufruire delle applicazioni da qualsiasi dispositivo in qualsiasi luogo tramite l'accesso internet;
- avere maggiore flessibilità nel provare nuovi servizi o apportare modifiche, con costi minimi;
- ridurre i rischi legati alla gestione della sicurezza (fisica e logica) delle infrastrutture IT;
- avere importanti economie nell'utilizzo del software, in quanto consentito pagare le risorse come servizi in base al consumo ("pay per use"), evitando investimenti iniziali nell'infrastruttura e costi legati alle licenze di utilizzo;
- ridurre i costi complessivi collegati alla location dei Data center (affitti, consumi elettrici, personale non ICT).

Inoltre, i servizi cloud sono tipicamente suddivisi in tre tipologie:

- *software-as-a-service (SaaS)*, si tratta di applicazioni software accessibili tramite Internet sfruttando diverse tipologie di dispositivi (Desktop, Mobile, etc);
- *platform-as-a-service (PaaS)*, ovvero piattaforme per sviluppare, testare e distribuire le applicazioni su internet;
- *infrastructure-as-a-service (IaaS)*, ovvero l'infrastruttura tecnologica fisica e virtuale in grado di fornire risorse di computing, networking e storage da remoto e mediante API (Application Programming Interfaces), senza la necessità di acquistare hardware.

[8] https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/

È possibile consultare le definizioni del modello cloud e le proprietà specifiche dei servizi presso il NIST[9].

[9] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

CAPITOLO 2

Perché usare il cloud

Questo documento è obsoleto

Il riferimento attuale è Strategia Cloud Italia[10].

> Per una vasta gamma di servizi e sistemi, che vanno dalla sicurezza informatica alla produttività e all'archiviazione, le soluzioni cloud rappresentano spesso la soluzione più vantaggiosa disponibile sul mercato e, in alcuni casi, anche la più utilizzata.

2.1 Riduzione dei costi

Le applicazioni che utilizzano risorse hardware locali (*on-premise*) richiedono un investimento iniziale significativo, anche se il software utilizzato è gratuito o open source. Data center, reti, server, storage e sistemi operativi sono necessari per ospitare anche il software gestionale più banale. Tutte queste componenti di supporto richiedono non solo investimenti, tempo e personale dedicato per ottenere delle infrastrutture di qualità, ma anche significativi aggiornamenti periodici.

Le applicazioni cloud (SaaS) si pagano generalmente in base al consumo, consentono di gestire la crescita di un servizio in maniera dinamica e richiedono investimenti iniziali estremamente limitati. La decisione di migrare verso una nuova soluzione non è, quindi, condizionata da eventuali investimenti già fatti; poiché si paga solo il consumo della risorsa, quando un servizio non è più utilizzato, non è più un costo.

Il ridotto investimento iniziale implica una riduzione del rischio, è così possibile sviluppare e testare, su scala ridotta, soluzioni che possono essere valutate velocemente per poi essere adottate, modificate radicalmente o abbandonate, con costi minimi.

Grazie alla sua natura dinamica il cloud computing facilita la sperimentazione e lo sviluppo di nuove soluzioni.

Le applicazioni basate su hardware in locale (data center) richiedono un piano di investimenti che deve tener conto dei prezzi riferiti al momento della sottoscrizione del contratto e di alcuni anni di manutenzione e supporto. I costi complessivi, per es. licenze, energia elettrica, potenza di calcolo, manodopera e così via, raramente diminuiscono nel

[10] https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/

corso della durata del servizio. Al contrario, i servizi cloud tendono ad essere sempre più economici per le dinamiche di mercato. La pressione competitiva, l'hardware migliorato e l'aumento dei tassi di utilizzo stanno riducendo progressivamente i costi delle applicazioni SaaS e delle infrastrutture virtuali (IaaS).

2.2 Facilità degli aggiornamenti

Le soluzioni IT commerciali o auto-sviluppate in locale richiedono finanziamenti, impegno e pianificazione per poter essere aggiornate costantemente. Il supporto e gli aggiornamenti sono attività costose e complicate da gestire ed è molto difficile per qualsiasi organizzazione tenere il passo con la costante richiesta di aggiornamenti e patch di sicurezza. Ne consegue che, spesso, le infrastrutture della PA non vengono adeguatamente aggiornate.

I servizi di cloud pubblico, invece, vengono generalmente aggiornati, migliorati e mantenuti durante tutto il loro ciclo di vita dal fornitore, e il tutto è incluso nei costi. Chi acquista questi servizi non ha bisogno di aggiornare i sistemi operativi dei server, acquistare hardware, contrattualizzare personale esterno, pianificare le operazioni o migrare i dati per ottenere i benefici della tecnologia più recente. Il miglioramento continuo viene garantito a chi usa tali servizi senza alcuno sforzo, in maniera incrementale.

2.3 Supporto semplificato

I servizi IT tradizionali spesso dipendono dal software client installato sul computer dell'utente. Il client installato deve essere gestito insieme a tutte le altre applicazioni locali dell'utente. In molti casi, questo rende necessario soddisfare dipendenze applicative molto specifiche legate alle versioni del sistema operativo e degli aggiornamenti di sistema affinché il software client sia installato e funzioni correttamente.

Gli aggiornamenti devono essere testati prima di essere applicati su numero elevato di sistemi e, a volte, un'applicazione obsoleta può rallentare l'adozione di nuovi sistemi operativi e di applicazioni più moderne.

I servizi cloud sono progettati per essere fruibili tramite internet. Per rimanere sul mercato, i fornitori devono aggiornare i propri servizi per supportare le ultime versioni dei browser, i sistemi operativi e le scelte dei dispositivi dei propri utenti.

Per una PA che gestisce migliaia di dispositivi, come laptop, desktop e dispositivi mobili, una qualsiasi soluzione che riduca la quantità di lavoro necessario a mantenere il software aggiornato rappresenta un gran vantaggio.

Oltre ai browser, i servizi cloud offrono altre modalità per utilizzare i servizi e accedere ai dati: spesso sono disponibili applicazioni per tablet e telefoni oppure i servizi sono accessibili tramite API che consentono di automatizzare l'accesso al servizio. Tutte queste opzioni standardizzano, semplificano e rendono user-friendly l'uso dei servizi cloud.

2.4 Elasticità reale

Anche quando le soluzioni IT *on-premise* sono scalabili hanno dei limiti, ad esempio, è necessario pianificare investimenti e sforzi costanti per mantenere i margini sufficienti di scalabilità ed evitare situazioni di sotto o sovradimensionamento. Per poter garantire la vera elasticità, è necessario mantenere costantemente un grande surplus di risorse che rimangono tuttavia inutilizzate per la maggior parte del tempo.

A differenza delle soluzioni *on-premise*, i servizi cloud sono davvero elastici, le risorse di calcolo, storage o rete possono essere consumate solo quando richiesto e dismesse quando non sono più necessarie, eliminando così tutta la complessità nella pianificazione della capacità dell'infrastruttura IT. Inoltre, non ci sono ritardi associati all'attesa per instanziare i server o lo storage durante la fase di ridimensionamento. Infine, il paradigma cloud non richiede alcun investimento a lungo termine e non comporta quello spreco di risorse determinato dalla sottoutilizzazione della capacità.

2.5 Sicurezza e Privacy

Amministrare le infrastrutture IT comporta responsabilità non solo di tipo economico-amministrativo ma soprattutto di sicurezza e di protezione dei dati personali. Le recenti normative in materia di privacy e di sicurezza informatica impongono infatti anche alle pubbliche amministrazioni l'adozione di misure tecniche e organizzative adeguate a garantire la sicurezza dei trattamenti dei dati.

Il modello cloud viene incontro alle esigenze delle PA anche sotto questo aspetto, facilitando la separazione delle problematiche di sicurezza per l'infrastruttura fisica, per il software e per la gestione logica delle applicazioni. Inoltre, le applicazioni cloud sono in grado di mettere a disposizione dell'amministratore strumenti di auditing e controllo delle informazioni che consentono interventi puntuali all'insorgere di eventuali problemi.

Certamente non basta dotarsi di soluzioni cloud per assicurare privacy ai propri utenti e sicurezza delle infrastrutture e servizi IT, bensì serve un processo continuo di vigilanza e controllo che fin dalla prima fase di progettazione dei servizi, agisca trasversalmente su tutte le aree di interesse, e che sia costantemente aggiornato rispetto allo stato dell'arte delle principali misure di sicurezza.

CAPITOLO 3

Il Cloud della PA

Questo documento è obsoleto

Il riferimento attuale è Strategia Cloud Italia[11].

Perché la PA ha deciso di definire e adottare un modello cloud *ad hoc* denominato "Cloud della PA"?

Non tutti i servizi e le infrastrutture di cloud computing sono uguali. In alcuni casi tali servizi possono anche non rispettare i principali standard di sicurezza, garanzie operative e affidabilità definiti a livello internazionale. Questa disomogeneità può rappresentare un rischio quando si affidano i propri dati a provider che non garantiscono dei livelli minimi di sicurezza e affidabilità.

Il modello *Cloud della PA* consente di mitigare tale rischio, qualificando servizi e infrastrutture cloud secondo specifici parametri di sicurezza e affidabilità idonei per le esigenze della PA, nel rispetto dei seguenti principi:

- miglioramento dei livelli di servizio, accessibilità, usabilità e sicurezza;
- interoperabilità dei servizi nell'ambito del modello Cloud della PA;
- riduzione del rischio di «vendor lock-in»;
- riqualificazione dell'offerta, ampliamento e diversificazione del mercato dei fornitori;
- resilienza, scalabilità, «reversibilità» e protezione dei dati;
- apertura del mercato alle Piccole e Medie Imprese (PMI).

Il Cloud della PA si compone di infrastrutture e servizi, qualificati da AgID sulla base di un insieme minimo di requisiti, secondo il modello riportato di seguito. Inoltre, servizi e infrastrutture saranno consultabili e confrontabili mediante una piattaforma dedicata, il Cloud Marketplace[12], una volta conseguita la qualificazione AgID secondo quanto descritto nelle circolari AgID n. 2 e n. 3 del 2018[13].

[11] https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/
[12] https://cloud.italia.it/marketplace/
[13] https://cloud.italia.it/it/latest/

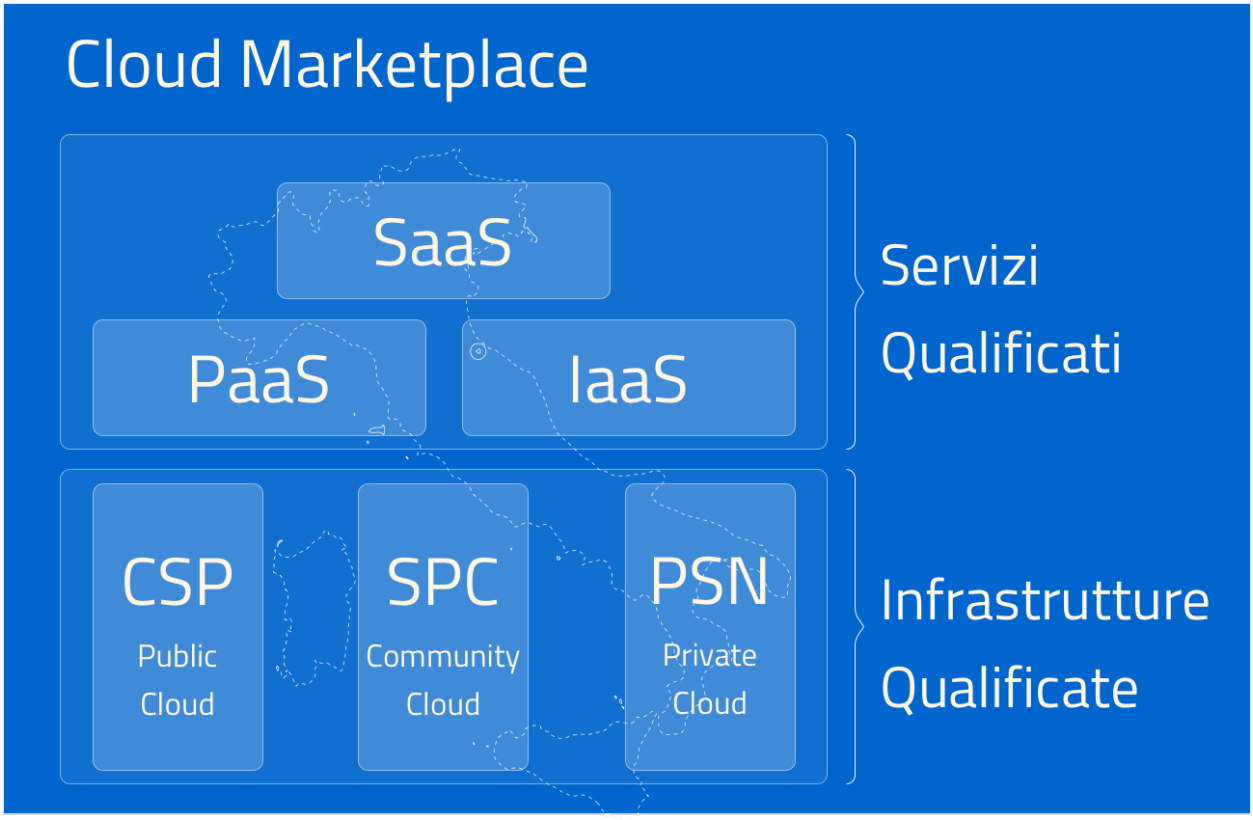

Fig. 3.1: Le componenti del modello del Cloud della PA

Il Cloud della PA è un modello cloud fortemente *misto* che include infrastrutture e servizi di tipo: **Public Cloud**[1], l'offerta dei Cloud Service Provider pubblici qualificati da AgID; **Private Cloud**[2], le infrastrutture e servizi erogati dai PSN; **Community Cloud**[3], i servizi SPC Cloud Lotto 1[14]. Questo modello consente di soddisfare le diverse e complesse esigenze del settore pubblico.

Le infrastrutture qualificate si suddividono in tre categorie:

- Poli strategici nazionali o PSN: l'insieme delle infrastrutture IT (centralizzate o distribuite), ad alta disponibilità, di proprietà dello Stato, elette a Polo Strategico Nazionale dalla Presidenza del Consiglio dei Ministri ed in grado di erogare, in maniera continuativa, servizi cloud e hosting ad altre amministrazioni;
- Cloud Service Provider o CSP: le infrastrutture e i servizi di *Public Cloud* offerti dai cloud service provider qualificati da AgID;
- SPC Cloud: i servizi cloud infrastrutturali erogati nell'ambito del contratto quadro Consip - Cloud SPC Lotto 1.

I servizi SaaS del *Cloud della PA* dovranno necessariamente essere erogati mediante una o più infrastrutture qualificate.

3.1 I criteri di scelta dei servizi cloud

Il modello Cloud della PA fornisce una visione unitaria delle diverse tipologie di servizi previste per la PA. Il modello si ispira al principio **Cloud First** che propone di valutare l'adozione del paradigma cloud prima delle soluzioni tradizionali (generalmente basate su servizi di hosting o housing).

Al fine di selezionare, nell'ambito del Cloud della PA, il servizio e la modalità di erogazione più rispondenti alle esigenze dell'Amministrazione è opportuno applicare *la preferenza* **SaaS First** , ovvero indirizzare la propria scelta sui servizi SaaS già presenti e attivi nel Marketplace Cloud, se conformi alle necessità dell'amministrazione. La scelta dei servizi SaaS consente di beneficiare in pieno dei vantaggi offerti dal paradigma cloud e di ridurre drasticamente costi e sforzi amministrativi, in quanto non necessita di attività tecnica di gestione e sviluppo dedicato, cosa necessaria invece con l'acquisizione di servizi IaaS e PaaS.

Nel caso in cui, invece, non fossero disponibili servizi SaaS specifici, la scelta dei servizi IaaS e PaaS può avvenire sempre mediante il Cloud Marketplace.

Diventa, quindi, cruciale individuare quale delle tre tipologie di infrastrutture qualificate scegliere, tale scelta è indirizzata da 2 fattori:

- la finalità del servizio all'utente e la tipologia di dati trattati;
- le caratteristiche commerciali del servizio cloud.

Non si tratta di una scelta tecnologica, in quanto le infrastrutture qualificate sono tutte tecnicamente omogenee come previsto dal Piano Triennale e in particolare dalla qualificazione delle infrastrutture.

Nella maggior parte dei casi in cui il servizio richiesto non gestisce dati di particolare rilevanza per la sicurezza nazionale la PA potrà ricorrere all'utilizzo di servizi commerciali o pubblici (*public cloud CSP o community cloud SPC*) dove la scelta sarà guidata esclusivamente dalle caratteristiche di qualità e prezzo offerte dai fornitori CSP o SPC, nel rispetto della normativa vigente in ambito di acquisizione di beni e servizi.

Nel caso dei PSN, vista la rilevanza e i costi correlati di tali infrastrutture sarà cura del Governo valutare e disporre quali servizi considerati asset strategici nazionali dovranno essere erogati per mezzo degli stessi.

[1] L'infrastruttura cloud è predisposta per fornire servizi cloud a molteplici tipologie di clienti (es. società private, enti pubblici, ecc.).

[2] L'infrastruttura cloud è predisposta per fornire servizi cloud ad uso esclusivo di una singola organizzazione (in questo caso la PA). L'infrastruttura deve essere di proprietà e può essere gestita dall'organizzazione stessa oppure da terze parti.

[3] L'infrastruttura cloud è predisposta per fornire servizi cloud ad una specifica comunità di organizzazioni che hanno requisiti e obiettivi condivisi. L'infrastruttura può essere di proprietà, gestita dall'organizzazione stessa oppure da terze parti (in questo caso da un Raggruppamento Temporaneo di Imprese).

[14] https://www.cloudspc.it

3.1.1 SaaS e interoperabilità

Quando i servizi SaaS sono erogati da una PA tramite API conformi alle Linee Guida di Interoperabilità, si hanno dei vantaggi in termini di uniformità dei modelli di dato e del rispetto delle indicazioni sulla gestione della disponibilità del servizio. In questo caso l'interoperabilità dell'erogatore SaaS «contagia» l'implementazione del fruitore, incentivando la creazione di nuovi servizi conformi (eg. quando le API vengono usate per creare a loro volta nuovi servizi). Per innescare questo circolo virtuoso è fondamentale che tutte le API della PA si adeguino alle Linee Guida di Interoperabilità.

3.2 Il Marketplace delle infrastrutture e dei servizi cloud

Servizi e infrastrutture qualificate del Cloud della PA sono esposti e consultabili mediante il *Marketplace Cloud*, una piattaforma che consente di visualizzare la scheda di ogni servizio mettendo in evidenza le caratteristiche, il costo e i livelli di servizio dichiarati dal fornitore. Le PA possono confrontare servizi analoghi e decidere, in base alle loro esigenze, le soluzioni più adatte. Il Marketplace indica anche le modalità di acquisizione con cui uno specifico servizio potrà essere acquisito da una amministrazione rimandando allo strumento di procurement disponibile (p.e. portale acquistinretepa.it[15]) per procedere con l'acquisizione.

Importante: A decorrere dal 1º aprile 2019, le Amministrazioni Pubbliche possono acquisire esclusivamente servizi IaaS, PaaS e SaaS qualificati da AgID e pubblicati nel Catalogo dei servizi Cloud per la PA qualificati.

Per maggiori informazioni si rimanda alle Circolari AgID 2/2018 e 3/2018[16].

3.3 La qualificazione dei Servizi cloud

> Le procedure di qualificazione dei servizi cloud sono state definite cercando di sviluppare un processo semplice e veloce, dove la maggior parte dei requisiti di qualificazione possono essere forniti in forma di autocertificazione.
>
> La procedura di qualificazione e tutti i requisiti previsti sono stati definiti dalle Circolari AgID n. 2 e n. 3 del 9 aprile 2018[17], cui si rimanda per le informazioni di dettaglio.

3.3.1 Servizi SaaS

La qualificazione dei servizi SaaS nell'ambito del Cloud della PA assicura il rispetto di alcuni requisiti, tra cui:

- la **sicurezza** applicativa, in termini di gestione dei dati, sicurezza di rete, aggiornamenti delle vulnerabilità note;
- la disponibilità di un adeguato **supporto tecnico** per il cliente (multicanale, con prefissati e garantiti orari di reperibilità);
- la **trasparenza** e la **disponibilità di informazioni** dettagliate e aggiornate sulle modalità di erogazione del servizio e di esportazione dei dati;
- la **disponibilità di incident report**, statistiche e strumenti di **monitoraggio** delle risorse utilizzate, dei costi e dei livelli di servizio;

[15] https://www.acquistinretepa.it/
[16] https://cloud.italia.it/it/latest/
[17] https://cloud.italia.it/it/latest/

- la **qualità del servizio**, con un insieme minimo di livelli di servizio garantiti obbligatori (ad es. disponibilità del servizio, tempistiche di risposta dell'assistenza tecnica), più ulteriori livelli di servizio proposti dal fornitore tipicamente riguardanti la larghezza di banda, i tempi di ripristino del servizio ed altre metriche relative alla capacità di elaborazione;
- la **protezione dei dati** e la **portabilità** in tutte le fasi di avanzamento della fornitura (attivazione del servizio, erogazione del servizio e disattivazione del servizio), con procedure chiare e documentate e tutte le necessarie garanzie per l'utilizzatore del servizio;
- l'**interoperabilità** mediante opportune API che dovranno rifarsi alle migliori pratiche di gestione (API management), prevedendo in particolare la tracciabilità delle versioni disponibili, la tracciabilità delle richieste ricevute ed evase, la documentazione degli endpoint SOAP e/o REST disponibili e delle rispettive modalità di invocazione;
- ridurre il rischio di dipendenza esclusiva dal fornitore (**lock in**), garantendo in tal modo alle PA l'esportabilità dei propri dati in un formato interoperabile verso un'altra piattaforma.

Inoltre, la qualificazione rafforza la richiesta di protezione dei dati, dando rilievo alla conformità con le prescrizioni previste dalle norme (nazionali ed europee) in materia di sicurezza informatica e riservatezza dei dati.

3.3.2 Servizi IaaS e PaaS

I servizi cloud di tipo IaaS e PaaS consentono di disporre rispettivamente di risorse virtuali e piattaforme di sviluppo con le quali le amministrazioni possono sviluppare nuove applicazioni e servizi non disponibili tra i SaaS presenti nel Marketplace. Inoltre le amministrazioni, laddove indispensabile, possono virtualizzare le applicazioni tradizionali non predisposte per il modello cloud.

La **qualificazione dei servizi IaaS e PaaS** pone particolare attenzione ai seguenti aspetti:

- la **gestione della sicurezza** estesa a tutti gli aspetti che riguardano sia l'infrastruttura che i servizi;
- la **gestione delle configurazioni** e la **gestione dei cambiamenti**, aspetti fondamentali per l'amministrazione di infrastrutture IT complesse;
- la **gestione degli incidenti** e il recovery dell'infrastruttura in seguito ad eventi critici;
- l'**interoperabilità** con altri servizi e altre infrastrutture cloud dello stesso tipo, mediante l'utilizzo di standard aperti (ad es. Open Virtualization Format) ed opportune API.

Per assicurare che tutte queste problematiche vengano gestite correttamente, la qualificazione richiede che il fornitore e i servizi sottoposti a qualificazione siano conformi alle buone pratiche previste dai più importanti e diffusi standard del settore (es. norme UNI, ISO/IEC, ecc.), oltre che, in alcuni casi, a certificazioni specifiche (es. ISO/IEC 27001).

3.4 La qualificazione delle Infrastrutture

Le infrastrutture IT fisiche e virtuali destinate all'utilizzo da parte della pubblica amministrazione devono dimostrare di possedere determinati requisiti:

- **organizzativi** - procedure certificate per l'erogazione dei servizi, la gestione di risorse e processi, il supporto agli utenti , la gestione dei cambiamenti;
- **di sicurezza e affidabilità** - definizione dei livelli di servizio, privacy, sicurezza e protezione dei dati;
- **di performance e interoperabilità** - garanzie sulle performance delle infrastrutture e sulla capacità di interoperare con altre infrastrutture analoghe mediante standard aperti, la possibilità di esportare i dati dei servizi erogati in formati aperti.

La verifica del possesso di tali requisiti costituisce una parte fondante del processo di qualificazione delle infrastrutture IT che possono operare nell'ambito del Cloud della PA.

Come precedentemente descritto, le infrastrutture qualificate ad erogare i servizi cloud qualificati possono essere CSP (Cloud Service Provider), SPC Cloud Lotto 1[18], PSN (Poli Strategici Nazionali).

3.4.1 Cloud Service Provider qualificati - Public Cloud

I Cloud service provider qualificati da AgID possono erogare servizi di tipo *Public Cloud* alle amministrazioni. Le qualificazioni AgID assicurano che le infrastrutture e i servizi dei CSP siano sviluppati ed operati secondo criteri minimi di affidabilità e sicurezza considerati necessari per i servizi digitali della PA.

La procedura di qualificazione delle **infrastrutture dei CSP** pone particolare attenzione ai seguenti aspetti:

- la **gestione della sicurezza** estesa a tutti gli ambiti che riguardano l'infrastruttura dei servizi cloud (ISO/IEC 27001 estesa ai controlli ISO/IEC 27017 e ISO/IEC 27018);
- la gestione delle **configurazioni** e dei **cambiamenti** *(change management)*;
- la **gestione degli incidenti** e il *recovery* dell'infrastruttura in seguito ad eventi critici;

Per assicurare che tutte queste problematiche vengano gestite correttamente, la qualificazione richiede che vengano adottate dal fornitore tutte le buone pratiche previste dai più importanti e diffusi standard del settore (es. ISO/IEC 27002).

L'elenco dei CSP qualificati è disponibile sul Marketplace Cloud.

3.4.2 Cloud SPC Lotto 1 - Community Cloud

L'infrastruttura di tipo "Community Cloud" è realizzata dal Raggruppamento Temporaneo d'Impresa aggiudicatario del Contratto Quadro Consip SPC Cloud Lotto 1[19]. La descrizione dettagliata dei servizi e delle modalità di approvvigionamento è presente sul sito dedicato[20].

3.4.3 Poli Strategici Nazionali - Private Cloud

Nel modello Cloud della PA, i Poli Strategici Nazionali (cd. PSN) soddisfano la necessità di mantenere il controllo diretto da parte dello Stato sulle infrastrutture IT (Connettività, Data Center e piattaforme cloud) che erogano servizi considerati asset strategici nazionali. I PSN sono destinati a tutti quei servizi di rilevanza strategica e di interesse nazionale per i quali non è consigliabile che la gestione dell'infrastruttura e dei dati venga delegata a terze parti (es. sicurezza nazionale).

I **Poli strategici nazionali** saranno individuati dal **Governo** sulla base di una selezione di soggetti idonei svolta attraverso il processo definito nella Circolare n. 5 del 30 novembre 2017[21] pubblicata da AgID.

I PSN, se individuati, dovranno rispettare elevati requisiti di sicurezza, affidabilità, e capacità operativa e saranno coordinati centralmente per erogare servizi cloud omogenei, utilizzando piattaforme condivise.

[18] https://www.cloudspc.it/
[19] https://www.cloudspc.it/
[20] https://www.cloudspc.it/
[21] https://www.censimentoict.italia.it/it/latest/docs/circolari/2017113005.html

3.5 La piattaforma da utilizzare per la qualificazione

AgID ha previsto l'utilizzo di una piattaforma dedicata con cui il fornitore dei servizi cloud, che intende conseguire la qualificazione CSP o SaaS, trasmette tutte le informazioni, le dichiarazioni e la documentazione prevista.

La piattaforma è accessibile all'indirizzo https://cloud.italia.it/marketplace/supplier/.

Note

CAPITOLO 4

Il Cloud Enablement

La situazione di elevata frammentazione e disomogeneità dei sistemi informativi delle PA necessita di un percorso evolutivo verso un utilizzo efficiente e flessibile delle tecnologie IT, al fine di garantire elevate economie gestionali e favorire una maggiore reattività nell'erogare servizi sempre più adeguati alle esigenze di cittadini e imprese.

Il consolidamento delle infrastrutture IT della Pubblica Amministrazione implica una massiccia migrazione dei servizi attualmente erogati in modalità tradizionale verso un ambiente cloud, così come descritto in precedenza.

In questo contesto AgID e Team Digitale hanno elaborato un piano di abilitazione al cloud. Il *Cloud Enablement* è il processo che abilita un'organizzazione a creare, operare e mantenere le proprie infrastrutture IT utilizzando tecnologie e servizi cloud. Nell'ottica del consolidamento e della razionalizzazione, tale attività riorganizza i processi IT in ambienti di cloud pubblico, privato o ibrido.

Nella definizione del **piano di abilitazione al Cloud della PA** sono stati individuati tre elementi principali che caratterizzano la strategia di questo percorso di trasformazione:

- *Il principio Cloud First*: per la definizione di nuovi progetti e per la progettazione dei nuovi servizi nell'ambito di nuove iniziative da avviare da parte della PA in coerenza con il modello Cloud della PA;
- *La strategia di Cloud Enablement*: per la migrazione delle infrastrutture e delle applicazioni esistenti verso il modello Cloud della PA;
- *Centri di competenza*: per il consolidamento e potenziamento delle competenze mediante la creazione di Centri di Competenze (Soggetti Aggregatori) - la creazione di una comunità allargata di tecnici, esperti e managers dell'IT per discutere, proporre standard e regolamenti dei servizi digitali, condividere informazioni, soluzioni e competenze utili a mantenere, aggiornare e aumentare l'affidabilità dei sistemi, automatizzandone le procedure.

4.1 Il principio Cloud First

In base al principio *Cloud First*, le PA in fase di definizione di un nuovo progetto, e/o sviluppo di nuovi servizi, devono, in via prioritaria, adottare il paradigma cloud in particolare i servizi SaaS, prima di qualsiasi altra opzione tecnologica, in coerenza con il modello Cloud della PA e le linee guida su acquisizione e riuso di software per le pubbliche amministrazioni[22].

[22] https://lg-acquisizione-e-riuso-software-per-la-pa.readthedocs.io/it/latest/

Per *Cloud First* si intende, quindi, anche la necessità di ricorrere a strumenti e tecnologie di tipo cloud, nelle sue diverse articolazioni IaaS, PaaS e SaaS, nel momento in cui le pubbliche amministrazioni intendono acquisire sul mercato nuove soluzioni e servizi ICT per la realizzazione di un nuovo progetto o nuovi servizi destinati a cittadini, imprese o utenti interni alla PA.

Per sfruttare in pieno i vantaggi del cloud, è opportuno che le amministrazioni valutino in prima istanza la presenza di servizi SaaS nel Marketplace Cloud[23] che rispondono alle proprie esigenze e, solo in seconda istanza, prendere in considerazione soluzioni PaaS e infine IaaS.

Sarà fondamentale per le stesse amministrazioni ribaltare la logica del servizio cloud sui servizi sviluppati ed erogati dalle stesse PA stabilendo adeguati livelli di servizio per i cittadini e le imprese.

In sinergia con la strategia di *Cloud Enablement* per la migrazione dell'esistente, il principio *Cloud First* nasce con l'obiettivo di adottare il modello Cloud della PA da subito per tutte le nuove iniziative che le PA intendono avviare.

4.2 La strategia di Cloud Enablement

AgID e il Team per la Trasformazione Digitale hanno definito il modello strategico evolutivo per la migrazione del patrimonio IT esistente verso il Cloud della PA mediante due componenti principali:

1. **il programma di Cloud Enablement nazionale**, ovvero l'insieme dei progetti specifici che consentiranno alle PA di migrare le applicazioni in ambiente cloud;
2. **l'ambiente (cd. framework) di lavoro del Cloud Enablement** costituito dall'insieme di risorse, strategie operative, metodologie e strumenti necessari per attuare il *Cloud Enablement Program* della PA.

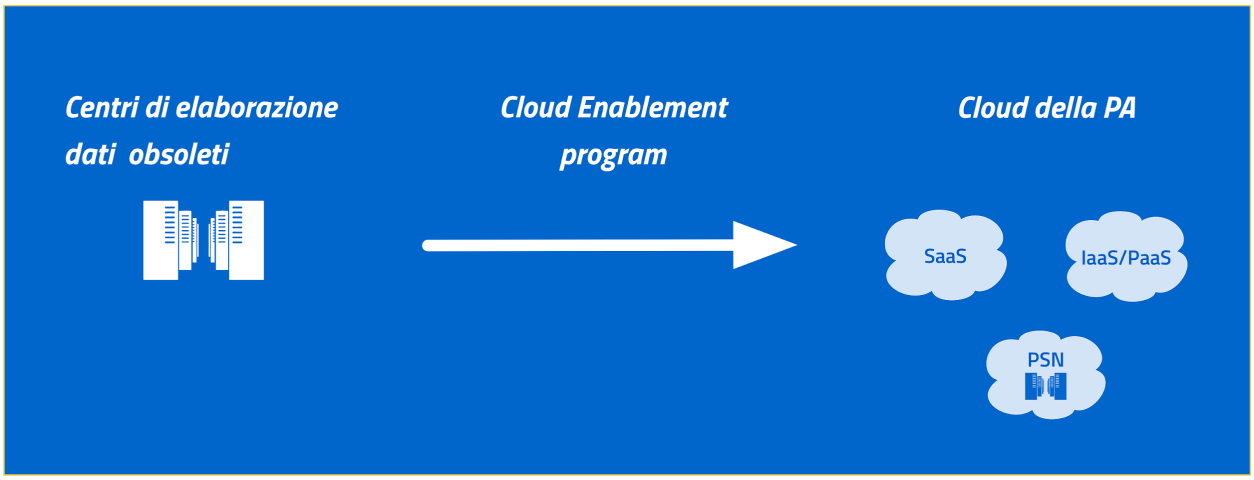

Fig. 4.1: Il Cloud Enablement program trasforma il patrimonio IT obsoleto in servizi

La figura 4.2 riassume i processi e l'uso delle risorse del framework utilizzate nell'ambito del programma di *Cloud Enablement*.

Il framework di lavoro del Cloud Enablement della PA è costituito da due elementi principali: **un'unità di controllo** e diverse **unità di esecuzione**.

L'unità di controllo ha il compito di aggiornare, gestire e monitorare il framework di lavoro e il programma di *Cloud Enablement*. Detta unità è costituita da un team specializzato in attività di abilitazione al cloud (supporto specialistico nella migrazione di applicazioni, data center, etc.) che, insieme ad AgID, al Team Digitale e ai centri di competenze, rappresenta la governance dell'intero progetto.

[23] https://cloud.italia.it/marketplace/

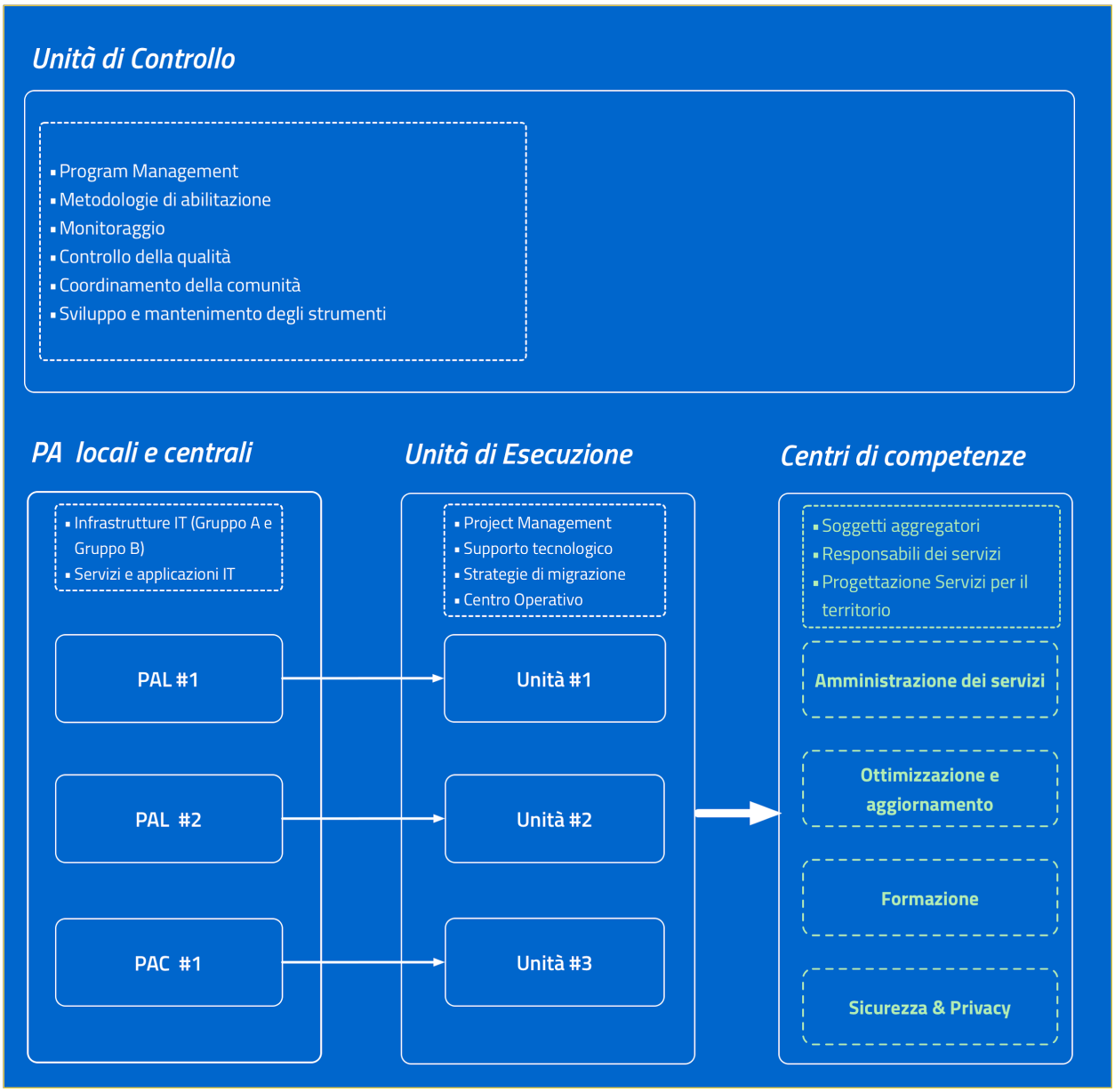

Fig. 4.2: Il Cloud Enablement program trasforma il patrimonio IT obsoleto in servizi

Le principali attività dell'**unità di controllo** sono:

1. **Definizione delle metodologie**: l'unità di controllo definisce e aggiorna le metodologie adottate nell'ambito del *framework* lavoro, in particolare per quanto riguarda il monitoraggio, *l'assessment*, le modalità di consegna e il controllo della qualità.
2. **Sviluppo e mantenimento degli strumenti**: l'unità di controllo è responsabile per la gestione degli strumenti di lavoro nell'ambito del *Framework* di lavoro, si preoccupa di sviluppare, selezionare, mantenere ed aggiornare gli strumenti di lavoro; presta inoltre supporto alle unità di esecuzione affinché gli strumenti vengano utilizzati correttamente.
3. **Program Management**: l'unità di controllo è responsabile della gestione del programma di *Cloud Enablement*, del coordinamento dei progetti e del coordinamento delle unità di esecuzione sul territorio. L'unità di controllo aggiorna il programma di *Cloud Enablement* tenendo in considerazione il *feedback* proveniente dalle unità di esecuzione.
4. **Controllo della qualità**: l'unità di controllo è anche responsabile di verificare la qualità delle consegne (la realizzazione di un progetto di *Cloud Enablement*); al termine di ogni progetto di migrazione dovrà verificare mediante opportuni strumenti (survey, design docs, test, etc) se quanto realizzato risponde ai parametri di qualità previsti dalla metodologia adottata.
5. **Monitoraggio**: l'unità di controllo si preoccupa infine di monitorare l'intero programma in termini di risultati attesi (deliverables) e parametri (KPI); a tale scopo, svilupperà un'infrastruttura di monitoraggio ovvero un'applicazione che da un lato, abilita le PA e le unità di esecuzione ad attivare e monitorare il singolo progetto di migrazione, dall'altro, fornisce una visione complessiva dello stato di avanzamento di tutti i progetti di migrazione in atto.

In questo modello **le unità di esecuzione** sono i soggetti responsabili della progettazione e dell'esecuzione di uno specifico progetto di migrazione cloud. Tali unità sono responsabili per la consegna (delivery), svolgono consulenza sul campo, progettando e implementando, insieme alle PA e/o ai centri di competenze, il percorso di migrazione dei servizi IT.

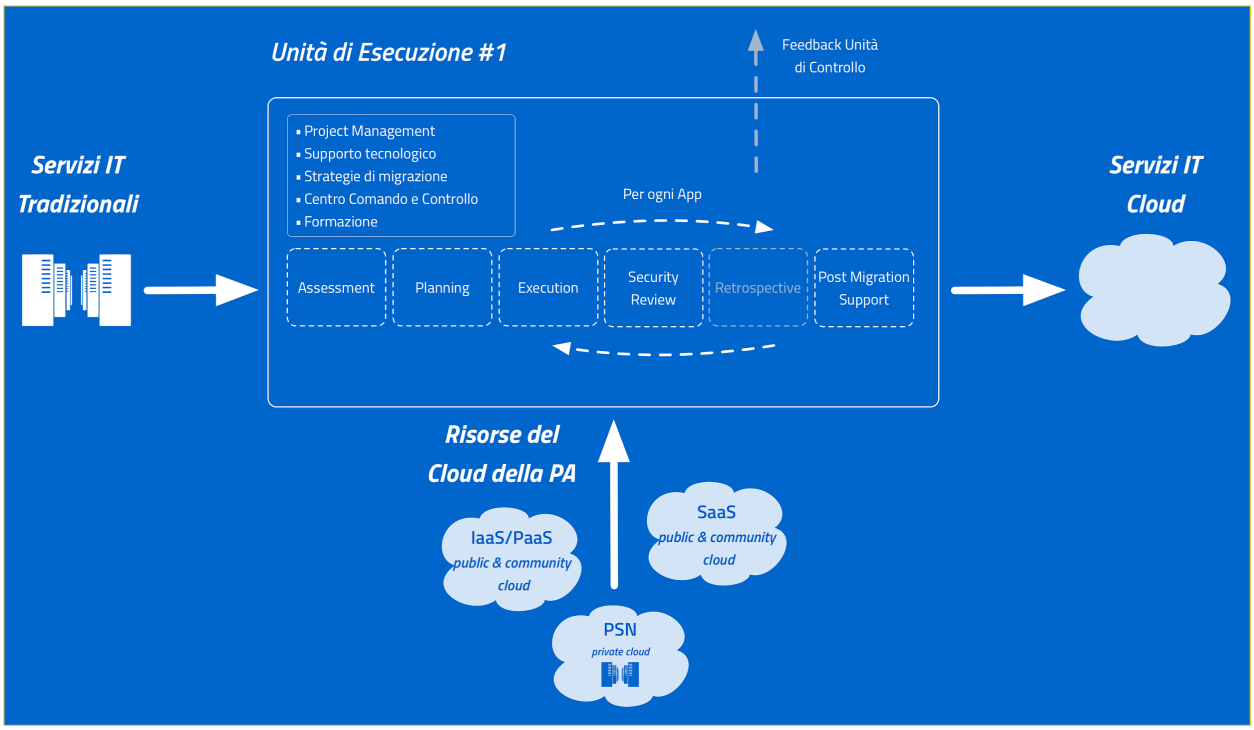

Fig. 4.3: Come opera l'unità di esecuzione nell'ambito del cloud enablement program

Le principali attività dell' **unità di esecuzione** sono:

1. **Assessment iniziale**: assessment infrastrutturale e delle applicazioni utilizzate dalla PA, prestando particolare attenzione ad individuare la criticità di ogni applicazione ed eventuali interdipendenze. Al termine di questa fase iniziale, si ottiene un catalogo delle infrastrutture da dismettere e delle applicazioni da migrare, congiuntamente ad una analisi complessiva dove si evidenziano possibili criticità nella fase di migrazione.
2. **Progettazione del processo di migrazione**: progettazione congiunta alle PA del piano di migrazione individuando le architetture, le strategie di migrazione per le diverse applicazioni, le soluzioni cloud ed infine i tempi di esecuzione. Questa fase produce un piano di lavoro dettagliato che sarà messo in atto nella fase successiva. Il *know how* prodotto durante la progettazione deve essere consolidato dalle unità di esecuzione.
3. **Esecuzione della migrazione**: l'esecuzione della migrazione è la parte operativa di tutto il processo. Mediante le metodologie definite dalle unità di esecuzione, con il supporto dell'unità di controllo, viene eseguito quanto descritto nel piano di migrazione frutto della precedente fase. Viene stabilito un centro di operativo di comando e controllo della migrazione in cui devono essere presenti anche componenti della PA coinvolta. Al termine di questa fase la PA dovrebbe poter disporre dei nuovi servizi IT in ambiente cloud. Questa fase è iterativa, dovrebbe svolgersi per ogni applicazione, in modo che si possa verificare il corretto funzionamento dell'applicazione una volta migrata.
4. **Revisione della sicurezza**: le unità di esecuzione effettuano la revisione della sicurezza applicativa e dell'infrastruttura, indicando le criticità per ogni ambito avvalendosi di soggetti terzi per una migliore e più indipendente analisi del rischio. La revisione prevede l'applicazione delle misure minime di sicurezza ICT per le pubbliche amministrazioni, emanate da AgID. Nell'ambito della *web application security*, è necessario applicare i controlli legati alle vulnerabilità più comuni, menzionate in dettaglio nella classifica TOP 10 del progetto OWASP. La revisione di sicurezza deve essere eseguita sempre prima di considerare conclusa la fase di esecuzione, e viene effettuata in maniera iterativa ogni qual volta il ciclo di esecuzione introduce un nuovo cambiamento.
5. **Retrospettiva post-migrazione e supporto**: al termine della fase di esecuzione, le unità di controllo effettuano un'analisi retrospettiva del processo di migrazione cercando di evidenziare le problematiche emerse nelle attività di progettazione specifiche. Le *lessons learnt*, emerse in questa fase, vengono presentate all'unità di controllo che le consolida in una knowledge base comune.
6. **Formazione**: formazione ai referenti dell'amministrazione sui servizi cloud (IaaS, PaaS, SaaS) e sul loro utilizzo attraverso sessioni di formazione specialistica sulle tematiche del cloud.
7. **Project Management**: le unità di esecuzione sviluppano e coordinano l'esecuzione del progetto di *Cloud Enablement* per le amministrazioni, utilizzando gli strumenti forniti dall'unità di controllo e le risorse cloud acquisite dalle stesse amministrazioni. Le unità di esecuzione insieme alle amministrazioni sono responsabili della gestione e dell'esecuzione del progetto.

4.3 I centri di competenze

Il terzo elemento della strategia di Cloud Enablement è costituito dall'individuazione di specifici **centri di competenze** sul territorio.

Tali centri, supportati da AgiD, hanno lo scopo di consolidare il *know how* e l'esperienza relativa alla gestione dei servizi cloud nella PA.

Inoltre possono svolgere la funzione di **soggetti aggregatori**, amministrando i servizi cloud per conto di altre PA, svolgendo pertanto un ruolo chiave nel modello di sviluppo della trasformazione digitale della PA.

Al termine del processo di trasformazione/migrazione cloud, le attività di aggiornamento, formazione, gestione del cambiamento e ottimizzazione delle risorse cloud, saranno affidate ai centri di competenze.

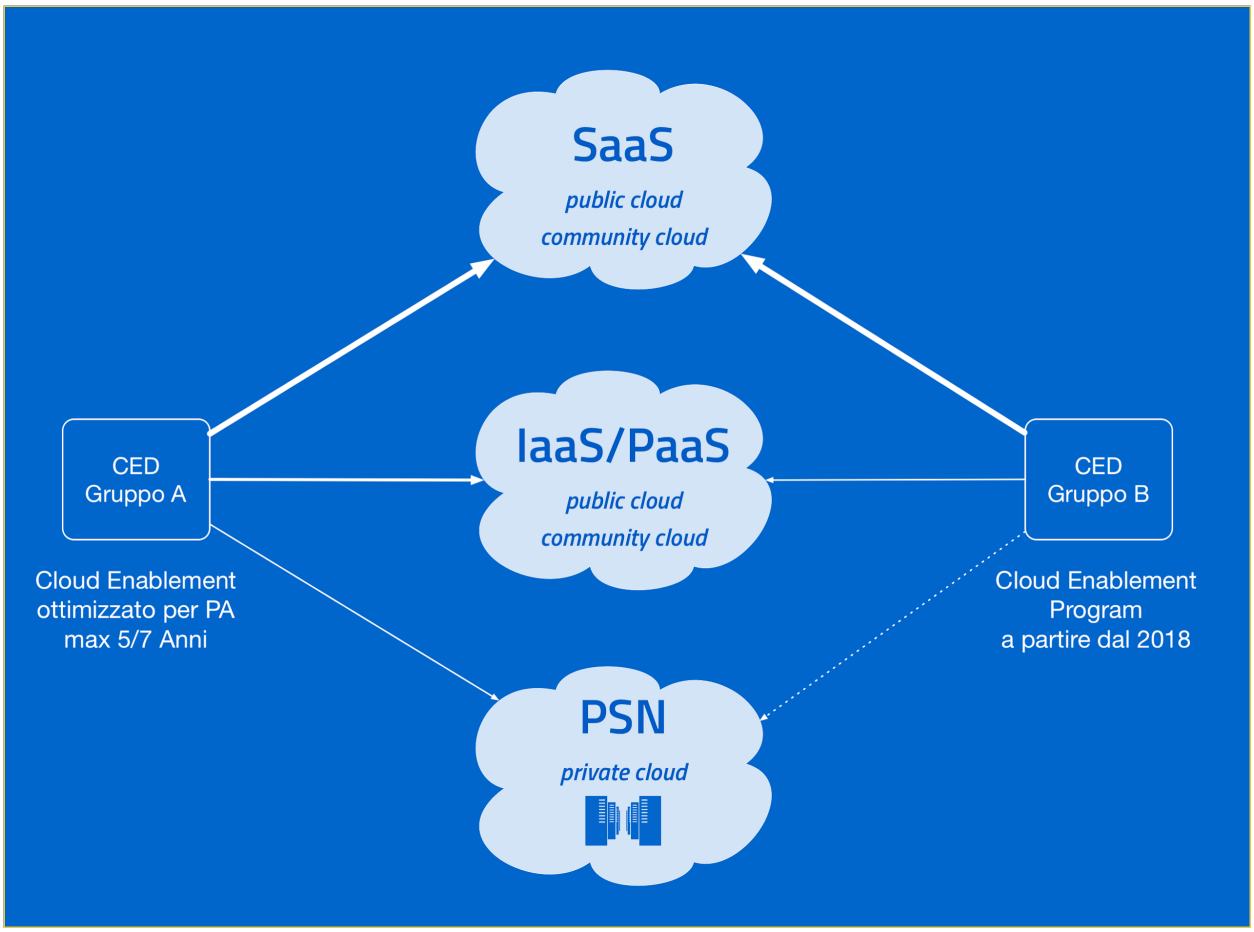

Fig. 4.4: La distribuzione dei servizi IT secondo il modello Cloud della PA

CAPITOLO 5

Riferimenti internazionali

Questo documento è obsoleto

Il riferimento attuale è Strategia Cloud Italia[24].

5.1 Strategia Cloud nei paesi europei

Nel **Regno Unito** è stato lanciato, a partire dal 2011, il Programma G-Cloud, per diffondere l'utilizzo del cloud tramite una serie di accordi quadro, uno store online di servizi cloud ed un'iniziativa di consolidamento dei data center. Gli accordi quadro – finalizzati alla semplificazione della fornitura di servizi cloud alle pubbliche amministrazioni da parte di operatori privati – consentono alle stesse PA di selezionare dallo store i servizi richiesti e concludere accordi di fornitura senza dover completare l'intero iter relativo all'assegnazione di appalti tramite bando pubblico. A fine 2016, gli accordi conclusi tramite lo store avevano superato 1,5 miliardi di sterline, con risparmi stimati in 339 milioni di sterline nel biennio 2016/17. Rispetto al consolidamento dei data center, il censimento ha identificato 220 strutture pubbliche. È attualmente in corso la fase di razionalizzazione, da completarsi entro il 2020, che prevede una riduzione dei costi stimata in circa 300 milioni di sterline all'anno.

UK Government Cloud First policy[25]

UK Government Cloud Strategy[26]

In **Germania** il cloud è uno dei pilastri della strategia di *information and communication technology* del governo federale (2010), lanciata con l'obiettivo di facilitare la diffusione presso le imprese. Tematiche come sicurezza dei dati, qualità del servizio, facilità di integrazione e standard aperti sono state invece inclusi nel *Cloud Computing Action Programme*. Iniziative più recenti quali la *Sharing Government IT – Bundescloud* (2015) hanno previsto il consolidamento applicativo all'interno di un cloud federale ad architettura privata, e il consolidamento operativo delle infrastrutture all'interno di una rete di proprietà pubblica, la *ITZbund*. È stata prevista anche la gestione centralizzata

[24] https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/
[25] https://www.gov.uk/guidance/government-cloud-first-policy
[26] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/266214/government-cloud-strategy_0.pdf

del procurement, coordinato sempre più in modalità digitale, questo tema è stato poi ripreso anche dall'iniziativa *Digital Administration 2020*.

Germany Cloud Computing[27]

In **Francia** è stata creata una *joint venture* Pubblico-Privato, che si chiama Andromede, e di cui fanno parte anche France Telecom-Orange, Thales e Dassault Systèmes. Per la "nuvola" lo Stato francese ha deciso di investire la quota più alta nell'alleanza, 135 milioni di euro, grazie ai quali acquisire una partecipazione del 33% mentre Orange e Dassault hanno investito 60 milioni di euro ciascuna, acquisendo una partecipazione del 26,7%, mentre Thales ha investito 30 milioni per una quota del 13,3%.

Pensata con l'obiettivo di fornire un cloud sicuro e "nazionale" per il settore pubblico e per le imprese, l'iniziativa ha subito numerose interruzioni. A partire dal 2014 è stata sviluppata una piattaforma di cloud interministeriale per fornire IaaS e PaaS per ministeri e amministrazione centrale, utilizzando architetture ibride. La piattaforma utilizzerà cloud privato operato da terzi per i dati sensibili, e cloud pubblico per sviluppi.

A livello nazionale, inoltre, nel 2012 è stato lanciato il progetto RIE (*Réseau interministériel de l'état*), per razionalizzare le varie reti in un'unica infrastruttura capace di collegare tutte le amministrazioni della PA. Attualmente raggiunge più di 11.500 siti e 18 entità ministeriali.

Ad oggi è disponibile una piattaforma di e-government[28] che offre servizi ai cittadini e alla pubblica amministrazione. Ai cittadini la piattaforma web offre informazioni su tasse, lavoro, immobili, mentre offre alle PA un cloud interministeriale con servizi di tipo IaaS, PaaS, SaaS basato su un modello di cloud ibrido.

Service Public[29]

Anche la **Spagna** si è mossa sul versante della diffusione del cloud nella pubblica amministrazione, lanciando nel 2011 l'iniziativa SARA. Il progetto consiste nella creazione di una rete che collega amministrazioni centrali, regionali e locali fornendo servizi di SaaS (Software as a service) e IaaS (Infrastructure as a service) per le amministrazioni locali. L'infrastruttura, nata come architettura privata, verrà convertita progressivamente in cloud ibrido, aggiungendo nodi pubblici ai nodi privati e la fornitura di servizi aperti al pubblico anche in modalità PaaS.

SARA offriva inizialmente soprattutto IaaS e SaaS per comunicazione, reportistica, fatturazione elettronica, resource management, incident management.

L'utilizzo di SARA è però aumentato negli anni con l'aumento del numero di servizi SaaS offerto agli enti e ai cittadini. Attualmente i servizi offerti includono anagrafe, tassazione, residenza, servizi sociali, disoccupazione, catasto ecc., e ne fanno un uso massivo gli Enti Locali. Si stima che a fine 2016 (Fonti OBSAE - 2016) circa il 93% della popolazione usufruisce dei servizi cloud.

Portal de Administración Electrónica[30]

5.2 Strategia cloud negli USA

Per quanto riguarda altri scenari internazionali merita una citazione l'esperienza statunitense (**US Department of Interior**).

> *«The Cloud First Strategy plays a pivotal role in helping the Federal Government close the productivity gap between the public and private sectors.»*

The Cloud First Strategy[31], su iniziativa della stessa Casa Bianca, è stata avviata fin dal 2011. È un insieme di politiche organizzative e linee guida tecnologiche definite per accelerare la crescita del cloud, considerato come la soluzione più efficace per garantire la sicurezza e il valore degli investimenti ICT.

[27] https://gettingthedealthrough.com/area/100/jurisdiction/11/cloud-computing-germany/
[28] https://www.service-public.fr/
[29] https://www.service-public.fr
[30] https://administracionelectronica.gob.es/pae_Home#.WwKYlYiFOUk
[31] https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf

La Pubblica Amministrazione Statunitense ha accelerato sul cloud per i rilevanti risultati economici ottenuti dalle imprese che si sono consolidate intorno a un gruppo molto selezionato di grandi fornitori di cloud, guidando poi il governo a spingere le Agenzie governative verso la medesima direzione.

A fine 2016, dei quasi 10.600 data center delle Agenzie federali esistenti nel 2010, ne sono stati chiusi oltre 3mila. Su 24 agenzie federali, i Dipartimenti di Agricoltura, Difesa, Interno e Tesoro rappresentano l'84% delle chiusure. Diciannove agenzie hanno riferito di aver raggiunto un risparmio di 2,8 miliardi di dollari in termini di costi operativi e di spese in conto capitale tra il 2011 e il 2015, e hanno spostato i carichi di lavoro nel cloud.

The Cloud First Strategy[32]

[32] https://www.doi.gov/cloud/strategy

CAPITOLO 6

Riferimenti normativi con estratti

Questo documento è obsoleto

Il riferimento attuale è Strategia Cloud Italia[33].

In questo paragrafo sono riportati i riferimenti normativi concernenti la spesa ICT e le qualificazioni cloud.

Si riportano di seguito i riferimenti normativi concernenti la spesa ICT.

Legge n. 208/2015 art. 1 comma 512[34]

> *al fine di garantire l'ottimizzazione e la razionalizzazione degli acquisti di beni e servizi informatici e di connettività, fermi restando gli obblighi di acquisizione centralizzata previsti per i beni e servizi dalla normativa vigente, le amministrazioni pubbliche e le società inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1 della legge 31 dicembre 2009, n. 196 provvedono ai propri approvvigionamenti esclusivamente tramite Consip SpA od i soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi soggetti.*

Legge n. 208/2015 art. 1 comma 512[35]

> *Ai fini di cui al comma 512, Consip SpA o il soggetto aggregatore interessato sentita l'AgID per l'acquisizione dei beni e servizi strategici indicati nel Piano triennale per l'informatica nella pubblica amministrazione di cui al comma 513, programma gli acquisti di beni e servizi informatici e di connettività, in coerenza con la domanda aggregata di cui al predetto Piano. AgID, Consip SpA e i soggetti aggregatori, sulla base di analisi delle informazioni in loro possesso relative ai contratti di acquisto di beni e servizi in materia informatica, propongono alle amministrazioni e alle società di cui al comma 512 iniziative e misure, anche organizzative e di processo, volte al contenimento della spesa. Consip SpA e gli altri soggetti aggregatori promuovono l'aggregazione della domanda funzionale all'utilizzo degli strumenti messi a disposizione delle pubbliche amministrazioni su base nazionale, regionale o comune a più amministrazioni.*

[33] https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/
[34] http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2015-12-28;208
[35] http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2015-12-28;208

Legge n. 208/2015 art. 1 comma 512[36]

> *La procedura di cui ai commi 512 e 514 ha un obiettivo di risparmio di spesa annuale, da raggiungere alla fine del triennio 2016-2018, pari al 50 per cento della spesa annuale media per la gestione corrente del solo settore informatico, relativa al triennio 2013-2015, al netto dei canoni per servizi di connettività e della spesa effettuata tramite Consip SpA o i soggetti aggregatori documentata nel Piano triennale di cui al comma 513, nonché tramite la società di cui all'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133. Sono esclusi dal predetto obiettivo di risparmio gli enti disciplinati dalla legge 8 marzo 1989, n. 88, nonché, per le prestazioni e i servizi erogati alle amministrazioni committenti, la società di cui all'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, la società di cui all'articolo 10, comma 12, della legge 8 maggio 1998, n. 146, e la Consip SpA, nonché l'amministrazione della giustizia in relazione alle spese di investimento necessarie al completamento dell'informatizzazione del processo civile e penale negli uffici giudiziari. I risparmi derivanti dall'attuazione del presente comma sono utilizzati dalle medesime amministrazioni prioritariamente per investimenti in materia di innovazione tecnologica.*

Legge n. 208/2015 art. 1 comma 512[37]

> *Le amministrazioni e le società di cui al comma 512 possono procedere ad approvvigionamenti al di fuori delle modalità di cui ai commi 512 e 514 esclusivamente a seguito di apposita autorizzazione motivata dell'organo di vertice amministrativo, qualora il bene o il servizio non sia disponibile o idoneo al soddisfacimento dello specifico fabbisogno dell'amministrazione ovvero in casi di necessità ed urgenza comunque funzionali ad assicurare la continuità della gestione amministrativa. Gli approvvigionamenti effettuati ai sensi del presente comma sono comunicati all'Autorità nazionale anticorruzione e all'AgID.*

Circolare del Mef n. 16 del 17 maggio 2016[38]

> *Si coglie l'occasione per rammentare che i commi da 512 a 520 della legge n. 208/2015 (legge di Stabilità per l'anno 2016) contengono una molteplicità di disposizioni tendenti ad incentivare l'acquisizione centralizzata di beni e servizi in materia informatica e di connettività, prevedendo, al fine di conseguire specifici obiettivi di risparmio nonché l'ottimizzazione e la razionalizzazione del settore, che le Amministrazioni pubbliche e le società inserite nel conto consolidato predisposto dall'ISTAT debbano approvvigionarsi MEF - RGS - Prot. 44712 del 17/05/2016 - U J •, " tramite la Consip o i soggetti aggregatori. E" disposto che solo in casi eccezionali, e con autorizzazione motivata dell'organo di vertice amministrativo, si possa procedere ad acquisti autonomi. E", altresì, prevista l'elaborazione da parte dell'Agenzia per l'Italia digitale (AGID) di un Piano triennale per l'informatica nella pubblica amministrazione. Il comma 515 individua l'obiettivo di risparmio di spesa annuale, da raggiungere alla fine del triennio 2016-2018, in relazione alle norme sull'acquisizione centralizzata di beni e servizi da parte delle Amministrazioni pubbliche in misura pari al 50 per cento della spesa annuale media per la gestione corrente del solo settore informatico relativa al triennio 2013-2015; tale risparmio prevede alcuni limitate deroghe, escludendo, tra l'altro, dall'applicazione delle disposizioni in questione l'Amministrazione della Giustizia con esclusivo riferimento alle spese di investimento necessarie al completamento dell'informatizzazione del processo civile e penale. A tal proposito occorre precisare il risparmio di spesa annuale nella misura indicata dal citato comma 515 è da conseguire come media nel triennio 2016-2018: in altre parole il risparmio può essere conseguito, ad esempio, interamente in un solo anno oppure ripartito nel triennio in modo uniforme o con diversa modalità, purché venga rispettato l'obiettivo complessivo in media annuale, da valutare in sede di consuntivo per l'anno finanziario 2018. Per l'attuazione delle disposizioni di cui ai commi da 512 a 520, le Amministrazioni pubbliche operano nel rispetto di quanto stabilito nel piano triennale per l'informatica e nelle linee guida emanate dall'AGID.*

Circolare AgID n.02/2016 - 4. Disposizioni per l'anno 2016[39]

[36] http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2015-12-28;208
[37] http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2015-12-28;208
[38] http://www.rgs.mef.gov.it/VERSIONE-I/circolari/2016/circolare_n_16_2016/
[39] https://www.agid.gov.it/sites/default/files/repository_files/documentazione/circolare_piano_triennale_24.6.2016._def.pdf

le pubbliche amministrazioni non possono effettuare acquisti di beni e servizi informatici, anche se per innovazione, qualora siano in contrasto con i principi generali definiti nel paragrafo 3. In particolare non potranno essere sostenute spese relative alla costituzione di nuovi data center. [. . .]

c) Per procedere ad acquisizioni di beni e servizi informatici e di connettività, ai sensi del comma 512, che fa salvi "gli obblighi di acquisizione centralizzata previsti per i beni e servizi dalla normativa vigente", le amministrazioni pubbliche e le società del conto economico consolidato ISTAT devono preliminarmente verificare se sussistono per l'acquisto in questione obblighi di acquisizione centralizzata e, cioè, strumenti di acquisto e strumenti di negoziazione centralizzata; in particolare, andrà verificata la sussistenza dell'obbligo di ricorso alle convenzioni Consip (di cui all'articolo 1, comma 449, della l. 296/2006); l'obbligo di ricorso al Mercato elettronico della pubblica amministrazione (di cui all'articolo 1, comma 450, della l. 296/2006); l'obbligo di ricorso ad accordi quadro e gare su delega individuati con decreto ministeriale (ai sensi dell'articolo 2, comma 574, della l. 244/2007); l'obbligo di ricorso a strumenti di acquisto e negoziazione telematici messi a disposizione da Consip o dalle centrali di committenza regionali di riferimento (di cui all'articolo 15, comma 13, lett. d), decreto .legge. 95/2012).

d) Qualora le amministrazioni non siano tenute a ricorrere a specifici strumenti di acquisto e negoziazione ai sensi delle disposizioni richiamate al punto precedente, la disposizione di cui al comma 512 richiede di ricorrere agli strumenti di acquisto e di negoziazione disponibili presso Consip ed i soggetti aggregatori. Fra i detti strumenti sono ricompresi le convenzioni-quadro, i contratti-quadro e gli accordi-quadro nonché il mercato elettronico della pubblica amministrazione, il sistema dinamico della pubblica amministrazione e le gare su delega che aggregano la domanda di più amministrazioni.

e) Pertanto le amministrazioni e le società inserite nel conto consolidato ISTAT possono effettuare acquisti di beni e servizi informatici in via autonoma solo dopo aver verificato che non siano disponibili strumenti di aggregazione, attraverso la consultazione delle apposite pagine web (www.consip.it, www.acquistinretepa.it, nonché la sezione "soggetti aggregatori"). Ogni qual volta le amministrazioni e le società di cui al comma 512 non possano ricorrere ai detti strumenti a causa dell'indisponibilità del bene/servizio o della sua inidoneità al soddisfacimento del fabbisogno ovvero nei casi di necessità ed urgenza comunque funzionali per assicurare la continuità della gestione amministrativa, esse potranno procedere ad acquisti autonomi soltanto previa autorizzazione motivata dell'organo di vertice amministrativo. Si ritiene che tale autorizzazione debba essere resa al momento dell'avvio della procedura di affidamento e, dunque, al momento dell'adozione della determina a contrarre. In tale momento andrà, pertanto, valutata la disponibilità o la compatibilità delle tempistiche preventivate da Consip e dai soggetti aggregatori per la messa a disposizione del bene/servizio rispetto ai fabbisogni della stazione appaltante, oltre ovviamente alla idoneità del bene/servizio. Le pubbliche amministrazioni, nell'ambito degli acquisti di beni e servizi informatici di cui al punto precedente, devono comunque adottare gli standard vigenti.

Piano triennale per l'informatica 2017-2019 - Data center e cloud - Linee di azione[40]

Le pubbliche amministrazioni non possono procedere all'acquisto di nuovi data center. Sono consentiti solo adeguamenti dei data center già in uso presso la pa, previa approvazione da parte di AgID, esclusivamente al fine di: evitare problemi di interruzione di pubblico servizio; anticipare processi di dismissione dei propri data center per migrare al Cloud della PA e consolidare i propri servizi su data center di altre PA al fine di ottenere economie di spesa.

Circolare AgID n.05/2017[41]

Si specifica altresì che, ai sensi della Circolare AgID 24 giugno 2016, n. 2, come richiamata dal Piano Triennale (cfr. Paragrafo 3.1.3. Linee di azione- azione 1), in materia di spesa le PA non possono effettuare spese o investimenti in materia di Data center, ma – previa approvazione di AgID – possono procedere agli adeguamenti dei propri Data center esclusivamente al fine di:

- *evitare problemi di interruzione di pubblico servizio (inclusi gli interventi necessari a garantire la sicurezza dei dati e dei sistemi, in applicazione delle regole AgID Basic Security Controls);*

[40] https://pianotriennale-ict.readthedocs.io/it/latest/doc/03_infrastrutture-fisiche.html#linee-di-azione
[41] https://censimentoict.italia.it/it/latest/docs/circolari/2017113005.html

- *anticipare processi di dismissione dei propri Data center per migrare al Cloud della PA;*
- *consolidare i propri servizi sui Data center di altre PA per ottenere economie di spesa.*

[....] Sono esclusi dalla richiesta di approvazione gli adeguamenti che prevedono acquisti nei seguenti ambiti: progetti di ricerca a titolarità di istituzioni universitarie e/o enti di ricerca; sistemi a supporto della diagnostica clinica.

Si riportano i riferimenti normativi concernenti la qualificazione dei servizi SaaS e CSP Circolari dell'Agenzia per l'Italia Digitale n. 2 del 09 aprile 2018 e n. 3 del 09 aprile 2018[42]

[42] https://cloud.italia.it/it/latest/

CAPITOLO 7

Domande frequenti

Questo documento è obsoleto

Il riferimento attuale è Strategia Cloud Italia[43].

7.1 Censimento del patrimonio ICT della PA e PSN

A cosa serve il Censimento del Patrimonio ICT della PA avviato da AgID?

Il Censimento del Patrimonio ICT della PA serve a costruire una base informativa comune sui principali asset IT (infrastrutture, hardware e software) utilizzati dalle pubbliche amministrazioni. Le informazioni raccolte sono utili per aiutare le amministrazioni a valorizzare il proprio patrimonio ICT e a razionalizzare la spesa ICT. Il censimento si è concluso il 20 Giugno 2018.

In base al censimento, come vengono classificate le infrastrutture IT delle amministrazioni?

Secondo quanto previsto dal Piano triennale, le infrastrutture IT delle amministrazioni vengono classificate in una delle seguenti categorie: gruppo A, gruppo B e strutture candidabili a Polo Strategico Nazionale (PSN). Nel gruppo A rientrano le infrastrutture IT delle amministrazioni che possiedono data center che, pur avendo carenze strutturali, svolgono un ruolo critico e non possono essere dismesse nel breve periodo, nel gruppo B quelle con data center che non garantiscono i minimi requisiti di affidabilità e sicurezza e che devono dismettere tali data center quanto prima, mentre nel gruppo dei candidabili a Poli Strategici Nazionali rientrano quelle amministrazioni dotate di infrastrutture ICT di qualità, che potranno essere prese in considerazione nella costituzione dei Poli Strategici Nazionali.

Durante il periodo di esecuzione del Piano triennale, le PA possono effettuare investimenti sui data center?

No, non potranno effettuare nuove spese e investimenti in hardware e infrastrutture, ma potranno effettuare spese/investimenti per realizzare progetti di consolidamento e virtualizzazione per migrare i propri servizi verso le infrastrutture del Cloud delle PA esistenti ad oggi (Catalogo dei servizi Cloud per la PA qualificati[44]).

Le pubbliche amministrazioni come possono partecipare al censimento?

[43] https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/
[44] https://cloud.italia.it/marketplace/

Il Censimento ICT[45] è chiuso.

Che succede se un'amministrazione non partecipa al questionario o lo compila solo parzialmente?

Le infrastrutture IT delle amministrazioni che non completano il questionario entro i termini stabiliti, vengono classificate d'ufficio nel gruppo B.

Come viene individuato un Polo Strategico Nazionale?

In seguito al censimento, le amministrazioni risultate "candidabili" come Poli Strategici Nazionali potranno presentare formale candidatura per svolgere tale ruolo. AgID, in seguito alla ricezione della candidatura, avvia l'istruttoria per la qualificazione a PSN. In caso di esito positivo, il Governo elegge mediante specifico provvedimento e a seguito di una propria valutazione in merito all'interesse nazionale per la costituzione del Polo Strategico Nazionale.

Quale sarà il compito dei Poli Strategici Nazionali?

I PSN gestiranno l'infrastruttura IT (Data Center e Cloud) del Paese con specifiche caratteristiche di affidabilità e sicurezza definite da AgID.

Tali infrastrutture ospitano le applicazioni che supportano l'erogazione di servizi al cittadino, di particolare rilevanza strategica e di interesse nazionale.

7.2 Circolare qualificazione Cloud Service Provider

Quali sono i servizi che i Cloud service provider possono offrire alle PA?

Le tre categorie di servizi cloud IaaS, PaaS e SaaS purchè qualificati da AgID.

Quali requisiti organizzativi deve avere un Cloud service provider per ottenere la qualifica di AgID?

I requisiti organizzativi sono pubblicati all'interno dell'Allegato A della Circolare AgID n. 2 del 9 aprile[46].

Quali requisiti specifici di sicurezza deve avere un Cloud service provider per ottenere la qualifica di AgID?

I requisiti specifici di sicurezza sono pubblicati all'interno dell'Allegato A della Circolare AgID n. 2 del 9 aprile[47].

Quali requisiti specifici di performance deve avere un Cloud service provider per ottenere la qualifica di AgID?

I requisiti specifici di performance sono pubblicati all'interno dell'Allegato A della Circolare AgID n. 2 del 9 aprile[48].

Quali requisiti di interoperabilità e portabilità deve avere un Cloud service provider per ottenere la qualifica di AgID?

I requisiti di interoperabilità e portabilità sono pubblicati all'interno dell'Allegato A della Circolare AgID n. 2 del 9 aprile[49].

Cosa bisogna fare per chiedere la qualificazione come Cloud service provider (CSP)?

Per chiedere la qualificazione occorre seguire i passaggi indicati nella piattaforma dedicata alle qualificazioni cloud[50].

Per quanto tempo è valida la qualificazione di fornitore di Public Cloud della PA?

La qualificazione ha durata pari a 24 mesi a decorrere dalla data di iscrizione al Marketplace Cloud, salvo i casi di revoca previsti.

In quali casi AgID può revocare la qualificazione al Cloud service provider?

[45] https://censimentoict.italia.it/it/latest/
[46] https://cloud.italia.it/projects/cloud-italia-circolari/it/latest/circolari/CSP/allegato_docs/requisiti-organizzativi.html
[47] https://cloud.italia.it/projects/cloud-italia-circolari/it/latest/circolari/CSP/allegato_docs/requisiti-specifici.html#sicurezza-privacy-e-protezione-dei-dati
[48] https://cloud.italia.it/projects/cloud-italia-circolari/it/latest/circolari/CSP/allegato_docs/requisiti-specifici.html#performance
[49] https://cloud.italia.it/projects/cloud-italia-circolari/it/latest/circolari/CSP/allegato_docs/requisiti-specifici.html#interoperabilita-e-portabilita
[50] https://cloud.italia.it/marketplace/info

AgID revoca la qualificazione nel caso di:

- perdita di almeno uno dei requisiti di cui all'Allegato A della Circolare AgID 2 del 9 aprile;
- riscontro da parte dei competenti organi di violazioni di norme relative
- all'attività oggetto di qualificazione.

In caso di revoca, il CSP può presentare una nuova richiesta di qualificazione all'AgID?

Sì, ma solo nel caso in cui siano venute meno le cause che hanno determinato la revoca della qualificazione.

Nel caso in cui il CSP abbia data center dislocati in Stati esteri ne dovrà dare comunicazione?

Sì, dovrà farlo per consentire all'acquirente di venire a conoscenza e valutare potenziali incompatibilità o restrizioni legislative dello Stato estero in questione. Il fornitore Cloud deve rendere noti i paesi in cui sono dislocati i data center tramite i quali verrà erogato anche parzialmente il servizio e/o all'interno dei quali transiteranno anche temporaneamente i dati.

Una pubblica amministrazione può usare prodotti IaaS o PaaS quali: Google Cloud, Azure, ecc. ? Un'amministrazione può accedere liberamente ad un qualunque servizio IaaS e/o PaaS erogato da soggetti pubblici o privati (fermo restando la compliance con la normativa vigente, come per esempio il GDPR). A partire dal 20 Novembre 2018 le amministrazioni potranno acquisire esclusivamente servizi Cloud IaaS e PaaS erogati da Cloud Service Provider qualificati secondo quanto disposto da AgID nella circolare N. 2 del 9 aprile 2018[51], tale procedura consentirà ai fornitori di servizi di certificare i servizi stessi per l'uso nella PA.

7.3 Circolare qualificazione dei servizi SaaS

Chi può fornire servizi Cloud di tipo Software as a Service (SaaS) alla PA?

Sia i fornitori privati, sia le pubbliche amministrazioni purchè qualificati da AgID.

Quali sono i requisiti di ammissibilità per poter chiedere la qualificazione come fornitore di soluzioni SaaS alla PA?

I servizi SaaS proposti dal fornitore devono essere compatibili con almeno una delle infrastrutture tra Cloud SPC Lotto 1 e/o Cloud service provider qualificato da AgID.

Cosa bisogna fare per chiedere la qualificazione come fornitore di soluzioni SaaS alla PA?

Per chiedere la qualificazione seguire i passaggi indicati nella piattaforma dedicata alla qualificazione nell'apposita sezione su cloud.italia.it[52].

In quali casi AgID può revocare la qualificazione al fornitore SaaS?

Nel caso di:

- perdita del criterio di ammissibilità. Ovvero quando l'infrastruttura che ospita il servizio SaaS non è più qualificata;
- perdita di almeno uno dei requisiti di cui all'Allegato A della Circolare
- AgID 3 del 9 aprile;
- riscontro da parte dei competenti organi di violazioni di norme relative
- all'attività oggetto di qualificazione.

[51] https://cloud.italia.it/projects/cloud-italia-circolari/it/latest/circolari/CSP/circolare_qualificazione_CSP_v1.2.html
[52] https://cloud.italia.it/marketplace/

Quali requisiti organizzativi deve avere un fornitore SaaS per ottenere la qualificazione di AgID?

I requisiti organizzativi sono pubblicati all'interno dell'Allegato A della Circolare AgID n. 3 del 9 aprile[53].

Quali requisiti di sicurezza deve possedere un fornitore SaaS per ottenere la qualificazione di AgID rispetto alle soluzioni SaaS offerte?

I requisiti di sicurezza sono pubblicati all'interno dell'Allegato A della Circolare AgID n. 3 del 9 aprile[54].

Quali sono i requisiti di performance e scalabilità che un fornitore SaaS deve avere per ottenere la qualificazione?

I requisiti di performance e scalabilità sono pubblicati all'interno dell'Allegato A della Circolare AgID n. 3 del 9 aprile[55].

Quali sono i requisiti di interoperabilità e portabilità che un fornitore SaaS deve avere per ottenere la qualificazione?

I requisiti di interoperabilità e portabilità sono pubblicati all'interno dell'Allegato A della Circolare AgID n. 3 del 9 aprile[56].

Una pubblica amministrazione può usare prodotti SaaS quali: Google Docs, Trello, Github, ecc. ? Un'amministrazione può accedere liberamente ad un qualunque servizio SaaS (fermo restando la compliance con la normativa vigente, come per esempio il GDPR). A partire dal 1 Aprile 2019 le amministrazioni potranno acquisire esclusivamente servizi Cloud SaaS qualificati secondo quanto disposto da AgID nella circolare N. 3 del 9 aprile 2018[57], tale procedura consentirà ai fornitori di servizi di certificare i servizi stessi per l'uso nella PA.

[53] https://cloud.italia.it/projects/cloud-italia-circolari/it/latest/circolari/SaaS/allegato_docs/requisiti-organizzativi.html
[54] https://cloud.italia.it/projects/cloud-italia-circolari/it/latest/circolari/SaaS/allegato_docs/sicurezza.html
[55] https://cloud.italia.it/projects/cloud-italia-circolari/it/latest/circolari/SaaS/allegato_docs/performance-scalabilita.html
[56] https://cloud.italia.it/projects/cloud-italia-circolari/it/latest/circolari/SaaS/allegato_docs/interoperabilita-portabilita.html
[57] https://cloud.italia.it/projects/cloud-italia-circolari/it/latest/circolari/SaaS/circolare_qualificazione_SaaS_v_4.12.27.html