Cloud PA

Release 20180409

09 apr 2018

Indice

Il progetto per il Cloud della Pubblica Amministrazione («Cloud della PA») dà attuazione a quanto previsto dal Piano Triennale per l'informatica nella Pubblica amministrazione 2017- 2019 in merito all'uso di infrastrutture e servizi di cloud computing all'interno della Pubblica Amministrazione.

Nota: *La consultazione pubblica per le circolari AgID riguardanti la qualificazione del Cloud della PA si è conclusa in data 1 Marzo 2018.*

Questo documento raccoglie le circolari relative al progetto *Cloud* della PA, integrate con i suggerimenti raccolti durate la fase di consultazione pubblica e rese pubbliche da AgID in data 09 Aprile 2018. È possibile consultare la versione iniziale sottoposta alla fase di consultazione e i relativi commenti selezionando la versione **v18.0301** (Versione del 01/03/2018) dal menù a sinistra.

Nota: Questo documento viene pubblicato su Docs Italia utilizzando la versione 2.0 del tema di stile Sphinx Italia, ancora in fase beta. Il tema offre nuove funzionalità alla piattaforma Docs Italia e permette una completa integrazione con Forum Italia per commentare i documenti. È possibile lasciare commenti o feedback riguardo a questo cambiamento nel Forum o nel repository docs-italia-theme.

CAPITOLO 1

Servizi SaaS

CIRCOLARE N. 3 del 9 aprile 2018

1.1 Criteri per la qualificazione di servizi SaaS per il Cloud della PA[1]

1.1.1 Premessa

La presente Circolare e i relativi allegati definiscono, in attuazione a quanto previsto nel "Piano Triennale per l'informatica nella Pubblica Amministrazione 2017 - 2019", approvato con DPCM del 31 maggio 2017, i requisiti di qualificazione dei servizi SaaS erogabili sul *Cloud della PA,* nonché la relativa procedura di qualificazione. Il possesso dei predetti requisiti è presupposto per l'inserimento dei servizi SaaS nel Marketplace Cloud.

Ai sensi del Piano Triennale, gli obiettivi strategici nell'ambito della razionalizzazione delle infrastrutture fisiche sono costituiti da:

1. aumento della qualità dei servizi offerti in termini di sicurezza, resilienza, efficienza energetica e continuità di servizio;
2. realizzazione di un ambiente cloud della PA, riqualificando le risorse interne alla PA già esistenti o facendo ricorso a risorse di soggetti esterni qualificati;
3. risparmio di spesa derivante dal consolidamento dei data center e migrazione dei servizi verso tecnologie cloud.

Per il raggiungimento di tali obiettivi, AgID ha previsto, tra le altre attività, una specifica procedura di qualificazione dei servizi SaaS nell'ambito della strategia di evoluzione del modello *Cloud della PA*.

Tale procedura consentirà alle Amministrazioni di utilizzare, nell'ambito del *Cloud della PA*, servizi SaaS conformi ad un insieme di requisiti comuni definiti dalla presente Circolare.

[1] Per "Cloud della PA" ai fini della presente circolare, dei suoi allegati e delle successive integrazioni e/o modifiche si intende: "l'insieme delle infrastrutture e servizi IaaS/PaaS erogati da Cloud SPC, dai PSN e dagli altri CSP che saranno qualificati ai sensi di quanto disposto dal Piano Triennale".

1.1.2 Definizioni

Termine o abbreviazione	Descrizione
AgID, Agenzia	Agenzia per l'Italia Digitale
Codice, Codice dell'Amministrazione Digitale, CAD	Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i.
Pubbliche amministrazioni/Amministrazioni/PA	Le Amministrazioni, come meglio definite all'art. 2, comma 2 del Codice dell'Amministrazione Digitale.
Fornitore	Soggetto economico che opera nel mercato della fornitura e/o distribuzione di servizi SaaS o PA interessata ad erogare servizi SaaS ad altre Amministrazioni
Cloud della PA	Il Cloud della PA è composto dalle infrastrutture e servizi IaaS/PaaS erogati da Cloud SPC, dai PSN e dagli altri CSP qualificati ai sensi della circolare "Criteri per la qualificazione dei Cloud Service Provider della PA"
Cloud	Insieme di infrastrutture tecnologiche remote utilizzate come risorsa virtuale per la memorizzazione e/o l'elaborazione nell'ambito di un servizio
Cloud SPC o SPC Cloud	Contratto Quadro stipulato da CONSIP con il RTI aggiudicatario della Gara SPC Cloud Lotto 1 (https://www.cloudspc.it/)
CSP	Cloud Service Provider, ovvero fornitore di servizi erogati in modalità Cloud
Giorni	Giorni solari
Marketplace Cloud	Piattaforma digitale che espone il catalogo dei servizi SaaS qualificati ai sensi della presente Circolare, nonchè i servizi IaaS e PaaS offerti dai CSP qualificati da AgID ai sensi della circolare "Criteri per la qualificazione dei Cloud Service Provider per la PA"
PSN	Soggetto titolare dell'insieme di infrastrutture IT (centralizzate o distribuite), ad alta disponibilità, di proprietà pubblica, eletto a Polo Strategico Nazionale dalla Presidenza del Consiglio dei Ministri, e qualificato da AgID ad erogare ad altre amministrazioni, in maniera continuativa e sistematica, servizi infrastrutturali on-demand, servizi di disaster recovery e business continuity, servizi di gestione della sicurezza IT ed assistenza ai fruitori dei servizi erogati
Software as a Service/SaaS	Tra i modelli di servizio offerti dalle piattaforme di Cloud computing, il Software as a Service (SaaS) identifica la classe di servizi fully-managed in cui il gestore del servizio (CSP) si occupa della predisposizione, configurazione, messa in esercizio e manutenzione dello stesso (utilizzando un'infrastruttura cloud propria o di terzi), lasciando al fruitore del servizio (PA) ilsolo ruolo di utilizzatore delle funzionalità offerte
SPID	Sistema Pubblico d'Identità Digitale, ovvero la soluzione che permette di accedere a tutti i servizi online della Pubblica Amministrazione e di privati federati con un'unica Identità Digitale (username e password) utilizzabile da computer, tablet e smartphone (http://www.spid.gov.it).
SLI	Service Level Indicator, una misura quantitativa definita di un determinato aspetto della qualità del servizio (ad es. numero di richieste al secondo, latency, throughput, availability, etc.)

1.1.3 Articolo 1 - Oggetto ed ambito di applicazione

La presente circolare definisce i requisiti e la procedura per la qualificazione dei servizi SaaS. Le disposizioni ivi contenute si applicano sia ai fornitori interessati ad offrire servizi SaaS alle PA, sia alle amministrazioni che intendono acquisire servizi SaaS.

In particolare come previsto dal Piano Triennale per l'informatica nella PA 2017 - 2019, con riferimento alle acquisizioni tramite Consip di servizi SaaS qualificati da AgID, si rimanda al documento "Disposizioni per il procurement dei servizi SaaS per il Cloud della PA" pubblicato da Consip e riportato nell'allegato "B" alla presente Circolare.

1.1.4 Articolo 2 – Il processo di qualificazione

Il soggetto richiedente può essere:

1. un fornitore privato di servizi SaaS che intende erogare tali servizi su una o più infrastrutture del *Cloud della PA*; il fornitore di servizi SaaS può essere esso stesso un CSP qualificato;
2. una PA che intende erogare servizi SaaS su una o più infrastrutture del *Cloud della PA*.

Il processo di qualificazione è articolato in tre fasi:

1. Richiesta di qualificazione
2. Conseguimento della qualificazione
3. Mantenimento della qualificazione *(Monitoraggio)*

Nella tabella seguente sono riportati i principali attori coinvolti nel processo di qualificazione ed il loro ruolo in termini di responsabilità (RACI) per ognuna delle fasi.

N.	Fasi del processo di qualificazione	Fornitore	AgID	PA acquirente
1	Richiesta di qualificazione	A, R	I	O
2	Conseguimento della qualificazione	I	A, R	O
3	Mantenimento della qualificazione (Monitoraggio)	C	A, R	R

```
R= Responsible:  è colui che esegue le attività della fase
A= Accountable: è colui che è responsabile del risultato della fase
C= Consulted: è colui che deve essere consultato prima di una decisione
I= Informed:  è colui che  deve essere informato relativamente ad una decisione presa
O= Out of the loop: è colui che non partecipa nel contesto della fase
```

A supporto del processo di qualificazione è previsto l'utilizzo di una piattaforma AgID dedicata ed integrata con il Marketplace Cloud. Tale piattaforma consentirà, tra l'altro, l'accesso tramite SPID e la trasmissione telematica dei documenti ai sensi degli art. 45 e 65 comma 1/b del CAD secondo le modalità operative che saranno pubblicate sul sito https://cloud.italia.it.

1.1.5 Articolo 3 - Criterio di ammissibilità

Al momento della richiesta di qualificazione, i servizi SaaS proposti per la qualificazione devono essere erogati mediante una o più infrastrutture del *Cloud della PA* (PSN, Cloud SPC o CSP qualificato da AgID). Nel caso in cui l'infrastruttura Cloud sia privata e di proprietà del fornitore SaaS, tale infrastruttura deve essere qualificata come CSP da AgID ai sensi di quanto disposto dalla circolare "Criteri per la qualificazione dei Cloud Service Provider per la PA".

1.1.6 Articolo 4 - Requisiti per la qualificazione

Sulla base degli obiettivi definiti nel Piano Triennale, AgID ha individuato i requisiti per la qualificazione dei servizi SaaS, suddividendoli in:

1. Requisiti organizzativi;
2. Requisiti specifici.

Il dettaglio di tali requisiti è fornito all'interno dell'allegato "A" alla presente Circolare, denominato "*Requisiti per la qualificazione dei servizi SaaS per il Cloud della PA*".

AgID si riserva la facoltà di modificare/aggiornare/integrare tali requisiti sulla base dell'evoluzione del contesto e delle tecnologie.

1.1.7 Articolo 5 - Fasi del processo di qualificazione.

Fase 1 - Richiesta di qualificazione

Il fornitore interessato alla qualificazione dei servizi SaaS provvede a trasmettere tramite la *piattaforma AgID dedicata* apposita richiesta, fornendo le informazioni e la documentazione in lingua italiana relative al possesso dei requisiti di cui all'allegato "A" alla presente Circolare. Per l'eventuale documentazione d'accompagnamento presentata in lingua straniera dovrà essere allegata idonea traduzione, anche per estratto.Nel caso in cui un fornitore non abbia alcuna rappresentanza diretta o indiretta in Italia, Agid su segnalazione di un'amministrazione proponente, acquisisce le informazioni necessarie alla qualificazione e potrà avviare d'ufficio la procedura mediante la piattaforma Agid dedicata alla qualificazione, secondo le modalità pubblicate sul sito Cloud Italia all'indirizzo: https://cloud.italia.it/

Fase 2 - Conseguimento della qualificazione

Il conseguimento della qualificazione SaaS coincide con la corretta acquisizione tramite la *piattaforma AgID dedicata* della richiesta di qualificazione. L'Agenzia di riserva di effettuare le verifiche necessarie di cui alla fase successiva. I servizi SaaS qualificati da AgID sono inseriti nel Marketplace Cloud.

Fase 3 – Mantenimento della qualificazione

L'Agenzia potrà verificare in ogni momento il possesso dei criteri di ammissibilità e dei requisiti previsti per la qualificazione di ogni servizio SaaS qualificato. Le verifiche potranno essere avviate anche sulla base di segnalazioni formali indirizzate all'Agenzia da parte dell'Amministrazione cliente/utente del servizio SaaS qualificato. L'Agenzia si riserva la facoltà di avvalersi di soggetti terzi per l'espletamento delle attività di verifica. Al fine del mantenimento della qualifica, il soggetto richiedente si impegna a comunicare tempestivamente all'Agenzia, tramite la piattaforma dedicata, ogni evento che modifichi il rispetto dei requisiti di cui all'allegato "A" alla presente Circolare. La perdita del possesso del/i criterio/i di ammissibilità e/o di almeno uno dei requisiti di cui all'allegato A, comporta la revoca della qualificazione, ai sensi del successivo articolo 6. Qualora durante le attività di verifica dovessero emergere elementi relativi a possibili violazioni della normativa sulla privacy, l'Agenzia ne informa tempestivamente il Garante per la protezione dei dati personali.

1.1.8 Articolo 6 - Revoca della qualificazione

L'Agenzia nel caso di:

- perdita del criterio di ammissibilità;
- perdita di almeno uno dei requisiti di cui all'Allegato A;

- riscontro da parte dei competenti organi di violazioni di norme relative all'attività oggetto di qualificazione;

comunica al fornitore il preavviso di revoca della qualificazione del servizio con previsione di un termine per le eventuali controdeduzioni. Nel caso di infruttuoso esperimento del termine o mancato accoglimento delle controdeduzioni presentate, l'Agenzia procede alla revoca della qualificazione del servizio con provvedimento motivato, disponendone la contestuale eliminazione dal Marketplace Cloud, nonchè relativa pubblicità.

Nei casi di revoca della qualificazione SaaS, il fornitore non può presentare una nuova richiesta di qualificazione all'Agenzia se non siano venute meno le cause che hanno determinato la revoca.

1.1.9 Articolo 7 – Durata della qualificazione dei servizi SaaS.

Salvo i casi di revoca, la qualificazione dei servizi SaaS ha durata pari a 24 mesi a decorrere dalla data di iscrizione al Marketplace Cloud.

1.1.10 Articolo 8 - Disposizioni transitorie

Nelle more dell'attivazione della piattaforma dedicata la richiesta di qualificazione potrà essere sottomessa mediante le modalità pubblicate sul sito https://cloud.italia.it

Nelle more dell'attivazione del Marketplace Cloud l'elenco dei servizi SaaS qualificati sarà pubblicato sul sito https://cloud.italia.it

1.1.11 Articolo 9 - Disposizioni finali

La presente Circolare entra in vigore a partire da 30 giorni dalla data di pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

A decorrere da sei mesi dall'entrata in vigore della presente Circolare, le Amministrazioni acquisiscono esclusivamente servizi SaaS qualificati dall'Agenzia e pubblicati sul Marketplace Cloud.

Nei contratti aventi ad oggetto servizi SaaS qualificati, le Amministrazioni prevedono gli SLI obbligatori presenti nella tabella "Indicatori della Qualità del Servizio" di cui all'Allegato A.

La data di attivazione della *piattaforma dedicata e del Marketplace Cloud* sarà comunicata insieme alle modalità operative della procedura di qualificazione sul sito https://cloud.italia.it.

1.1.12 Allegati

ALLEGATO A "Requisiti per la qualificazione di servizi SaaS per il *Cloud della PA*"

ALLEGATO B "Disposizioni per il procurement dei servizi SaaS per il *Cloud della PA*"

IL DIRETTORE GENERALE

Note

Allegato alla CIRCOLARE N. 3 del 9 aprile 2018

1.2 Requisiti per la qualificazione di servizi SaaS per il Cloud della PA.

Versione 1 del 9 Aprile 2018

1.2.1 Acronimi e definizioni

Termine o abbreviazione	Descrizione
AgID, Agenzia	Agenzia per l'Italia Digitale
Codice /Codice dell'Amministrazione Digitale/CAD	Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i.
Cloud della PA	Il Cloud della PA è composto dalle infrastrutture e servizi IaaS/PaaS erogati da Cloud SPC, dai PSN e dai CSP qualificati da AgID ai sensi della Circolare "Criteri per la qualificazione dei Cloud Service Provider per la PA"
Cloud	Insieme di infrastrutture tecnologiche remote utilizzate come risorsa virtuale per la memorizzazione e/o l'elaborazione nell'ambito di un servizio
Cloud SPC o SPC Cloud	Contratto Quadro stipulato da CONSIP con il RTI aggiudicatario della Gara SPC Cloud Lotto 1 (https://www.cloudspc.it/)
CSP	Cloud Service Provider, ovvero fornitore di servizi erogati in modalità Cloud
CSC	Cloud Service Consumer acquirente e fruitore di servizi erogati in modalità Cloud
Fornitore	Soggetto economico che opera nel mercato della fornitura e/o distribuzione di servizi SaaS o PA interessata ad erogare servizi SaaS ad altre Amministrazioni
Giorni	Giorni solari
Marketplace Cloud	Piattaforma digitale che espone il catalogo dei servizi IaaS e PaaS qualificati ai sensi della circolare "Criteri per la qualificazione dei Cloud Service Provider per la PA", nonchè i servizi SaaS qualificati da AgID ai sensi della presente Circolare
Pubbliche amministrazioni/Amministrazioni/PA	Le Amministrazioni, come meglio definite all'art. 2, comma 2 del Codice dell'Amministrazione Digitale
PSN	Soggetto titolare dell'insieme di infrastrutture IT (centralizzate o distribuite), ad alta disponibilità, di proprietà pubblica, eletto a Polo Strategico Nazionale dalla Presidenza del Consiglio dei Ministri, e qualificato da AgID ad erogare ad altre amministrazioni, in maniera continuativa e sistematica, servizi infrastrutturali on-demand, servizi di disaster recovery e business continuity, servizi di gestione della sicurezza IT ed assistenza ai fruitori dei servizi erogati
Software as a Service/SaaS	Tra i modelli di servizio offerti dalle piattaforme di Cloud computing, il Software as a Service (SaaS) identifica una classe di servizi fully-managed in cui il gestore del servizio (CSP) si occupa della predisposizione, configurazione, messa in esercizio e manutenzione dello stesso (utilizzando un'infrastruttura cloud propria o di terzi), lasciando al fruitore del servizio (PA) il solo ruolo di utilizzatore delle funzionalità offerte

Continued on next page

Tabella 1.2 – continued from previous page

Termine o abbreviazione	Descrizione
SPID	Sistema Pubblico d'Identità Digitale, ovvero la soluzione che permette di accedere a tutti i servizi online della Pubblica Amministrazione e di privati federati con un'unica Identità Digitale (username e password) utilizzabile da computer, tablet e smartphone (http://www.spid.gov.it)
PagoPA	Sistema di pagamenti elettronici verso la Pubblica Amministrazione
SLI	Service Level Indicator, una misura quantitativa definita di un determinato aspetto della qualità del servizio (ad es. numero di richieste al secondo, latency, throughput, availability, etc)
SLO	Service Level Objective, un valore o un intervallo di valori di riferimento per un livello di servizio misurato da un indicatore (SLI)
SLA	Service Level Agreement, un accordo formale che prevede le conseguenze del mancato raggiungimento degli obiettivi (SLO) prefissati relativamente alla qualità del servizio
Dati Derivati	Dati che risiedono sotto il controllo del Cloud Service Provider, originati dall'interazione con il servizio Cloud da parte del Cloud Service Customer. I dati derivati includono tipicamente dati di logging, contenenti informazioni su chi ha utilizzato il servizio, quando lo ha utilizzato e che funzionalità ha utilizzato; possono anche includere informazioni circa il numero di utenti autorizzati e le loro identità; includono tutte le configurazioni e customizzazioni supportate dal servizio
Circolare	Circolare AgID "Criteri per la qualificazione di servizi SaaS per il Cloud della PA".
Reversibilità	Il processo attraverso il quale il CSC, in previsione della cessazione del rapporto contrattuale con il CSP, è in grado di recuperare tutti i propri dati memorizzati dal servizio. Il processo di reversibilità prevede diverse fasi in cui, completate le operazioni di recupero dei dati e trascorso il periodo di salvaguardia concordato, il CSP procederà all'eliminazione definitiva di tutti i dati di proprietà del CSC. Le attività di recupero e cancellazione dei dati riguardano anche i dati derivati e le copie di backup.
Autocertificazione	Dichiarazione sostitutiva resa ai sensi del DPR 28 dicembre 2000 n. 445

Si richiamano inoltre i concetti e le definizioni relativi al *Cloud computing* pubblicati dal National Institute of Standards and Technologies nel documento NIST Special Publication 800-145 "The NIST Definition of Cloud Computing", in particolare con riferimento a:

- Platform as a service (PaaS), Infrastructure as a Service (IaaS)
- Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
- le cinque caratteristiche essenziali del Cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service.

Per maggiori dettagli si veda: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

1.2.2 Introduzione

Il presente documento allegato alla Circolare è stato redatto al fine di definire nel dettaglio i requisiti di cui all'art. 4 della Circolare che i CSP devono rispettare per ottenere la qualificazione dei servizi SaaS da parte di AgID.

I servizi SaaS soggetti a qualificazione riguardano applicativi software erogati secondo il paradigma SaaS e compatibili con il *Cloud della PA*. Dal punto di vista tecnico sono dunque individuati i seguenti soggetti che svolgono diversi ruoli durante e/o successivamente al processo di qualificazione:

- **Fornitore Cloud**, un CSP che eroga e amministra le risorse Cloud infrastrutturali di tipo IaaS e/o PaaS utilizzate dai servizi applicativi SaaS per l'erogazione del servizio e rispetto alle quali devono essere compatibili;
- **Fornitore SaaS**, un CSP che richiede la qualificazione della propria soluzione SaaS affinché sia disponibile all'acquisto da parte delle PA;
- **Acquirente**, PA che acquisisce e utilizza i servizi SaaS ed indirettamente le risorse IaaS e/o PaaS sottostanti erogate dal Fornitore Cloud.

E' opportuno notare che le figure del Fornitore Cloud e del Fornitore SaaS possono in alcuni casi specifici coincidere con lo stesso soggetto.

Si intende, preliminarmente, fornire un quadro di riferimento riguardante le modalità di progettazione e realizzazione di una soluzione SaaS da parte dei CSP e il ciclo di vita di un servizio SaaS. Le definizioni del ciclo di vita e dei modelli di deployment che seguono sono altresì utili per contestualizzare e inquadrare i requisiti richiesti per la qualificazione delle soluzioni SaaS.

Ciclo di vita di un servizio SaaS

Una soluzione SaaS prevede un tipico *ciclo di vita* attraverso attraverso il quale viene resa disponibile agli utilizzatori (Acquirenti) da parte del Fornitore SaaS:

- *Provisioning(Predisposizione)*, ossia la predisposizione delle risorse Cloud infrastrutturali necessarie all'installazione ed erogazione della soluzione SaaS. Le attività di predisposizione sono eseguite a cura del Fornitore SaaS nell'ambito dell'infrastruttura Cloud messa a disposizione dal Fornitore Cloud. Tipicamente si tratta di risorse virtuali di tipo computazionale, di storage e di rete; più in generale possono essere comprese risorse di tipo IaaS e/o PaaS;
- *Deployment (Dispiegamento)*, fase in cui avviene da parte del Fornitore SaaS l'installazione e la configurazione dei moduli e componenti applicativi che costituiscono la soluzione SaaS;
- *Esercizio*, fase in cui la soluzione SaaS è fruibile da parte dell'Acquirente che è in grado di utilizzarla secondo quanto previsto contrattualmente;
- *Manutenzione*, fase costituita da brevi periodi temporali in cui la soluzione SaaS esce dalla fase di esercizio risultando non fruibile da parte dell'Acquirente in occasione di attività di aggiornamento, manutenzione o risoluzione di malfunzionamenti da parte del Fornitore SaaS oppure del Fornitore Cloud; al termine di tali brevi periodi si avrà nuovamente una regolare fase di esercizio;
- *Disattivazione*, fase di terminazione della fornitura in seguito alla quale la soluzione SaaS non sarà più utilizzabile dall'Acquirente.

Modelli architetturali delle soluzioni SaaS

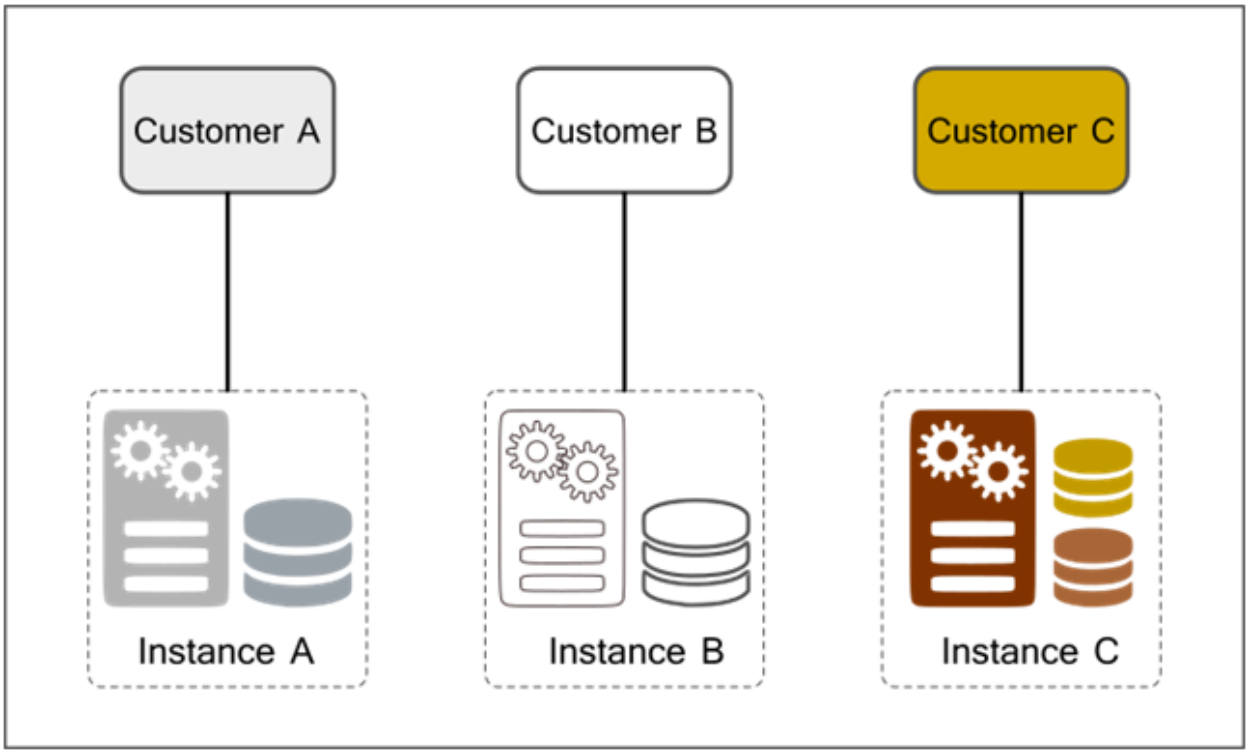
Esistono diversi modelli architetturali per l'erogazione delle soluzioni SaaS che si sono sviluppati nel tempo e a cui i fornitori di soluzioni software fanno tipicamente riferimento durante l'implementazione o il porting del loro software in modalità SaaS. Tali modelli architetturali sono riepilogati anche nella raccomandazione ITU "Recommendation ITU-T X.1602 (2016)" e identificati come livelli di maturità delle applicazioni SaaS.

L'inquadramento rispetto al modello architetturale è importante per poter identificare e verificare le principali caratteristiche di sicurezza, interoperabilità e scalabilità dell'applicazione SaaS.

Si richiamano i quattro seguenti modelli architetturali delle soluzioni SaaS; ciascun modello copre le caratteristiche del precedente ed include proprietà più estese e avanzate.

1. Modello "Custom SaaS application"

Il modello Custom è simile al tradizionale modello di application service provisioning (ASP), in cui ciascun acquirente (o cliente) viene associato ad una specifica istanza applicativa dedicata e quindi dimensionata e personalizzata, anche in termini di middleware, gestione dei dati e sistema operativo. Rispetto al modello ASP classico si ha come differenza principale il fatto che vengono usati dei server virtuali in ambiente cloud.



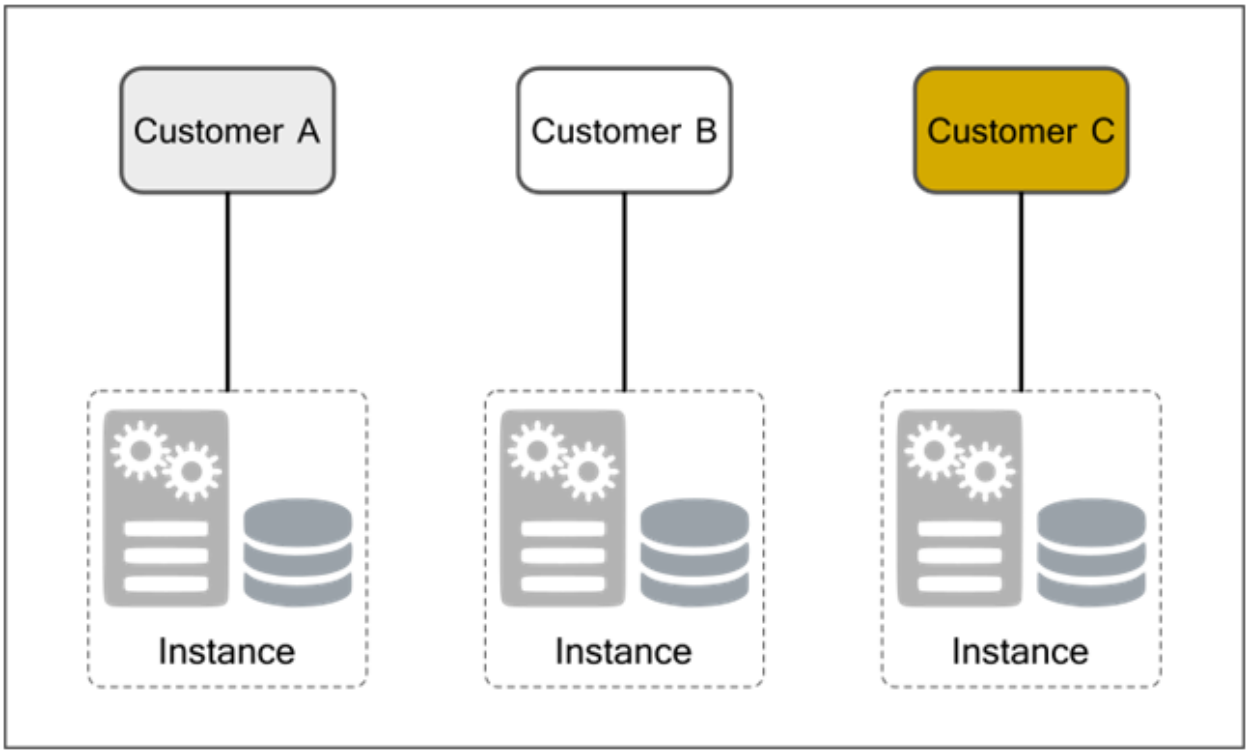
Fanno riferimento a questo modello le applicazioni preesistenti presso il fornitore, oppure presso l'acquirente, di cui viene fatto il porting verso il paradigma Cloud minimizzando gli interventi di adattamento e di re-factoring dell'applicazione. Le applicazioni che vengono esplicitamente pensate per il paradigma Cloud e che vengono riprogettate non dovrebbero mai adottare questo modello.

Il forte limite di questo modello è rappresentato dalla difficoltà con cui può scalare ed adattarsi alle variazioni di domanda dell'utenza. Inoltre l'elevata personalizzazione e la conseguente rigidità di gestione lo rendono un modello con costi operativi tipicamente elevati (in primis per il fornitore e di riflesso anche per l'acquirente).

Rispetto ai cinque elementi essenziali identificati da NIST, le caratteristiche di *resource pooling* e *rapid elasticity *risultano notevolmente limitate in questo modello.

2. Modello "Configurable SaaS application"

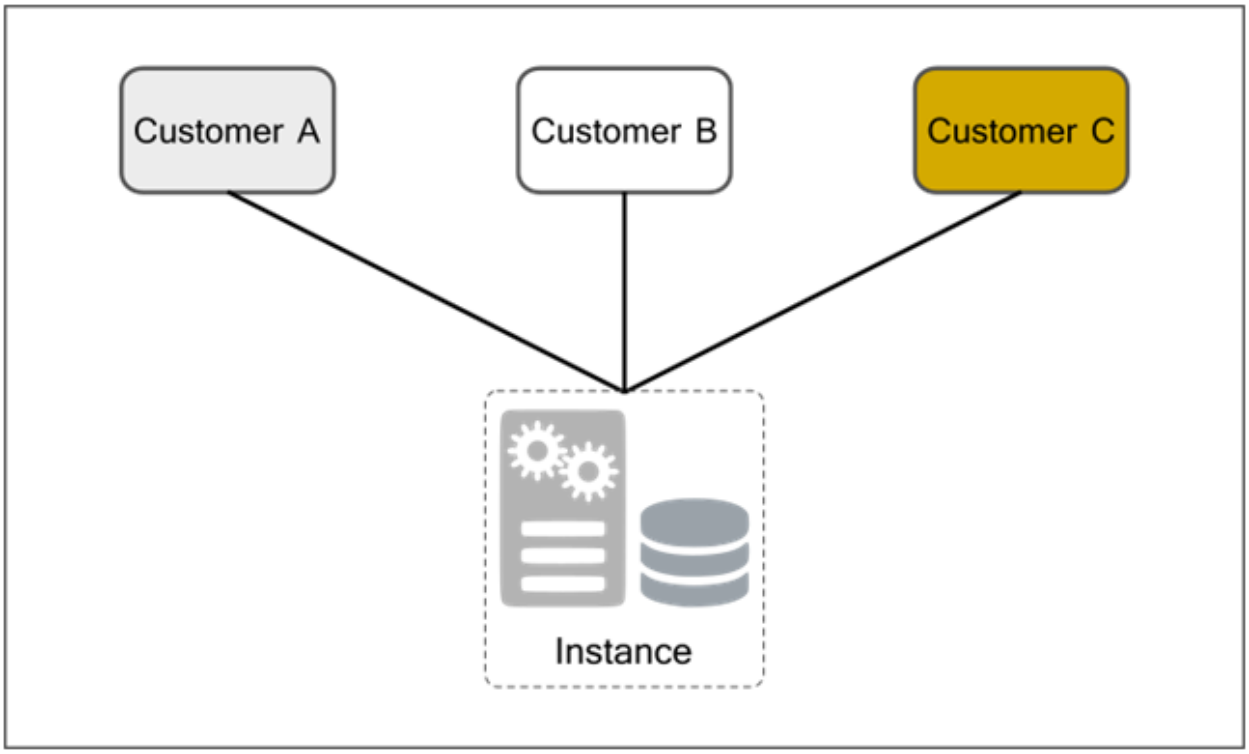
In questo modello l'applicazione risulta essere più standardizzata pur permettendo un certo livello di personalizzazione ("configurazione" di aspetto e comportamento), ma viene comunque dispiegata ed eseguita su risorse virtuali dedicate ed indipendenti. Un tipico esempio è quello dei servizi software offerti dai fornitori di hosting Web per poter costruire siti Web, Blog, Forum, ecc. in modalità self service. Ciascun cliente potrà configurare il software secondo le proprie preferenze, potrà scegliere anche il tipo di sistema operativo. Ciascuna istanza applicativa risulta essere una copia di un pacchetto software standard dispiegata ed eseguita su risorse virtuali assegnate esclusivamente al cliente (in questo ultimo aspetto si mantiene la similitudine col modello precedente).



Dal punto di vista del fornitore SaaS è presente una maggiore flessibilità di gestione per cui le modifiche al codice del pacchetto software potranno essere applicate a tutti i clienti simultaneamente. Questo modello è molto simile al precedente con alcuni aspetti meno rigidi, ma comunque non abbraccia appieno la filosofia e i vantaggi offerti dal paradigma Cloud di tipo SaaS.

3. Modello "Multi-tenant SaaS application"

Una singola istanza applicativa è in grado di servire contemporaneamente più clienti, i quali accedono alla medesima istanza applicativa in esecuzione su risorse virtuali condivise. L'isolamento dei dati e degli utenti avviene a livello applicativo e di gestione dei dati (DBMS), utilizzando gli opportuni meccanismi di autenticazione, autorizzazione e sicurezza. Tipici esempi di questo modello sono i software di CRM (ad es. SalesForce) e di Business Intelligence erogati in modalità SaaS.

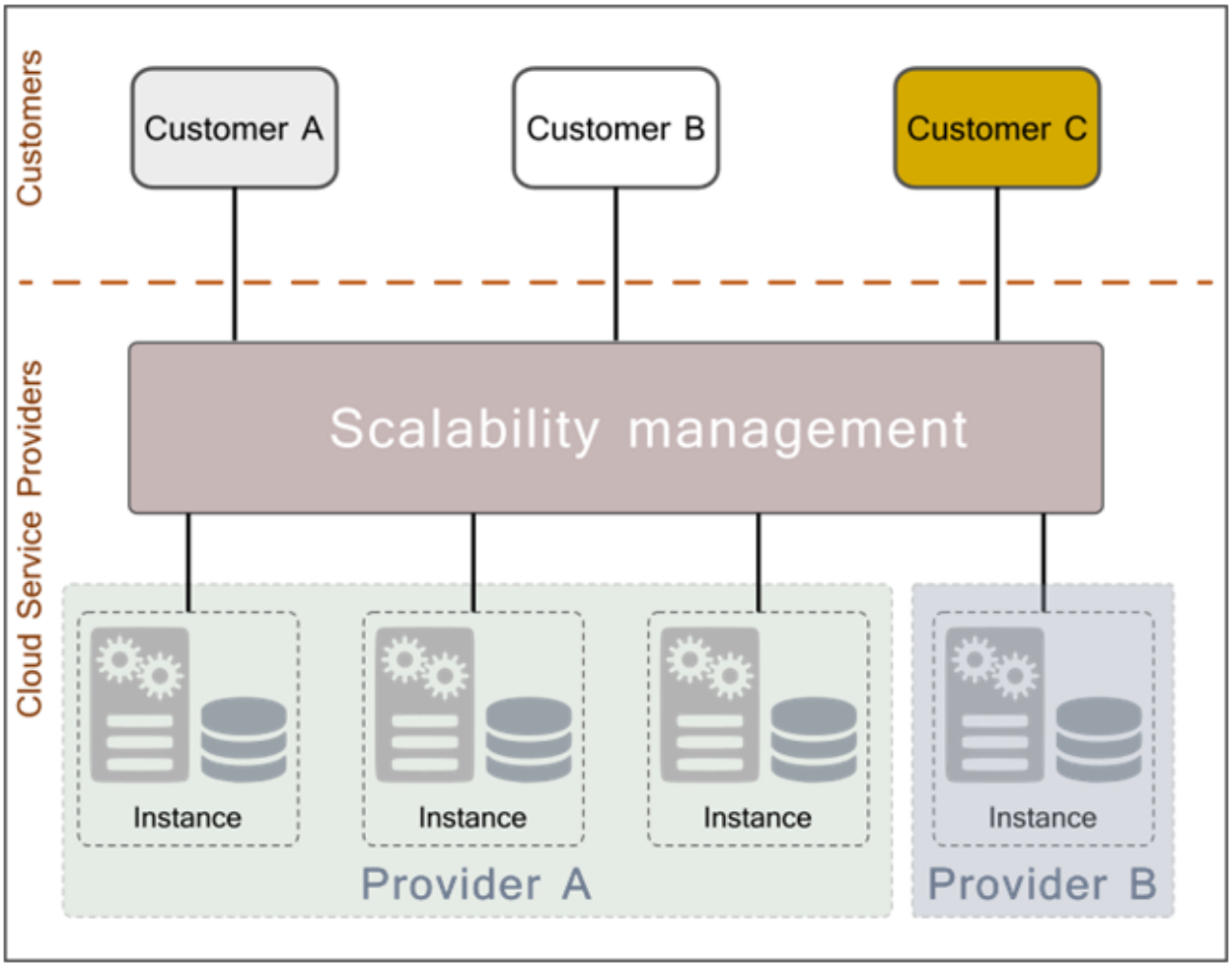


In questo modello viene esaltato l'uso efficiente delle risorse software, computazionali e di storage, con l'evidente vantaggio di riuscire a servire un maggior numero di clienti da parte dei provider. Efficienze che si riflettono anche nella possibilità di abbassare i costi di esercizio e di vendita. Tutto ciò senza andare a discapito della scalabilità e delle performance, che vengono comunque garantite tramite lo sfruttamento dell'elasticità delle risorse Cloud ed un opportuno impiego di tecniche di partizionamento dei dati e di calcolo parallelo.

In questo modello si estrinsecano tutte le caratteristiche essenziali del Cloud computing secondo la definizione NIST. Il livello multi-tenant si sposa bene con i modelli di deployment Public, Private e Community.

4. Modello "Scalable SaaS application"

Nel modello scalabile la dinamicità e la scalabilità dell'ambiente sono messi in primo piano. Questo permette di avere configurazioni più flessibili. I clienti potranno avere la loro istanza applicativa in esecuzione su risorse condivise o dedicate (o un misto delle due) in maniera trasparente e configurabile. Il sistema di load balancing permette di implementare le politiche di allocazione (delle nuove istanze applicative) in funzione di una moltitudine di criteri (uno dei più importanti è la qualità del servizio). Da notare che le istanze applicative possono essere aggiunte e rimosse dinamicamente in qualunque momento ed in base alle esigenze. Anche le risorse virtuali necessarie alle applicazioni sono allocate in modo dinamico. L'allocazione di nuove istanze applicative o di risorse virtuali non richiede nessuna modifica architetturale del sistema che è già stato realizzato in modo da adattarsi dinamicamente. Tutto ciò permette di offrire ed attuare SLA diversificati per i vari clienti.



Infine è da tenere presente che il modello scalabile, per via delle caratteristiche di dinamicità evidenziate si presta ad essere utilizzato (senza richiedere riconfigurazioni o modifiche sostanziali) anche in modalità ibrida (ad es. misto di Public e Private cloud) oppure in modalità multi-cloud in cui diversi cloud provider offrono le risorse virtuali. Un altro scenario è quello del cloud bursting, in cui si ha un misto di Private e Public Cloud oppure una modalità multi-cloud, dove le risorse di un fornitore vengono impiegate automaticamente solo in caso di necessità di espansione del sistema e di maggiori performance.

1.2.3 Requisiti delle soluzioni SaaS

Ciò premesso, AgID, come indicato all'art. 4 della Circolare, ha classificato i requisiti per la qualificazione delle soluzioni SaaS come segue:

- Requisiti organizzativi (RO),
- Requisiti specifici.

Nell'ambito del presente allegato i *requisiti specifici* vengono ulteriormente raggruppati in:

- sicurezza (RS),
- performance e scalabilità (RPS),
- interoperabilità e portabilità (RIP),
- conformità legislativa (RCL).

1.2.4 Requisiti organizzativi

È richiesto che i fornitori di servizi SaaS siano in possesso di alcuni requisiti organizzativi tra cui:

- disponibilità di un servizio di *supporto clienti* strutturato ed in grado di coprire le esigenze operative che possono manifestarsi nel contesto dell'erogazione dei servizi proposti.
- disponibilità di un processo maturo e affidabile in grado di assicurare un continuo *aggiornamento del software* relativo alle soluzioni fornite in modalità SaaS.
- adozione delle *"best-practice" del settore*, nonché delle linee guida descritte in questo allegato tecnico per quanto riguarda lo sviluppo, configurazione e manutenzione del software utilizzato per implementare i servizi erogati.

Nello specifico, si riporta l'elenco dei requisiti organizzativi:

RO1 - Il Fornitore SaaS dovrà rendere disponibile, su richiesta, un account di test utilizzabile da AgID per effettuare ogni tipo di verifica che si renderà necessaria per il mantenimento della qualificazione.

RO2 - Il Fornitore SaaS mette a disposizione i necessari canali di comunicazione e sistemi di gestione (issue tracking) al fine di consentire all'Acquirente di segnalare anomalie, malfunzionamenti e potenziali pericoli per la sicurezza del servizio. Il Fornitore SaaS assicura procedure chiare e con tempistiche garantite per la presa in carico e gestione delle segnalazioni, garantendo all'Acquirente adeguata visibilità dei processi di tracking e supporto (con riferimento agli aspetti di interesse per l'Acquirente).

RO3 - Il Fornitore SaaS assicurara la disponibilità di manuali tecnici e guide d'uso (e/o altro materiale di supporto), ivi compresa la documentazione tecnica delle API e delle interfacce SOAP/REST, specificando se disponibili anche in lingua italiana.

RO4 - Il Fornitore SaaS garantisce la tempestiva disponibilità di informazioni all'Acquirente circa i cambiamenti e le migliorie introdotti in seguito ad aggiornamenti delle modalità di funzionamento e fruizione dei servizi SaaS erogati. In caso di interventi di manutenzione che comportino l'indisponibilità (anche parziale) del servizio, il Fornitore SaaS li comunica all'Acquirente con almeno 3 giorni lavorativi di anticipo utilizzando un canale di comunicazione diretto.

RO5 - Il Fornitore SaaS dichiara gli obiettivi (SLO) corrispondenti agli indicatori di servizio (SLI) identificati come obbligatori nella Tabella 1.1 "Indicatori della Qualità del Servizio" e ne garantisce il rispetto nei rapporti contrattuali con l'Acquirente (come previsto dall'art. 9 della Circolare). Il Fornitore SaaS può dichiarare eventuali ulteriori indicatori della medesima tabella, oppure indicarne di nuovi, che potranno essere inseriti (insieme agli specifici SLO) quali impegni sulla qualità del servizio nei rapporti contrattuali.

RO6 - Il Fornitore SaaS rende disponibile l'accesso a strumenti di monitoraggio e di logging, consentendo all'Acquirente di filtrare e limitare i risultati agli eventi di suo interesse.

RO7 - Il calcolo dei costi imputati all'Acquirente deve essere trasparente e accurato, rispettare le condizioni contrattuali ed essere monitorabile dall'Acquirente. In aggiunta, il Fornitore SaaS rende disponibile all'Acquirente una dashboard e delle API che permettono di acquisire le informazioni di dettaglio sulle metriche di "billing".

Il fornitore potrà dichiarare e documentare il possesso di ulteriori requisiti di tipo organizzativo e/o altre certificazioni tecniche che abbiano attinenza con la soluzione SaaS sottoposta alla procedura di qualificazione.

1.2.5 Requisiti specifici

I requisiti specifici riguardano le seguenti tematiche:

- sicurezza,
- performance e scalabilità,
- interoperabilità e portabilità,
- conformità legislativa.

1.2.6 Sicurezza

Il Fornitore SaaS, prima della messa in esercizio del servizio SaaS, deve garantire che il codice applicativo sia stato sviluppato seguendo i principi dello sviluppo sicuro. Il fornitore deve dichiarare se il software viene sottoposto a periodiche verifiche di sicurezza secondo il framework OWASP, in particolare a seguito di operazioni di manutenzione del servizio (aggiornamenti e modifiche).

Il Fornitore SaaS deve dotarsi di una adeguata organizzazione e di procedure operative in grado di gestire attività continue e documentabili di aggiornamenti e migliorie in tema di sicurezza. Deve inoltre gestire tempestivamente eventuali situazioni emergenziali.

Il Fornitore SaaS deve garantire che il verificarsi di incidenti di sicurezza oppure gravi disfunzioni del servizio (ad esempio nel caso di denial of service) siano prontamente rilevati e gestiti.

Di seguito è riportato il dettaglio dei requisiti di sicurezza:

RS1 - Il Fornitore SaaS dichiara se le componenti che costituiscono il servizio SaaS sono state sottoposte ai test OWASP con esito positivo.

RS2 - Il Fornitore SaaS dichiara di esserere in possesso della certificazione secondo lo standard ISO/IEC 27001 estesa con i controlli degli standard ISO/IEC 27017 e ISO/IEC 27018. La certificazione deve essere stata rilasciata da organismi nazionali di accreditamento riconosciuti dalla Unione Europea. In alternativa, il Fornitore SaaS effettua il CSA STAR Self-Assessment2 con riferimento al servizio che intende qualificare (nella versione denominata CAIQ), ne produce la relativa documentazione e la rende pubblicamente consultabile sul proprio sito Web.

[2] Si veda https://cloudsecurityalliance.org/star/self-assessment/

1.2.7 Performance e scalabilità

Il Fornitore SaaS è tenuto a dichiarare la qualità offerta e l'affidabilità del servizio durante tutto il ciclo di vita. Le Amministrazioni Acquirenti sono tenute a verificare che le pattuizioni relative alla qualità del servizio costituiscano parte integrante del contratto di fornitura, all'interno del quale dovrà essere ricompresa una specifica sezione relativa ai "livelli di servizio garantiti" ovvero al Service Level Agreement (SLA).

Le Amministrazioni acquirenti assicurano che gli accordi relativi ai *livelli di servizio garantiti* (SLA) siano specificati mediante la quantificazione di un insieme di valori *obiettivo* (SLO) o intervalli di valori riferibili ad altrettanti specifici *indicatori* di performance, affidabilità, risultato (SLI). Sulla base di tali accordi il Fornitore SaaS risulterà impegnato a rispettare gli obiettivi dichiarati che dovranno essere monitorabili dall'Acquirente.

La sezione del contratto di fornitura relativa ai *livelli di servizio garantiti* include le *penali compensative* che il Fornitore SaaS corrisponde all'Acquirente in caso di mancato rispetto di uno o più valori obiettivo (SLO). I metodi di quantificazione e le condizioni di riconoscimento delle penali compensative sono inclusi nel contratto e sono allineati ai valori e alle condizioni di mercato riscontrabili per servizi analoghi o appartenenti alla medesima categoria.

Si richiama inoltre quanto previsto dallo standard ISO/IEC 19086-1:2016 per quanto concerne i livelli di servizio garantiti (SLA):

- deve essere inclusa la definizione chiara e non ambigua di tutti gli indicatori (SLI) e dei relativi valori obiettivo (SLO);
- lo SLA deve essere consultabile pubblicamente mediante l'accesso ad un apposito URL Web;
- devono essere riportate all'interno del SLA le definizioni di tutti i termini specifici riferiti al servizio offerto o di quelli particolarmente rilevanti per la comprensione dell'accordo;
- deve essere previsto esplicitamente che, se successivamente all'avvio della fornitura si dovesse rendere necessaria una qualsiasi modifica ai livelli di servizio garantiti, questa dovrà essere preventivamente notificata all'Acquirente per ottenerne la sua approvazione;

Il Fornitore SaaS produce e invia all'Acquirente un report periodico (almeno con cadenza mensile), contenente il riepilogo dell'andamento dei livelli di servizio nel periodo e che evidenzi gli eventuali sforamenti rispetto agli SLO e le penali compensative maturate.

Il Fornitore SaaS implementa delle politiche e dei piani operativi per garantire la continuità del servizio (business continuity). Inoltre, gestisce tempestivamente il ripristino dell'operatività del servizio in seguito ad eventi catastrofici o imprevisti (disaster recovery).

Il Fornitore SaaS, laddove applicabile, dichiara quali sono le condizioni massime di carico sopportabili dal servizio sia in termini di numero di utenti concorrenti che utilizzano il sistema e/o volume di richieste processabili. Nel caso in cui sia prevista la scalabilità automatica dell'applicativo, il Fornitore SaaS specifica e garantisce quali sono le condizioni e i tempi di attivazione delle istanze aggiuntive.

RPS1 - In aggiunta a quanto previsto nell'ambito del requisito RO5, il Fornitore SaaS descrive la performance del servizio utilizzando parametri tecnici oggettivi e misurabili, sfruttando ove possibile, gli indicatori (SLI) definiti nella direttiva ISO/IEC 19086-1:2016.

RPS2 - Il Fornitore SaaS dichiara che i servizi offerti sono soggetti ad opportuni processi di gestione della continuità operativa (business continuity) in cui sono previste azioni orientate al ripristino dell'operatività del servizio e dei dati da esso gestiti al verificarsi di eventi catastrofici/imprevisti, specificando l'applicazione delle buone pratiche presenti nello standard ISO/IEC 22313.

RPS3 - Nel caso in cui sia prevista la scalabilità automatica del servizio SaaS, il Fornitore SaaS indica le condizioni ed i tempi di attivazione delle risorse aggiuntive che vengono attivate per sopportare i maggiori carichi.

1.2.8 Interoperabilità e portabilità

I servizi SaaS devono consentire l'interoperabilità dei sistemi informativi fra le Amministrazioni pubbliche e fra gli altri applicativi in uso presso il medesimo Acquirente. A tal fine devono esporre opportune *Application Programming Interface* (API).

Tali API 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.

Deve essere sempre possibile la migrazione dell'Acquirente verso un altro Fornitore SaaS con conseguente eliminazione permanentemente dei propri dati al termine della procedura di migrazione. In aggiunta, il Fornitore SaaS dovrà documentare le procedure e modalità di reversibilità del servizio.

Dettaglio dei requisiti di interoperabilità e portabilità:

RIP1 - Il Fornitore SaaS dichiara che il servizio SaaS espone opportune Application Programming Interface (API) di tipo SOAP e/o REST associate alle funzionalità applicative, di gestione e configurazione del servizio.

RIP2 - Il Fornitore SaaS dichiara se il servizio SaaS è interoperabile con i servizi pubblici SPID e PagoPA.

RIP3 - Il Fornitore SaaS garantisce all'Acquirente la possibilità di estrarre in qualsiasi momento una copia completa di dati, metadati e documenti memorizzati dal servizio SaaS in formati pubblici e aperti.

RIP4 - Allo scopo di consentire la migrazione da un altro Fornitore SaaS o servizio SaaS, il Fornitore SaaS garantisce all'Acquirente la possibilità di importare i dati all'interno del servizio SaaS tramite formati pubblici e aperti.

RIP5 - Il Fornitore SaaS dettaglia le procedure per garantire la reversibilità del servizio SaaS.

1.2.9 Conformità legislativa

Il servizio SaaS deve rispettate le norme vigenti riguardanti la sicurezza e la riservatezza dei dati, anche in considerazione del fatto che il servizio prevede l'utilizzo di risorse di calcolo e di storage di tipo Cloud che non sono sotto il diretto e completo controllo dell'Acquirente.

Per consentire all'Acquirente di venire a conoscenza e valutare potenziali incompatibilità o restrizioni legislative, il Fornitore SaaS deve rendere noti gli eventuali Stati esteri in cui sono dislocati i data center, propri e/o dell'infrastruttura Cloud utilizzata, e tramite i quali verrà erogato anche parzialmente il servizio e/o all'interno dei quali transiteranno anche temporaneamente i dati gestiti dal servizio.

Dettaglio dei requisiti di conformità legislativa.

RCL1 - Il Fornitore SaaS specifica per quali aspetti il servizio SaaS è conforme agli obblighi e agli adempimenti previsti dalla normativa europea e italiana in materia di protezione dei dati personali.

RCL2 - Il Fornitore SaaS rende nota la localizzazione dei data center propri e dell'infrastruttura Cloud utilizzata per erogare anche parzialmente il servizio e/o all'interno dei quali transitano anche temporaneamente i dati gestiti dal servizio (ivi compresi i siti di disaster recovery e di backup), specificando quando la localizzazione sia all'interno del territorio nazionale, all'interno della UE o extra UE.

RCL3 - Il Fornitore SaaS, in caso di localizzazione dei data center in territorio extra UE, dichiara l'eventuale applicabilità di accordi bilaterali (ad es. Privacy Shield EU-USA, ecc.) volti alla salvaguardia dei dati elaborati, conservati ed a vario titolo gestiti per erogare il servizio.

1.2.10 Appendice 1

Tabella 1.1 - Indicatori della Qualità del Servizio

Codice SLI	Indicatore	Descrizione
Indicatori obbligatori		
SLI1	Availability	La percentuale di tempo in un dato periodo di riferimento in cui il servizio risulta essere accessibile e usabile. Quale periodo di riferimento si assume convenzionalmente il mese. Il tempo totale del periodo di riferimento, che funge da base di calcolo del dato percentuale, può tenere conto dei fermi programmati del servizio (in tal caso il CSP deve esplicitare questa circostanza).
SLI2	Support hours	L'orario in cui il servizio di supporto tecnico è operativo (eventualmente differenziato per "support plan" sottoscrivibile).
SLI3	Maximum First Support Response Time	Il tempo massimo che intercorre tra la segnalazione di un inconveniente da parte del cliente e la risposta iniziale alla segnalazione da parte del CSP.
Indicatori facoltativi		
SLI4	Cloud Service Bandwidth	La quantità di dati che può essere trasferita in un determinato periodo di tempo. Da intendersi rispetto all'interfaccia Client (laddove applicabile) oppure nell'ambito della virtual network.
SLI5	Limit of Simultaneous Cloud Service Connections	Numero massimo di connessioni simultanee supportate dal servizio.
SLI6	Cloud Service Throughput	Il numero di input o insieme di input correlati tra di loro (transazione) che possono essere processati in ciascuna unità di tempo dal servizio.

Continued on next page

Tabella 1.3 – continued from previous page

Codice SLI	Indicatore	Descrizione
SLI7	Elasticity Speed	Descrive quanto velocemente reagisce il servizio alla richiesta di nuove risorse allorquando: • viene effettuata una richiesta di riallocazione (nel caso di elasticità manuale), oppure • il carico di lavoro cambia (in caso di elasticità automatica).
SLI8	Maximum Time to Service Recovery	Il massimo tempo che intercorre tra l'indisponibilità del servizio dovuta a malfunzionamento di una delle sue componenti e il ripristino della sua normale operatività.
SLI9	Backup Interval	Il tempo che intercorre tra un backup e l'altro.
SLI10	Retention period of backup data	Il periodo di tempo in cui vengono mantenuti i backup da parte del CSP.
SLI11	Backup restoration testing	Il numero di test di restore (a partire dai dati di backup) eseguiti durante un determinato periodo di tempo.
SLI12	Recovery Time Objective (RTO)	Il tempo massimo necessario a ripristinare completamente il servizio dopo un'interruzione dovuta ad un "evento catastrofico" che ha innescato l'attivazione di un ambiente di erogazione secondario (disaster recovery).
SLI13	Recovery Point Objective (RPO)	L'intervallo massimo di tempo che precede un "evento catastrofico" rispetto al quale si può verificare la perdita delle modifiche ai dati come conseguenza delle attività di ripristino del servizio (disaster recovery).
SLI14	Data retention period	Il periodo di tempo in cui i dati del cliente vengono mantenuti dal CSP dopo la notifica di cessazione del servizio.
SLI15	Log retention period	l periodo di tempo in cui i file di log relativi al servizio vengono conservati dopo la notifica di cessazione del servizio.

Tabella 1.2 - Riepilogo requisiti e adempimenti previsti

Requisito	Adempimenti previsti
Requisiti organizzativi	
RO1	Autocertificazione
RO2	Autocertificazione
RO3	Autocertificazione
RO4	Autocertificazione
RO5	Autocertificazione
RO6	Autocertificazione
RO7	Autocertificazione
Sicurezza	
RS1	Autocertificazione
RS2	Autocertificazione Produzione documentazione

Continued on next page

Tabella 1.4 – continued from previous page

Requisito	Adempimenti previsti
Performance e Scalabilità	
RPS1	Autocertificazione
RPS2	Autocertificazione
RPS3	Autocertificazione
Interoperabilità e Portabilità	
RIP1	Autocertificazione
RIP2	Autocertificazione
RIP3	Autocertificazione
RIP4	Autocertificazione
RIP5	Autocertificazione
Conformità legislativa	
RCL1	Autocertificazione
RCL2	Autocertificazione
RCL3	Autocertificazione

1.2.11 Appendice 2 - Scheda tecnica del Servizio SaaS

Nome del servizio

Descrizione generale
Max 800 caratteri

Elenco delle caratteristiche funzionali
10 punti elenco + max 200 caratteri

Ambito di applicazione	
Soggetto richiedente	Per conto proprio (CSP) / soggetto delegato da un CSP
Cloud deployment model	Public/Private/Hybrid
Cloud platform	Openstack/Amazon AWS/Microsoft Azure/Google Cloud/IBM Bluemix/…..
Multi-tenant	Si/No
Eventuali Servizi correlati	
Dipendenze e prerequisiti	

Supporto Clienti	
e-mail	
Online ticketing	
Telefono	
Web chat	
Disponibilità del supporto clienti (giorni e orari)	
Tempi di risposta e di risoluzione garantiti	(indicare se previsti e quantificare)
Assistenza on site	(descrivere se prevista)
Assistenza remota	(descrivere se prevista)

Attivazione e disattivazione del servizio	
Tempi di attivazione e disattivazione	
Processo di attivazione	
Processo di disattivazione	
Estrazione dei dati a seguito di disattivazione	(descrivere tempistiche e modalità)
Formati in cui sarà possibile estrarre i dati	
Estrazione e formati di altri asset (in seguito a disattivazione)	(descrivere tempistiche, modalità e formati di VM, Container descriptor files, ecc.)

Piattaforme abilitanti	
PagoPA	Si/No
SPID	Si/No
Altro	(elenco di eventuali altre piattaforme abilitanti rispetto alle quali il servizio è compatibile)

Reti pubbliche disponibili	
Rete SPC	Si/No
GARR	Si/No
Altro	

Utilizzo del servizio	
Web Browser	Si/No
Browser supportati	(elenco dei browser supportati)
Applicativo da installare	Si/No
App Mobile	Si/No
Differenze nella fruizione del servizio tra la versione Mobile e la versione Desktop	
Altro tipo di fruizione	(se prevista)
Documentazione utente	
Elenco delle lingue in cui è resa disponibile la documentazione utente	
API	URL Autenticazione Altre info
Funzionalità invocabili tramite API e funzionalità che non sono accessibili via API	
Documentazione delle API	URL Web PDF
Disponibilità di un ambiente di test delle API (sandbox)	URL Autenticazione Altro

Scalabilità	
Presente/Assente	
Automatica/Manuale	
Modalità e condizioni previste per la scalabilità del servizio	(descrizione)

Trasparenza, metriche e statistiche di utilizzo	
Strumenti di monitoraggio delle risorse utilizzate, dei costi, e della qualità del servizio	
Metriche disponibili	
Statistiche disponibili	
Report disponibili	

Conformità legislativa	
Localizzazione dei data centers	Italia/EU/Extra EU Elenco nazioni estere
Conformità GDPR	Si/No/Parziale Elementi non conformi Tempistiche di adeguamento previste
Conformità ad altre norme sulla sicurezza e riservatezza dei dati (nazionali ed europee)	(descrivere se presenti)
Accordi bilaterali	(descrivere l'eventuale applicabilità di accordi bilaterali quali Privacy Shield EU-USA, ecc. volti alla salvaguardia dei dati)

Portabilità dei dati del servizio	
Dati esportabili	
Formati dei dati esportabili	
Dati derivati (configurazioni, template, log, ecc.)	

Livelli di servizio garantiti	
Availability	
Support hours	
Maximum First Support Response Time	
Altri indicatori	Elencare
Disponibilità di monitoraggio in tempo reale sullo stato del servizio	Si/No
Disponibilità di notifiche via SMS/email degli eventi di indisponibilità del servizio	Si/No

Misure di sicurezza e protezione dei dati	
Controllo da parte dell'utilizzatore sulla localizzazione dei siti in cui verranno memorizzati e processati i dati	Si/No
Standard di sicurezza dei data center utilizzati per erogare il servizio	Elenco
Approccio utilizzato per eseguire test di penetrazione	
Frequenza con cui sono eseguiti i test di penetrazione	
Approcci utilizzati per proteggere i dati memorizzati dal servizio	
Presenza di procedure per la cancellazione permanente dei dati	Si/No
Approcci utilizzati per la protezione dei dati in transito nelle reti esterne	(Ad es. VPN, IPSEC, HTTPS, ecc.)
Approcci utilizzati per la protezione dei dati in transito nelle reti interne	(Ad es. VPN, IPSEC, HTTPS, ecc.)
Meccanismi di autenticazione degli utenti supportati	
Possibilità di configurazione/ customizzazione dei meccanismi di autenticazione	Si/No (eventuale descrizione, anche con riferimento alla possibilità di federazione delle identità)
Disponibilità di autenticazione a 2 fattori	Si/No
Politiche di accesso alle informazioni di audit	In tempo reale (Si/No) Differenziata tra utilizzatori e fornitore (Si/No) Tempo minimo e massimo di conservazione delle informazioni di audit Tempo minimo e massimo di conservazione dei log del servizio

Standard e certificazioni	
Elenco standard	
Elenco certificazioni	
Codici di condotta	(il fornitore può specificare se aderisce a uno o più codici di condotta di cui agli art. 40 e 41 del GDPR)

Prezzi e modalità di imputazione dei costi	
Prezzo del servizio	
Unità di misura	
Altre condizioni	

CAPITOLO 2

Cloud Service Provider

CIRCOLARE N. 2 del 9 Aprile 2018

2.1 Criteri per la qualificazione dei Cloud Service Provider per la PA

2.1.1 Premessa

La presente Circolare e i relativi allegati definiscono, in attuazione a quanto previsto nel "Piano Triennale per l'informatica nella Pubblica amministrazione 2017- 2019", approvato con DPCM del 31 maggio 2017, i requisiti di qualificazione dei Cloud Service Provider (qui di seguito indicati semplicemente CSP), nonché la relativa procedura di qualificazione. Il possesso dei predetti requisiti è presupposto affinchè le infrastrutture e i servizi IaaS e PaaS erogati dal fornitore possano ricevere la qualificazione "CSP" nell'ambito del *Cloud della Pa* (NOTE: Per "Cloud della PA" ai fini della presente circolare, dei suoi allegati e delle successive integrazioni e/o modifiche si intende: l'insieme delle infrastrutture e servizi IaaS e PaaS erogati da Cloud SPC, dai PSN e dai CSP qualificati ai sensi di quanto disposto da questa Circolare.).

I CSP qualificati sono abilitati a richiedere l'inserimento nel *Marketplace Cloud* dei servizi IaaS e PaaS, nonchè i SaaS qualificati ai sensi della Circolare "Criteri per la qualificazione di servizi SaaS per il Cloud della PA".

Ai sensi del Piano Triennale, gli obiettivi strategici nell'ambito della razionalizzazione delle infrastrutture fisiche sono costituiti da:

1. aumento della qualità dei servizi offerti in termini di sicurezza, resilienza, efficienza energetica e continuità di servizio;
2. realizzazione di un ambiente *Cloud della PA*, riqualificando le risorse interne alla PA già esistenti o facendo ricorso a risorse di soggetti esterni qualificati;
3. risparmio di spesa derivante dal consolidamento dei data center e migrazione dei servizi verso tecnologie cloud.

Per il raggiungimento di tali obiettivi, AgID ha previsto, tra le altre attività, una specifica procedura di qualificazione dei CSP nell'ambito della strategia di evoluzione del modello *Cloud della PA*.

Tale procedura consentirà alle Amministrazioni di individuare, nell'ambito del *Marketplace Cloud*, servizi IaaS e PaaS conformi ad un insieme di requisiti comuni definiti dalla presente Circolare e dal relativo allegato.

2.1.2 Definizioni

Termine o abbreviazione	Descrizione
AgID, Agenzia	Agenzia per l'Italia Digitale
Codice /Codice dell'Amministrazione Digitale/CAD	Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i.
Cloud della PA	Il Cloud della PA è composto dalle infrastrutture e servizi IaaS/PaaS erogati da Cloud SPC, dai PSN e dagli altri CSP qualificati da AgID ai sensi della presente Circolare.
Cloud	Insieme di infrastrutture tecnologiche remote utilizzate come risorsa virtuale per la memorizzazione e/o l'elaborazione nell'ambito di un servizio
Cloud SPC o SPC Cloud	Contratto Quadro stipulato da CONSIP con il RTI aggiudicatario della Gara SPC Cloud Lotto 1 (https://www.cloudspc.it)
Fornitore Cloud, CSP, Fornitore	Soggetto titolare dell'infrastruttura e dei servizi IaaS e PaaS o Pubblica Amministazione interessata ad erogare servizi IaaS e PaaS ad altre PA.
Giorni	Giorni solari
Marketplace Cloud	Piattaforma digitale che espone il catalogo dei servizi IaaS e PaaS qualificati ai sensi della presente Circolare, nonchè i servizi SaaS qualificati da AgID ai sensi della circolare "Criteri per la qualificazione dei servizi SaaS per il Cloud della PA"
Pubbliche amministrazioni/Amministrazioni/PA	Le Amministrazioni, come meglio definite all'art. 2, comma 2 del Codice dell'Amministrazione Digitale.
PSN	Soggetto titolare dell'insieme di infrastrutture IT (centralizzate o distribuite), ad alta disponibilità, di proprietà pubblica, eletto a Polo Strategico Nazionale dalla Presidenza del Consiglio dei Ministri, e qualificato da AgID ad erogare ad altre amministrazioni, in maniera continuativa e sistematica, servizi infrastrutturali on-demand, servizi di disaster recovery e business continuity, servizi di gestione della sicurezza IT ed assistenza ai fruitori dei servizi erogati.
Software as a Service, SaaS	Tra i modelli di servizio offerti dalle piattaforme di Cloud computing, il Software as a Service (SaaS) identifica una classe di servizi fully-managed in cui il gestore del servizio (CSP) si occupa della predisposizione, configurazione, messa in esercizio e manutenzione dello stesso (utilizzando un'infrastruttura cloud propria o di terzi), lasciando al fruitore del servizio (PA) il solo ruolo di utilizzatore delle funzionalità offerte.
Platform as a Service, PaaS	Una categoria di servizi cloud in cui le funzionalità cloud offerte sono di tipo programmatico ovvero il CSC può amministrare, dispiegare ed eseguire applicazioni Cloud utilizzando uno o più linguaggi di programmazione, uno o più ambienti di sviluppo/esecuzione supportati dal CSP e i relativi componenti software a corredo (code di messaggi, database, ecc.)
Infrastructure as a Service, IaaS	Una categoria di servizi cloud in cui le funzionalità cloud offerte sono di tipo infrastrutturale, tali funzionalità consentono all CSC di disporre autonomamente in modo programmatico di risorse di computing, di storage e networking.
SPID	Sistema Pubblico d'Identità Digitale, ovvero la soluzione che permette di accedere a tutti i servizi online della Pubblica Amministrazione e di privati federati con un'unica Identità Digitale (username e password) utilizzabile da computer, tablet e smartphone (http://www.spid.gov.it).

Continued on next page

Tabella 2.1 – continued from previous page

Circolare	Circolare AgID "Criteri per la qualificazione dei Cloud Service Provider per la PA".
Mercato elettronico	Il Mercato Elettronico della P.A. (MePA) è il mercato digitale gestito da CONSIP in cui le Amministrazioni abilitate possono acquistare per valori inferiori alla soglia comunitaria, i beni e servizi offerti da fornitori abilitati a presentare i propri cataloghi sul sistema.
SLI	Service Level Indicator, una misura quantitativa definita di un determinato aspetto della qualità del livello di servizio (ad es. numero di richieste al secondo, latency, throughput, availability, etc)

2.1.3 Articolo 1 - Oggetto ed ambito di applicazione

La presente circolare definisce i requisiti e la procedura per la qualificazione dell'infrastruttura e dei servizi IaaS e PaaS dei Cloud Service Provider. Le disposizioni ivi contenute si applicano sia ai fornitori interessati ad offrire servizi IaaS e PaaS alle PA, sia alle amministrazioni che intendono acquisire servizi IaaS e PaaS erogati dai CSP nell'ambito del Cloud della PA.

In particolare come previsto dal Piano Triennale per l'informatica della PA 2017 - 2019, Consip provvede ad abilitare l'accesso agli strumenti del mercato elettronico / convenzioni / accordi quadro ai soli Cloud Service Provider che erogano servizi IaaS e PaaS qualificati da AgID.

2.1.4 Articolo 2 – Il processo di qualificazione

Il fornitore di servizi Cloud, che intende ottenere da AgID la qualificazione della propria infrastruttura, può richiedere la qualificazione CSP per:

1. erogare servizi di tipo Public Cloud (IaaS o PaaS) per la PA - Richiesta "Tipo A";
2. erogare servizi SaaS da qualificare ai sensi della Circolare AgID "Criteri per la qualificazione di servizi SaaS per il *Cloud della PA*" utilizzando la propria infrastruttura Cloud - Richiesta "Tipo B";
3. erogare tutti i servizi previsti nei punti precedenti - Richiesta "Tipo C".

Il processo di qualificazione è articolato in tre fasi:

1. Richiesta di qualificazione
2. Conseguimento della qualificazione
3. Mantenimento della qualificazione *(Monitoraggio)*

Nella tabella seguente sono riportati tutti gli attori coinvolti nel processo di qualificazione ed il loro ruolo in termini di responsabilità (RACI).

N.	Fasi del processo di qualificazione	Fornitore	AgID	PA acquirente
1	Richiesta di qualificazione	A, R	I	O
2	Conseguimento della qualificazione	I	A, R	O
3	Mantenimento della qualificazione (Monitoraggio)	C	A, R	R

```
R= Responsible:  è colui che esegue le attività della fase
A= Accountable: è colui che è responsabile del risultato della fase
C= Consulted: è colui che deve essere consultato prima di una decisione
```

```
I= Informed:  è colui che  deve essere informato relativamente ad una decisione presa
O= Out of the loop: è colui che non partecipa nel contesto della fase
```

A supporto del processo di qualificazione è previsto l'utilizzo di una piattaforma AgID dedicata ed integrata con il Marketplace Cloud. Tale piattaforma consentirà, tra l'altro, l'accesso tramite SPID e la trasmissione telematica dei documenti ai sensi degli art. 45 e 65 comma 1/b del CAD secondo le modalità operative che saranno pubblicate sul sito https://cloud.italia.it.

2.1.5 Articolo 3 - Requisiti della qualificazione

I requisiti per la qualificazione si suddividono in:

1. Requisiti organizzativi;
2. Requisiti specifici.

Il dettaglio di tali requisiti differenziati per tipologia di richiesta (di cui all'art.2) è fornito all'interno dell'allegato "A" alla presente Circolare, denominato "*Requisiti per la qualificazione dei Cloud Service Provider della PA*".

AgID si riserva la facoltà di modificare/aggiornare/integrare tali requisiti sulla base dell'evoluzione del contesto e delle tecnologie.

2.1.6 Articolo 4 - Fasi del processo di qualificazione.

Fase 1 - Richiesta di qualificazione

Il fornitore interessato alla qualificazione CSP provvede a trasmettere tramite la *piattaforma AgID dedicata* apposita richiesta, fornendo le informazioni e la documentazione in lingua italiana relative al possesso dei requisiti di cui all'allegato "A" alla presente Circolare. Per l'eventuale documentazione d'accompagnamento presentata in lingua straniera dovrà essere allegata idonea traduzione, anche per estratto.

Nel caso in cui un fornitore non abbia alcuna rappresentanza diretta o indiretta in Italia, l'Agenzia per l'Italia Digitale su segnalazione di un'amministrazione proponente, acquisisce le informazioni necessarie alla qualificazione e potrà avviare d'ufficio la procedura mediante la piattaforma AgID dedicata alla qualificazione, secondo le modalità pubblicate sul sito Cloud Italia all'indirizzo: https://cloud.italia.it/

Fase 2 - Conseguimento qualificazione

Il conseguimento della qualificazione CSP coincide con la corretta acquisizione tramite la *piattaforma AgID dedicata* della richiesta di qualificazione. L'Agenzia si riserva di effettuare le verifiche necessarie di cui alla fase successiva del presente processo. I servizi IaaS e PaaS qualificati da AgID sono inseriti nel Marketplace Cloud. I CSP qualificati sono inseriti in apposito registro pubblico nell'ambito di marketplace Cloud.

Fase 3 – Mantenimento della qualificazione

L'Agenzia potrà verificare in ogni momento il possesso del criterio di ammissibilità e dei requisiti previsti per la qualificazione CSP.

Le verifiche potranno essere avviate anche sulla base di segnalazioni formali indirizzate all'Agenzia da parte dell'Amministrazione cliente/utente del CSP qualificato.

L'Agenzia si riserva la facoltà di avvalersi di soggetti terzi per l'espletamento delle attività di verifica.

Al fine del mantenimento della qualifica, il soggetto richiedente si impegna a comunicare tempestivamente all'Agenzia, tramite la piattaforma dedicata, ogni evento che modifichi il rispetto dei requisiti di cui all'allegato "A" alla presente Circolare.

La perdita del possesso del/i criterio/i di ammissibilità e/o di almeno uno dei requisiti di cui all'allegato A, comporta la revoca della qualificazione, ai sensi del successivo articolo 5.

Qualora durante le attività di verifica dovessero emergere elementi relativi a possibili violazioni della normativa sulla privacy, l'Agenzia ne informa tempestivamente il Garante per la protezione dei dati personali.

2.1.7 Articolo 5 - Revoca della qualificazione

L'Agenzia nel caso di:

- perdita di almeno uno dei requisiti di cui all'Allegato A;
- riscontro da parte dei competenti organi di violazioni di norme relative all'attività oggetto di qualificazione;

comunica al fornitore il preavviso di revoca della qualificazione CSP con previsione di un termine per le eventuali controdeduzioni. Nel caso di infruttuoso esperimento del termine o mancato accoglimento delle controdeduzioni presentate, l'Agenzia procede alla revoca della qualificazione CSP con provvedimento motivato, disponendone la contestuale eliminazione dei servizi IaaS e PaaS dal Marketplace Cloud, nonchè la relativa annotazione della cancellazione del fornitore dal registro pubblico dei CSP qualificati, dandone adeguata pubblicità.

Nei casi di revoca della qualificazione CSP, il fornitore non può presentare una nuova richiesta di qualificazione all'Agenzia se non siano venute meno le cause che hanno determinato la revoca.

2.1.8 Articolo 6 – Durata della qualificazione CSP

Salvo i casi di revoca, la qualificazione CSP ha durata pari a 24 mesi a decorrere dalla data di iscrizione nel registro pubblico di cui all'articolo 4.

2.1.9 Articolo 7 - Disposizioni transitorie

Nelle more dell'attivazione della piattaforma dedicata la richiesta di qualificazione potrà essere sottomessa mediante le modalità pubblicate sul sito https://cloud.italia.it

Nelle more dell'attivazione del Marketplace Cloud l'elenco dei servizi IaaS/PaaS dei CSP qualificati sarà pubblicato sul sito https://cloud.italia.it

2.1.10 Articolo 8 - Disposizioni finali

La presente Circolare entra in vigore a partire da 30 giorni dalla data di pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

A decorrere da sei mesi dall'entrata in vigore della presente Circolare, le Amministrazioni acquisiscono esclusivamente servizi IaaS e PaaS qualificati e pubblicati sul Marketplace Cloud.

Nei contratti aventi ad oggetto servizi IaaS e PaaS qualificati, le Amministrazioni prevedono gli SLI obbligatori presenti nella tabella "Indicatori della Qualità del Servizio" di cui all'Allegato A.

La data di attivazione della *piattaforma dedicata e del Marketplace Cloud* sarà comunicata insieme alle modalità operative della procedura di qualificazione sul sito https://cloud.italia.it.

2.1.11 Allegati

ALLEGATO A "Requisiti per la qualificazione dei Cloud Service Provider della PA."

IL DIRETTORE GENERALE

Allegato alla CIRCOLARE N. 2 del 9 Aprile 2018

2.2 Requisiti per la qualificazione dei Cloud Service Provider per la PA

Versione 1 del 6/4/2018

2.2.1 Acronimi e definizioni

Termine o abbreviazione	Descrizione
AgID, Agenzia	Agenzia per l'Italia Digitale
Codice /Codice dell'Amministrazione Digitale/CAD	Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i.
Cloud della PA	Il Cloud della PA è composto dalle infrastrutture e servizi IaaS/PaaS erogati da Cloud SPC, dai PSN e dai CSP qualificati da AgID ai sensi della presente Circolare.
Cloud	Insieme di infrastrutture tecnologiche remote utilizzate come risorsa virtuale per la memorizzazione e/o l'elaborazione nell'ambito di un servizio
Cloud SPC o SPC Cloud	Contratto Quadro stipulato da CONSIP con il RTI aggiudicatario della Gara SPC Cloud Lotto 1 (https://www.cloudspc.it)
CSC	Cloud Service Consumer acquirente e fruitore di servizi erogati in modalità Cloud.
CSN	Cloud Service Partner, è un soggetto terzo che può svolgere attività di supporto o di consulenza per conto del CSP, del CSC o di entrambi.
Fornitore Cloud, CSP, Fornitore	Soggetto titolare dell'infrastruttura e dei servizi IaaS e PaaS o Pubblica Amministrazione interessata ad erogare servizi IaaS e PaaS ad altre PA.
Giorni	Giorni solari
Marketplace Cloud	Piattaforma digitale che espone il catalogo dei servizi IaaS e PaaS qualificati ai sensi della presente Circolare, nonchè i servizi SaaS qualificati da AgID ai sensi della circolare "Criteri per la qualificazione dei servizi SaaS per il Cloud della PA"
Provisioning	Predisposizione delle risorse Cloud infrastrutturali funzionale all'erogazione di servizi Cloud. Le attività di predisposizione sono eseguite a cura del Fornitore Cloud, tipicamente si tratta di attività automatizzate su risorse virtuali di tipo computazionale, di storage e di rete che vengono attivate e configurate opportunamente.
Pubbliche amministrazioni/Amministrazioni/PA	Le Amministrazioni, come meglio definite all'art. 2, comma 2 del Codice dell'Amministrazione Digitale.

Continued on next page

Tabella 2.2 – continued from previous page

PSN	Soggetto titolare dell'insieme di infrastrutture IT (centralizzate o distribuite), ad alta disponibilità, di proprietà pubblica, eletto a Polo Strategico Nazionale dalla Presidenza del Consiglio dei Ministri, e qualificato da AgID ad erogare ad altre amministrazioni, in maniera continuativa e sistematica, servizi infrastrutturali on-demand, servizi di disaster recovery e business continuity, servizi di gestione della sicurezza IT ed assistenza ai fruitori dei servizi erogati.
Platform as a Service, PaaS	Una categoria di servizi cloud in cui le funzionalità cloud offerte sono di tipo programmatico ovvero il CSC può amministrare, dispiegare ed eseguire applicazioni Cloud utilizzando uno o più linguaggi di programmazione, uno o più ambienti di sviluppo/esecuzione supportati dal CSP e i relativi componenti software a corredo (code di messaggi, database, ecc.).
Infrastructure as a Service, IaaS	Una categoria di servizi cloud in cui le funzionalità cloud offerte sono di tipo infrastrutturale, tali funzionalità consentono all CSC di disporre autonomamente in modo programmatico di risorse di computing, di storage e networking.
SLI	Service Level Indicator, una misura quantitativa definita di un determinato aspetto della qualità del servizio (ad es. numero di richieste al secondo, latency, throughput, availability, etc)
SLO	Service Level Objective, un valore o un intervallo di valori di riferimento per un livello di servizio misurato da un indicatore (SLI)
SLA	Service Level Agreement, un accordo formale che prevede le conseguenze del mancato raggiungimento degli obiettivi (SLO) prefissati relativamente alla qualità del servizio.
Dati Derivati	Dati che risiedono sotto il controllo del Cloud Service Provider, originati dall'interazione con il servizio Cloud da parte del Cloud Service Customer. I dati derivati includono tipicamente dati di logging, contenenti informazioni su chi ha utilizzato il servizio, quando lo ha utilizzato e che funzionalità ha utilizzato; possono anche includere informazioni circa il numero di utenti autorizzati e le loro identità; includono tutte le configurazioni e customizzazioni supportate dal servizio.
Circolare	Circolare AgID sui "Criteri per la qualificazione dei Cloud Service Provider per la PA".
Autocertificazione	Dichiarazione sostitutiva resa ai sensi del DPR 28 dicembre 2000 n. 445.

Si richiamano inoltre i concetti e le definizioni relativi al *Cloud computing* pubblicati dal National Institute of Standards and Technologies nel documento NIST Special Publication 800-145 "The NIST Definition of Cloud Computing" e quanto definito negli Standard ISO/IEC 17788:2014 e ISO/IEC 17789:2014 in particolare i concetti di:

- Software as a Service (SaaS), Platform as a service (PaaS), Infrastructure as a Service (IaaS)
- Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
- le caratteristiche essenziali del Cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service.

2.2.2 Introduzione

Il presente documento definisce nel dettaglio i requisiti, di cui all'art. 3 della Circolare, che le infrastrutture e i servizi IaaS e PaaS del Fornitore Cloud devono rispettare per ottenere la qualificazione da parte di AgID quale "CSP qualificato per il *Cloud della PA*". Nella richiesta di qualificazione il Fornitore Cloud include le informazioni relative

alla propria infrastruttura e può includere uno o più servizi IaaS/PaaS. Resta inteso che tutti i servizi per i quali è stata fatta richiesta di qualificazione devono possedere i requisiti di cui al presente allegato e dovranno essere conformi alla vigente disciplina nazionale e europea in materia di protezione dei dati personali (regolamento GDPR - General Data Protection Regulation - Regolamento UE 2016/679).

Sono individuati i seguenti soggetti come attori del processo di qualificazione:

- *Fornitore Cloud o CSP*, che fornisce, gestisce e amministra i l'infrastruttura e i servizi Cloud infrastrutturali di tipologia IaaS e/o PaaS, oggetto della qualificazione;
- *Acquirente o CSC*, PA che acquisisce e/o utilizza i servizi Cloud;
- *Partner o CSN*, è un soggetto terzo che può svolgere attività di supporto e/o di consulenza per conto del CSP. Qualora il partner agisse per conto del Fornitore Cloud per mezzo di opportuna delega e dandone visibilità, può richiedere la qualificazione per conto del CSP;
- *AgID o Agenzia*, Agenzia per l'Italia Digitale in qualità di soggetto responsabile della procedura di qualificazione.

2.2.3 Requisiti delle soluzioni Cloud

AgID, come indicato all'art. 3 della Circolare, ha classificato i requisiti per la qualificazione dei Cloud Service Provider e delle soluzioni Cloud come segue:

- Requisiti organizzativi (RO),
- Requisiti specifici.

Nell'ambito del presente allegato i *requisiti specifici* vengono ulteriormente raggruppati in:

- sicurezza (RS),
- privacy e protezione dei dati personali (RPP)
- performance e scalabilità (RPS),
- interoperabilità e portabilità (RIP),
- conformità legislativa (RCL).

2.2.4 Requisiti organizzativi

Il Fornitore Cloud produce la documentazione necessaria al fine di provare il rispetto dei seguenti requisiti organizzativi:

- di aver gestito in passato ed essere in grado di gestire "situazioni critiche" quali: operazioni di disaster recovery, verifica dell'integrità dei dati e eventuale recupero;
- di disporre di un adeguato sistema di gestione della qualità applicato all'erogazione dei servizi offerti.
- di disporre un servizio di *supporto clienti* strutturato (24x7) ed in grado di coprire le esigenze operative che possono manifestarsi nel contesto dell'erogazione dei servizi proposti.
- di aver adottato procedure formali che disciplinano attività quali:
  - gestione del cambiamento (change management);
  - gestione delle configurazioni (configuration management);
  - gestione degli incidenti (sicurezza e infrastruttura);
- di garantire trasparenza e semplicità dell'offerta economica nelle soluzioni contrattuali.

Gli standard di riferimento per questo insieme di requisiti sono quelli che appartengono alla famiglia ISO/IEC 20000, in particolare gli standard ISO/IEC 20000-1 e ISO/IEC TR 20000-9.

Al fine di garantire un'adeguata gestione della fornitura il Fornitore Cloud deve permettere all'Acquirente di amministrare in maniera strutturata e automatizzata le fasi di acquisto e di gestione/configurazione di ciascun servizio e, ove applicabile, di tutte le risorse/elementi/funzionalità associate (ad es. selezione dei template PaaS, configurazione dei server virtuali, gestione delle risorse di rete, ecc.), garantendo controlli di coerenza durante il processo.

Esperienza del Fornitore Cloud nell'ambito dei servizi IaaS/PaaS

RO1 - Produrre una documentazione storica (almeno 2 case studies negli ultimi 24 mesi) che fornisca evidenza della gestione di "situazioni critiche" e conseguente ripristino dell'infrastruttura (rapporti post mortem). Nel caso in cui non si siano registrate "situazioni critiche" negli ultimi 24 mesi, può essere prodotta analoga documentazione riferita ai test di DR.

Supporto clienti e assistenza tecnica

RO2 - Il Fornitore Cloud deve essere in possesso della certificazione ISO 9001 per la gestione della qualità aziendale.

RO3 - Il Fornitore Cloud mette a disposizione dell'Acquirente un servizio di supporto tecnico disponibile 24/7 e accessibile mediante opportuni canali di comunicazione e adeguati sistemi di gestione (issue tracking), al fine di consentire all'Acquirente di effettuare in completa autonomia le eventuali segnalazioni di malfunzionamenti e potenziali pericoli per la sicurezza e la fruibilità del servizio.

RO4 - Il Fornitore Cloud assicura la massima trasparenza nella gestione delle segnalazioni, garantendo all'Acquirente appropriata visibilità dei processi di issue tracking e assistenza tecnica. Il Fornitore Cloud deve definire le tempistiche per la presa in carico e gestione delle segnalazioni in funzione delle diverse priorità, dichiarando i livelli di servizio garantiti.

RO5 - Il Fornitore Cloud fornisce la documentazione tecnica, le guide d'uso e/o altro materiale di supporto, ivi compresa la documentazione dettagliata delle API e delle interfacce CLI e GUI se previste dal servizio.

Gestione del cambiamento (change management)

RO6 - Al fine di garantire che vengano utilizzate procedure e metodi standard per la gestione tempestiva ed efficiente di ogni cambiamento nell'ambito dell'infrastruttura e dei servizi offerti, il Fornitore Cloud garantisce l'applicazione di un processo di change management, dandone evidenza mediante opportuna documentazione.

RO7 - Il Fornitore Cloud garantisce la disponibilità tempestiva di informazioni all'Acquirente circa i cambiamenti e le migliorie introdotti in seguito ad aggiornamenti apportati alle modalità di funzionamento e fruizione dei servizi Cloud erogati. In caso di interventi di manutenzione il Fornitore ne dà comunicazione all'Acquirente con almeno 3 giorni lavorativi di anticipo utilizzando un canale di comunicazione diretto.

RO8 - Il Fornitore Cloud garantisce che la documentazione tecnica sia sempre aggiornata e coerente con la versione del servizio in esercizio.

Gestione della configurazione (configuration management)

RO9 - Il Fornitore Cloud garantisce che i servizi offerti siano soggetti ad un processo di gestione della configurazione che consente, mediante procedure standard e relativi tool, il controllo di tutte le componenti rilevanti del servizio, indicando inoltre la compliance alle buone pratiche presenti nello standard ISO/IEC 20000-2.

Gestione degli Incidenti (incident & problem management)

RO10 - Il Fornitore Cloud garantisce l'adozione di processi di gestione degli incidenti coerenti con quanto raccomandato dagli standard di sicurezza internazionali (p.e. ISO/IEC 27002, ISO/IEC 27035).

Livelli di servizio e trasparenza

RO11 - Il Fornitore Cloud dichiara gli obiettivi (SLO) corrispondenti agli indicatori di servizio (SLI) identificati come obbligatori nella Tabella 1.1 "Indicatori della Qualità del Servizio" e ne garantisce il rispetto nei rapporti contrattuali. Il Fornitore può comunicare eventuali ulteriori indicatori della medesima tabella, o indicarne di nuovi, che potranno essere inseriti come impegni contrattuali con specifici SLO nei rapporti contrattuali.

RO12 - Il Fornitore Cloud rende disponibile all'Acquirente l'accesso a strumenti di monitoraggio e di logging che permettono di filtrare e limitare i risultati in modo appropriato agli eventi di interesse per l'Acquirente.

RO13 - Il calcolo dei costi imputati all'Acquirente deve essere trasparente e accurato, rispettare le condizioni contrattuali ed essere monitorabile dall'Acquirente. In aggiunta il Fornitore Cloud rende disponibile all'Acquirente una dashboard e delle API che permettono di acquisire le informazioni di dettaglio sulle metriche di "billing".

2.2.5 Requisiti specifici

Il Fornitore Cloud deve dimostrare di essere in grado di erogare i servizi proposti dal punto di vista tecnologico, rispettando i requisiti specifici concernenti le seguenti tematiche:

- sicurezza, privacy e protezione dei dati (RSI)
- performance (RPE),
- interoperabilità e portabilità (RIP),
- conformità legislativa (RCL).

Sicurezza, Privacy e protezione dei dati

RSI1 - Il Fornitore Cloud dichiara di esserere in possesso della certificazione secondo lo standard ISO/IEC 27001 estesa con i controlli degli standard ISO/IEC 27017 e ISO/IEC 27018. La certificazione deve essere stata rilasciata da organismi nazionali di accreditamento riconosciuti dalla Unione Europea.

Performance

Il Fornitore Cloud è tenuto a dichiarare la qualità offerta e l'affidabilità del servizio durante tutto il ciclo di vita. Le Amministrazioni Acquirenti sono tenute a verificare che le pattuizioni relative alla qualità del servizio costituiscano parte integrante del contratto di fornitura, all'interno del quale dovrà essere ricompresa una specifica sezione relativa ai "livelli di servizio garantiti" ovvero al Service Level Agreement (SLA).

Le Amministrazioni acquirenti assicurano che gli accordi relativi ai *livelli di servizio garantiti* (SLA) siano specificati mediante la quantificazione di un insieme di valori *obiettivo* (SLO) o intervalli di valori riferibili ad altrettanti specifici *indicatori* di performance, affidabilità, risultato (SLI). Sulla base di tali accordi il Fornitore Cloud risulterà impegnato a rispettare gli obiettivi dichiarati che dovranno essere monitorabili dall'Acquirente.

La sezione del contratto di fornitura relativa ai *livelli di servizio garantiti* include le *penali compensative* che il Fornitore Cloud corrisponde all'Acquirente in caso di mancato rispetto di uno o più valori obiettivo (SLO). I metodi di quantificazione e le condizioni di riconoscimento delle penali compensative sono inclusi nel contratto e sono allineati ai valori e alle condizioni di mercato riscontrabili per servizi analoghi o appartenenti alla medesima categoria.

Si richiama inoltre quanto previsto dallo standard ISO/IEC 19086-1:2016 per quanto concerne i livelli di servizio garantiti (SLA):

- deve essere inclusa la definizione chiara e non ambigua di tutti gli indicatori (SLI) e dei relativi valori obiettivo (SLO);
- lo SLA deve essere consultabile pubblicamente mediante l'accesso ad un apposito URL Web;
- devono essere riportate all'interno del SLA le definizioni di tutti i termini specifici riferiti al servizio offerto o di quelli particolarmente rilevanti per la comprensione dell'accordo;
- deve essere previsto esplicitamente che, se successivamente all'avvio della fornitura si dovesse rendere necessaria una qualsiasi modifica ai livelli di servizio garantiti, questa dovrà essere preventivamente notificata all'Acquirente per ottenerne la sua approvazione;

Il Fornitore Cloud produce e invia all'Acquirente un report periodico (almeno con cadenza mensile), contenente il riepilogo dell'andamento dei livelli di servizio nel periodo e che evidenzi gli eventuali sforamenti rispetto agli SLO e le penali compensative maturate.

RPE1 - In aggiunta a quanto previsto nell'ambito del requisito RO11, il Fornitore Cloud descrive la performance del servizio utilizzando parametri tecnici oggettivi e misurabili, sfruttando ove possibile, gli indicatori (SLI) definiti nella direttiva ISO/IEC 19086-1:2016.

RPE2 - Il Fornitore Cloud dichiara che i servizi offerti sono soggetti ad opportuni processi di gestione della continuità operativa (business continuity) in cui sono previste azioni orientate al ripristino dell'operatività del servizio e delle risorse da esso gestite al verificarsi di eventi catastrofici/imprevisti, specificando l'applicazione delle buone pratiche presenti nello standard ISO/IEC 22313.

RPE3 - Nel caso in cui sia prevista la scalabilità automatica del servizio (o di alcune sue componenti), il Fornitore Cloud dichiara gli indicatori di performance associati alle caratteristiche di elasticità e scalabilità.

RPE4 - Laddove prevista, la scalabilità automatica del servizio (o di sue componenti) deve attivarsi correttamente al verificarsi delle condizioni operative prestabilite (eventualmente configurabili) e deve garantire che non si verifichino interruzioni nell'erogazione del servizio.

Interoperabilità e portabilità

I servizi IaaS e PaaS qualificati devono consentire l'interoperabilità con altri servizi dello stesso tipo, mediante l'utilizzo di standard aperti (ad es. Open Virtualization Format) ed opportune *Application Programming Interface* (API).

Il Fornitore Cloud deve consentire all'Acquirente di poter migrare le proprie applicazioni verso un altro Fornitore Cloud in maniera semplice e sicura, garantendo la possibilita di estrarre ed eventualmente eliminare permanentemente i propri dati in qualsiasi momento mediante opportuna interfaccia di gestione ed API. Il Fornitore Cloud garantisce l'assenza di ogni tipo *lock-in* dell'Acquirente nei confronti del Fornitore Cloud.

RIP1 - I servizi IaaS/PaaS espongono opportune Application Programming Interface (API) di tipo SOAP e/o REST associate alle funzionalità del servizio e alle procedure di gestione e configurazione del servizio.

RIP2 - Il Fornitore Cloud rende disponibile una adeguata documentazione tecnica delle API che ne chiarisce l'utilizzo.

RIP3 - In caso di aggiornamento delle funzionalità del servizio e/o delle relative API il Fornitore Cloud garantisce la tracciabilità delle diverse versioni delle API disponibili, allo scopo di consentire evoluzioni non distruttive (versioning). Anche la documentazione tecnica delle API dovrà essere tempestivamente aggiornata.

RIP4 - Il Fornitore Cloud garantisce la possibilità di tracciare le richieste SOAP/REST ricevute dal servizio e il loro esito (logging e accounting), anche al fine della non ripudiabilità della comunicazione.

RIP5 - Il Fornitore Cloud garantisce all'Acquirente la possibilità di estrarre in qualsiasi momento una copia completa dei dati e metadati memorizzati (in formato pubblico e aperto) come, a titolo esemplificativo ma non esaustivo: volumi, object e block storage, dump di DB, ecc.

Conformità legislativa

Il Fornitore Cloud mette a disposizione dell'Acquirente gli strumenti e le informazioni necessarie per consentirgli il rispetto della normativa europea e italiana nell'ambito dell'utilizzo dei servizi e dell'infrastruttura qualificata.

RCL1 - Il Fornitore Cloud deve indicare per quali aspetti il servizio proposto è conforme agli obblighi e agli adempimenti previsti dalla normativa (europea e italiana) in materia di protezione dei dati personali.

RCL2 - Il Fornitore Cloud rende nota la localizzazione dei data center propri e/o dell'infrastruttura Cloud utilizzata per erogare anche parzialmente il servizio e/o all'interno dei quali transiteranno anche temporaneamente i dati gestiti dal servizio (ivi compresi i siti di disaster recovery e di backup), specificando quando la localizzazione sia all'interno del territorio nazionale, all'interno della UE oppure extra UE.

RCL3 - Il Fornitore Cloud, in caso di localizzazione dei data center in territorio extra UE, dichiara l'eventuale applicabilità di accordi bilaterali (Privacy Shield EU-USA, ecc.) volti alla salvaguardia dei dati elaborati, conservati ed a vario titolo gestiti per erogare il servizio.

2.2.6 Appendice 1 - Indicatori della Qualità del Servizio

Indicatori della Qualità del Servizio

Codice SLI	Indicatore	Descrizione
Indicatori obbligatori		
SLI1	Availability	La percentuale di tempo in un dato periodo di riferimento in cui il servizio risulta essere accessibile e usabile. Quale periodo di riferimento si assume convenzionalmente il mese. Il tempo totale del periodo di riferimento, che funge da base di calcolo del dato percentuale, può tenere conto dei fermi programmati del servizio (in tal caso il CSP deve esplicitare questa circostanza).
SLI2	Support hours	L'orario in cui il servizio di supporto tecnico è operativo (eventualmente differenziato per "support plan" sottoscrivibile).
SLI3	Maximum First Support Response Time	Il tempo massimo che intercorre tra la segnalazione di un inconveniente da parte del cliente e la risposta iniziale alla segnalazione da parte del CSP.
Indicatori discrezionali (o facoltativi)		
SLI4	Cloud Service Bandwidth	La quantità di dati che può essere trasferita in un determinato periodo di tempo. Da intendersi rispetto all'interfaccia Client (laddove applicabile) oppure nell'ambito della virtual network.
SLI5	Limit of Simultaneous Cloud Service Connections	Numero massimo di connessioni simultanee supportate dal servizio.
SLI6	Cloud Service Throughput	Il numero di input o insieme di input correlati tra di loro (transazione) che possono essere processati in ciascuna unità di tempo dal servizio.

Continued on next page

Tabella 2.3 – continued from previous page

Codice SLI	Indicatore	Descrizione
SLI7	Elasticity Speed	Descrive quanto velocemente reagisce il servizio alla richiesta di nuove risorse allorquando: • viene effettuata una richiesta di riallocazione (nel caso di elasticità manuale), oppure • il carico di lavoro cambia (in caso di elasticità automatica).
SLI8	Maximum Time to Service Recovery	Il massimo tempo che intercorre tra l'indisponibilità del servizio dovuta a malfunzionamento di una delle sue componenti e il ripristino della sua normale operatività.
SLI9	Backup Interval	Il tempo che intercorre tra un backup e l'altro.
SLI10	Retention period of backup data	Il periodo di tempo in cui vengono mantenuti i backup da parte del CSP.
SLI11	Backup restoration testing	Il numero di test di restore (a partire dai dati di backup) eseguiti durante un determinato periodo di tempo.
SLI12	Recovery Time Objective (RTO)	Il tempo massimo necessario a ripristinare completamente il servizio dopo un'interruzione dovuta ad un "evento catastrofico" che ha innescato l'attivazione di un ambiente di erogazione secondario (disaster recovery).
SLI13	Recovery Point Objective (RPO)	L'intervallo massimo di tempo che precede un "evento catastrofico" rispetto al quale si può verificare la perdita delle modifiche ai dati come conseguenza delle attività di ripristino del servizio (disaster recovery).
SLI14	Data retention period	Il periodo di tempo in cui i dati del cliente vengono mantenuti dal CSP dopo la notifica di cessazione del servizio.
SLI15	Log retention period	l periodo di tempo in cui i file di log relativi al servizio vengono conservati dopo la notifica di cessazione del servizio.

Riepilogo applicabilità requisiti e adempimenti previsti

Requisito	Applicabilità alla richiesta di qualificazione	Adempimenti previsti
Requisiti organizzativi		
RO1	Tipo A Tipo B Tipo C	Autocertificazione Produzione documentazione
RO2	Tipo A Tipo B Tipo C	Autocertificazione Produzione documentazione
RO3	Tipo A Tipo C	Autocertificazione

Continued on next page

Tabella 2.4 – continued from previous page

Requisito	Applicabilità alla richiesta di qualificazione	Adempimenti previsti
RO4	Tipo A Tipo C	Autocertificazione Produzione documentazione
RO5	Tipo A Tipo C	Autocertificazione Produzione documentazione
RO6	Tipo A Tipo B Tipo C	Autocertificazione Produzione documentazione
RO7	Tipo A Tipo C	Autocertificazione
RO8	Tipo A Tipo C	Autocertificazione
RO9	Tipo A Tipo C	Autocertificazione Produzione documentazione
RO10	Tipo A Tipo B Tipo C	Autocertificazione Produzione documentazione
RO11	Tipo A Tipo C	Autocertificazione
RO12	Tipo A Tipo C	Autocertificazione
RO13	Tipo A Tipo C	Autocertificazione
Sicurezza		
RSI1	Tipo A Tipo B Tipo C	Autocertificazione Produzione documentazione
Performance		
RPE1	Tipo A Tipo C	Autocertificazione
RPE2	Tipo A Tipo C	Autocertificazione
RPE3	Tipo A Tipo C	Autocertificazione
RPE4	Tipo A Tipo C	Autocertificazione
Interoperabilità e Portabilità		
RIP1	Tipo A Tipo C	Autocertificazione
RIP2	Tipo A Tipo C	Autocertificazione Produzione documentazione
RIP3	Tipo A Tipo C	Autocertificazione
RIP4	Tipo A Tipo C	Autocertificazione
RIP5	Tipo A Tipo C	Autocertificazione
Conformità legislativa		

Continued on next page

Tabella 2.4 – continued from previous page

Requisito	Applicabilità alla richiesta di qualificazione	Adempimenti previsti
RCL1	Tipo A Tipo B Tipo C	Autocertificazione
RCL2	Tipo A Tipo B Tipo C	Autocertificazione
RCL3	Tipo A Tipo B Tipo C	Autocertificazione

2.2.7 Appendice 2 - Scheda tecnica del Servizio (CSP)

Nome del servizio

Descrizione generale
Max 800 caratteri

Elenco delle caratteristiche funzionali
10 punti elenco + max 200 caratteri

Ambito di applicazione	
Soggetto richiedente	Per conto proprio (CSP) / soggetto delegato da un CSP
Tipo di qualificazione	Solo infrastruttura / Infrastruttura + servizi
Cloud deployment model	Public/Private/Hybrid
Cloud platform	Openstack/Amazon AWS/Microsoft Azure/Google Cloud/IBM Bluemix/…..
Eventuali Servizi correlati	
Dipendenze e prerequisiti	

Supporto Clienti	
e-mail	
Online ticketing	
Telefono	
Web chat	
Disponibilità del supporto clienti (giorni e orari)	
Tempi di risposta e di risoluzione garantiti	(indicare se previsti e quantificare)
Assistenza on site	(descrivere se prevista)
Assistenza remota	(descrivere se prevista)

Attivazione e disattivazione del servizio	
Tempi di attivazione e disattivazione	
Processo di attivazione	
Processo di disattivazione	
Estrazione dei dati a seguito di disattivazione	(descrivere tempistiche e modalità)
Formati in cui sarà possibile estrarre i dati	
Estrazione e formati di altri asset (in seguito a disattivazione)	(descrivere tempistiche, modalità e formati di VM, Container descriptor files, ecc.)

Reti pubbliche disponibili	
Rete SPC	Si/No
GARR	Si/No
Altro	

Utilizzo del servizio	
Web Browser	Si/No
Browser supportati	(elenco dei browser supportati)
Applicativo da installare	Si/No
App Mobile	Si/No
Differenze nella fruizione del servizio tra la versione Mobile e la versione Desktop	
Altro tipo di fruizione	(se prevista)
Accesso via SSH	(se applicabile)
Accesso via RDP	(se applicabile)
Altro tipo di accesso	(se previsto)
Documentazione utente	
Elenco delle lingue in cui è resa disponibile la documentazione utente	
API	URL Autenticazione Altre info
Funzionalità invocabili tramite API e funzionalità che non sono accessibili via API	
Documentazione delle API	URL Web PDF Altro
Disponibilità di un ambiente di test delle API (sandbox)	URL Autenticazione Altro

Scalabilità	
Presente/Assente	
Automatica/Manuale	
Modalità e condizioni previste per la scalabilità del servizio	(descrizione)

Trasparenza, metriche e statistiche di utilizzo	
Strumenti di monitoraggio delle risorse utilizzate, dei costi, e della qualità del servizio	
Metriche disponibili	
Statistiche disponibili	
Report disponibili	

Conformità legislativa	
Localizzazione dei data centers	Italia/EU/Extra EU Elenco nazioni estere
Conformità GDPR	Si/No/Parziale Elementi non conformi Tempistiche di adeguamento previste
Conformità ad altre norme sulla sicurezza e riservatezza dei dati (nazionali ed europee)	(descrivere se presenti)
Accordi bilaterali	(descrivere l'eventuale applicabilità di accordi bilaterali quali Privacy Shield EU-USA, ecc. volti alla salvaguardia dei dati)

Portabilità dei dati del servizio	
Dati esportabili	
Formati dei dati esportabili	
Dati derivati (configurazioni, template, log, ecc.)	

Livelli di servizio garantiti	
Availability	
Support hours	
Maximum First Support Response Time	
Altri indicatori	Elenco indicatori
Disponibilità di monitoraggio in tempo reale sullo stato del servizio	Si/No
Disponibilità di notifiche via SMS/email degli eventi di indisponibilità del servizio	Si/No

Misure di sicurezza e protezione dei dati	
Controllo da parte dell'utilizzatore sulla localizzazione dei siti in cui verranno memorizzati e processati i dati	Si/No
Standard di sicurezza dei data center utilizzati per erogare il servizio	Elenco
Approccio utilizzato per eseguire test di penetrazione	
Frequenza con cui sono eseguiti i test di penetrazione	
Approcci utilizzati per proteggere i dati memorizzati dal servizio	
Presenza di procedure per la cancellazione permanente dei dati	Si/No
Approcci utilizzati per la protezione dei dati in transito nelle reti esterne	(Ad es. VPN, IPSEC, HTTPS, ecc.)
Approcci utilizzati per la protezione dei dati in transito nelle reti interne	(Ad es. VPN, IPSEC, HTTPS, ecc.)
Meccanismi di autenticazione degli utenti supportati	
Possibilità di configurazione/ customizzazione dei meccanismi di autenticazione	Si/No (eventuale descrizione, anche con riferimento alla possibilità di federazione delle identità)
Disponibilità di autenticazione a 2 fattori	Si/No
Politiche di accesso alle informazioni di audit	In tempo reale (Si/No) Differenziata tra utilizzatori e fornitore (Si/No) Tempo minimo e massimo di conservazione delle informazioni di audit Tempo minimo e massimo di conservazione dei log del servizio

Standard e certificazioni	
Elenco standard	
Elenco certificazioni	
Codici di condotta	(il fornitore può specificare se aderisce a uno o più codici di condotta di cui agli art. 40 e 41 del GDPR)

Prezzi e modalità di imputazione dei costi	
Prezzo del servizio	
Unità di misura	
Altre condizioni	