Cloud PA

Release versione 0.1

09 apr 2018

Indice

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

Il progetto per il Cloud della Pubblica Amministrazione («Cloud 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.

Questo documento raccoglie le circolari relative al progetto Cloud PA e ne permette la consultazione pubblica. I commenti utilizzano ora la piattaforma Forum Italia. I precedenti commenti, inseriti tramite la funzionalità di Disqus, sono ancora visibili nel documento, nelle sezioni Archivio dei commenti alla circolare «Qualificazione Servizi SaaS per il Cloud della PA» e Archivio dei commenti alla circolare «Qualificazione dei Cloud Service Provider per servizi IaaS/PaaS». Per maggiori informazioni, consulta le Istruzioni per la consultazione pubblica.

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

Istruzioni per la consultazione pubblica

1.1 Informazioni sulla consultazione

- **Durata della consultazione:** dal 29 dicembre 2017 al 1 marzo 2018 per lo schema della circolare AgID "Criteri per la qualificazione di servizi SaaS per il Cloud della PA"
- **Durata della consultazione:** dal 29 gennaio 2018 al 1 marzo 2018 per lo schema della circolare AgID "Criteri per la qualificazione dei Cloud Service Provider per la PA".
- **Settore:** ICT
- **Servizi:** Cloud per la PA

1.2 Esiti della consultazione

I risultati della consultazione pubblica on line saranno presi in considerazione dall'Agenzia per l'Italia Digitale e dal Team per la trasformazione Digitale per la redazione del testo definitivo della Circolare.

1.3 Destinatari

Tutte le parti interessate, compresi i fornitori privati di servizi Cloud e le pubbliche amministrazioni sono invitate a contribuire alla presente consultazione.

1.4 Obiettivo della consultazione

Le Circolari 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 e dei Cloud Service Provider (qui di seguito indicati semplicemente CSP), nonché la relativa procedura

di qualificazione. Il possesso dei predetti requisiti è presupposto per l'inserimento dei CSP tra i soggetti del *Cloud della PA*.

Per "Cloud della PA" si intende l'insieme delle infrastrutture e servizi IaaS/PaaS erogati da Cloud SPC, dai PSN e dai CSP qualificati da AgID.

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.

Tali procedure di qualificazione consentiranno alle Amministrazioni di utilizzare, nell'ambito del *Cloud della PA*, soluzioni IaaS e PaaS fornite dai CSP qualificati e/o servizi SaaS qualificati erogate sulle infrastrutture del Cloud della PA.

1.5 Come partecipare

La consultazione pubblica si arricchisce di una nuova funzionalità che rende i commenti più efficaci. Da oggi con Docs Italia è possibile inserire commenti specifici e puntuali relativi a ciascuna sezione del documento in consultazione. Per farlo utilizza i link che trovi nel documento. Inoltre, i commenti saranno immediatamente visibili anche in Forum Italia, dove sarà possibile continuare la discussione.

La partecipazione alla consultazione pubblica è possibile anche via email all'indirizzo consultazioni-Cloud@agid.gov.it, esclusivamente per le comunicazioni contenenti eventuali informazioni coperte da segreto tecnico-commerciale.

È possibile inviare i propri commenti fino al 1 marzo 2018.

1.6 Link correlati

- Consultazione Circolare CSP
- Consultazione Circolare SaaS
- Forum Consultazione Circolare CSP
- Forum Consultazione Circolare SaaS

1.7 Contatti

- **AgID**: consultazioniCloud@agid.gov.it
- **Team per la Trasformazione Digitale**: info@teamdigitale.governo.it

CAPITOLO 2

Servizi SaaS

Nota: Il documento rappresenta lo schema della Circolare AgID sui «Criteri per la qualificazione di servizi SaaS per il Cloud della PA». Lo schema della circolare è in consultazione e aperto ai commenti **fino al 1 Marzo 2018**.

Nota: Inserisci il tuo contributo: scegli l'argomento cliccando su una delle voci dell'indice e inserisci i tuoi commenti usando il link apposito.

CIRCOLARE N. XX del YY gennaio 2018

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

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 di una soluzione SaaS per la PA erogabile sul *Cloud della PA,* nonché la relativa procedura di qualificazione. Il possesso dei predetti requisiti è presupposto per l'inserimento di una soluzione SaaS destinata a essere erogata sul *Cloud della PA* nel Marketplace SaaS in corso di realizzazione.

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;

[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", per come definito nella seguente tabella.

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 di soluzioni 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*, soluzioni SaaS in possesso di un set minimo di requisiti comuni.

A tale scopo verrà realizzato il catalogo di tutte le applicazioni SaaS disponibili per le PA che darà vita al marketplace delle soluzioni SaaS, per i servizi acquisibili dal mercato, secondo quanto previsto nelle *Disposizioni per il procurement dei servizi SaaS per il Cloud della PA* redatte da CONSIP e riportate nell'allegato B alla presente Circolare, denominato "*Disposizioni per il procurement dei servizi SaaS per il Cloud della PA*".

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 che saranno qualificati come compatibili con i requisiti 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
Fornitore	Soggetto richiedente la qualificazione SaaS
Giorni	Giorni solari
Marketplace SaaS	Piattaforma digitale che permette la selezione e l'acquisto di applicazioni software erogate in Cloud secondo il modello Software-as-a-Service
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	Tra i modelli di servizio offerti dalle piattaforme di Cloud computing, il Software as a Service (SaaS) è il servizio fully-managed in cui il gestore del servizio si occupa della predisposizione, configurazione, messa in esercizio e manutenzione dello stesso, lasciando al fruitore del servizio il solo ruolo di utilizzatore delle funzionalità offerte e che, quindi, non senza oneri di gestione, gestisce o controlla l'infrastruttura cloud necessaria all'erogazione del servizio sottostante.

Continued on next page

Tabella 2.1 – 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).

2.1.3 Articolo 1 - Ambito di applicazione

La presente Circolare definisce i requisiti di qualificazione delle soluzioni SaaS erogabili sul *Cloud della PA* nonché la relativa procedura di qualificazione e si applica a tutti i soggetti pubblici e fornitori ICT privati che hanno interesse a proporre soluzioni alle Pubbliche Amministrazioni in modalità SaaS (Software as a Service).

2.1.4 Articolo 2 – Il processo di qualificazione

Il soggetto richiedente può essere:

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

Il processo di qualificazione è articolato in cinque fasi:

1. Richiesta di qualificazione
2. Istruttoria documentale
3. Test e collaudo *(solo su richiesta del fornitore e in caso di erogazione su SPC Cloud o PSN)*
4. Istruttoria post-collaudo *(solo su richiesta del fornitore e in caso di erogazione su SPC Cloud o PSN)*
5. Mantenimento della qualificazione *(Monitoraggio)*

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

Negli articoli seguenti sono previste le eccezioni di processo, in relazione alle fasi ed ai casi sopra elencati.

N.	Fasi del processo di qualificazione	Soggetto	AgID	CONSIP	PSN / SPC Cloud	Clienti (PA)
1	Richiesta di qualificazione	A, R	I	I	O	O
2	Istruttoria documentale	I	R, A	C	O	O
3	Test e collaudo (solo su richiesta del fornitore e in caso di erogazione su SPC Cloud o PSN)	R	R, A	I	I	O
4	Istruttoria post-collaudo (solo su richiesta del fornitore e in caso di erogazione su SPC Cloud o PSN)	I	R, A	C	O	O
5	Mantenimento della qualificazione (Monitoraggio)	C	A	C	O	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 alla gestione del workflow ed integrata con il marketplace SaaS. 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.

Le modalità operative di trasmissione saranno definite in apposita comunicazione pubblicata sul sito AgID.

2.1.5 Articolo 3 - Criteri di ammissibilità

Al momento della richiesta di qualificazione:

1. il soggetto richiedente, se fornitore SaaS privato, deve risultare abilitato sul sistema "Acquistinretepa" di Consip;
2. la soluzione SaaS proposta per la qualificazione deve essere erogata 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 nel Piano Triennale.

Ai fini dell'ammissibilità alla procedura di qualificazione, il possesso dei requisiti di cui al presente articolo può essere oggetto di autocertificazione.

2.1.6 Articolo 4 - Requisiti per la qualificazione

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

1. Requisiti preliminari;
2. Requisiti organizzativi;
3. Requisiti specifici.

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

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

2.1.7 Articolo 5 - Fasi del processo di qualificazione.

2.1.7.1 Fase 1 - Richiesta di qualificazione

Il soggetto interessato alla qualificazione della soluzione SaaS provvede ad inserire sulla *piattaforma AgID dedicata* apposita richiesta, fornendo le informazioni e la documentazione relativa sia ai criteri di ammissibilità sia al possesso dei requisiti di cui all'allegato "A" alla presente Circolare.

All'atto della presentazione della richiesta di qualificazione SaaS, il soggetto richiedente dovrà dichiarare che, conseguita la qualificazione, si impegna a rispettare, in maniera integrale e incondizionata, senza eccezione, deroga o riserva alcuna, per tutta la durata dei contratti di fornitura stipulati con le Amministrazioni clienti, quanto previsto all'appendice 1 dell'Allegato "A" alla presente Circolare.

Il soggetto richiedente dovrà altresì dichiarare che si impegna ad accettare nei contratti con le Amministrazioni clienti la clausola di risoluzione anticipata in caso di revoca della qualificazione della soluzione SaaS da parte di AgID ed a sottoporsi a qualsiasi verifica che l'Agenzia potrà disporre a garanzia del rispetto degli impegni assunti e del mantenimento dei requisiti e dei criteri di ammissibilità richiesti.

2.1.7.2 Fase 2 - Istruttoria documentale

La fase istruttoria inizia con la verifica preliminare delle informazioni e della documentazione fornita dai soggetti richiedenti, relative al possesso dei requisiti di cui all'articolo 3 della presente Circolare.

L'eventuale esito negativo di tale verifica preliminare viene notificato telematicamente da AgID al soggetto interessato, secondo le modalità operative di trasmissione definite in apposita comunicazione, entro 30 giorni dalla ricezione della richiesta di qualificazione SaaS. Il silenzio dell'Agenzia nel termine indicato equivale all'ammissione della richiesta di qualificazione per come proposta.

Per le richieste ammesse, AgID effettua la verifica delle informazioni e della documentazione fornita dai soggetti richiedenti rispetto ai requisiti di cui all'art.4, per come dettagliati all'Allegato "A" della presente Circolare.

L'esito della verifica delle richieste ammesse potrà essere:

1. **Positivo**: la richiesta di qualificazione rispetta i requisiti oggetto di verifica documentale. Nel solo caso di soluzioni SaaS erogate su SPC Cloud o su PSN, il fornitore che ne abbia fatta esplicita richiesta, concorda con AgID la data del test e del collaudo della soluzione. Il collaudo avviene previo invio all'Agenzia di un documento denominato "Piano di Test" almeno 20 giorni prima della data concordata. A garanzia del fornitore, il "Piano di Test" dovrà contenere le istruzioni per effettuare le fasi di *provisioning* e *deployment* della soluzione SaaS e consentirne la verifica del corretto funzionamento, secondo i requisiti indicati nell'allegato "A" alla presente Circolare;
2. **Negativo con riserva**: la richiesta di qualificazione deve essere oggetto di ulteriori verifiche. AgID trasmette l'esito negativo con riserva e contestuale richiesta di documentazione ed informazioni ad integrazione e completamento di quanto inserito nella *piattaforma AgID dedicata*. Il soggetto richiedente fornisce i documenti e le informazioni integrative all'Agenzia entro 20 giorni dalla ricezione della richiesta. Qualora il soggetto richiedente invii nei termini i documenti e le informazioni integrative, l'Agenzia, previa verifica, comunicherà l'esito dell'istruttoria (Positivo o Negativo). Qualora il soggetto richiedente non invii nei termini i documenti e le informazioni integrative, la richiesta di qualificazione SaaS si intenderà respinta;
3. **Negativo**: la richiesta di qualificazione è respinta. Il soggetto non può presentare una nuova richiesta per la medesima soluzione SaaS se non siano venute meno le cause che hanno determinato il mancato accoglimento e/o superamento del collaudo e comunque non prima di 90 giorni dalla comunicazione dell'esito negativo.

Il provvedimento avente per oggetto l'esito della verifica viene notificato telematicamente da AgID al soggetto interessato in apposita comunicazione, entro 60 giorni dalla ricezione della richiesta. Nel caso di esito negativo con riserva, il termine di 60 giorni si intende interrotto.

2.1.7.3 Fase 3 – Test e collaudo (Opzionale)

Nel caso di richieste di qualificazione SaaS erogate su SPC Cloud o su PSN, qualora il fornitore ne abbia fatta esplicita richiesta, in seguito alla notifica positiva della Fase 2 "Istruttoria documentale", avrà luogo la fase di test e collaudo su ambiente SPC Cloud Lotto 1 o equivalente. L'ambiente SPC Cloud Lotto 1 o altro ambiente tecnologicamente omogeneo sarà messo a disposizione e comunicato da AgID al fornitore SaaS.

Durante questa fase il fornitore SaaS ed AgID eseguono congiuntamente i test contenuti nel documento "Piano dei Test".

AgID si riserva di effettuare ulteriori test non previsti all'interno di tale documento volti a verificare il possesso dei requisiti (cfr. Allegato A) da parte della soluzione SaaS oggetto di qualificazione.

2.1.7.4 Fase 4 –Istruttoria post-collaudo (Opzionale)

Al termine della fase 3, AgID procede alla verifica del mantenimento dei criteri di ammissibilità e comunica al soggetto l'esito della procedura di qualificazione che potrà essere:

1. **Positivo**: la richiesta di qualificazione si considera accolta;
2. **Negativo con riserva**: è necessario ripetere il test e collaudo di cui alla Fase 3 concordando con AgID i nuovi termini e modalità;
3. **Negativo**: la richiesta di qualificazione è respinta. Il soggetto non può presentare una nuova richiesta per la medesima soluzione SaaS se non siano cessate le cause che hanno determinato il mancato accoglimento e comunque non prima di 90 giorni.

L'esito viene notificato da AgID al soggetto interessato, secondo le modalità operative di trasmissione definite in apposita comunicazione, entro 60 giorni dalla conclusione della Fase 3 "Test e Collaudo". A seguito dell'avvenuta qualificazione, l'Agenzia comunica a Consip la soluzione SaaS qualificata.

2.1.7.5 Fase 5 – Mantenimento della qualificazione

L'Agenzia verifica la persistenza del possesso dei criteri di ammissibilità e dei requisiti previsti per la qualificazione e di quanto dichiarato nel corso della procedura di qualificazione.

La verifica è avviata sulla base di segnalazioni formali indirizzate all'Agenzia da parte dell'Amministrazione cliente/utente della soluzione SaaS qualificata e svolta con l'esecuzione di attività ispettive e/o richieste di nuovi test da parte di AgID o di soggetti terzi dalla stessa incaricati.

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

L'Agenzia si riserva, inoltre, la facoltà di richiedere al soggetto ogni ulteriore documento correlato all'espletamento del processo di qualificazione, che consideri necessario per poter svolgere le previste attività di verifica. Le difformità riscontrate nel corso dell'attività di verifica sono comunicate al soggetto interessato con indicazione delle modalità e del termine per la loro risoluzione. 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.

2.1.8 Articolo 6 - Revoca della qualificazione

L'Agenzia dispone la revoca della qualificazione SaaS, con provvedimento motivato nel caso di:

- perdita dei criteri di ammissibilità;
- mancato rispetto del termine assegnato, ove non sussistano adeguati motivi di proroga, per l'eliminazione delle difformità riscontrate;
- riscontro da parte dei competenti organi di violazioni di norme relative all'attività oggetto di qualificazione.

La revoca della qualificazione comporta l'eliminazione della soluzione dal marketplace delle soluzioni SaaS ed il divieto di utilizzo del logo rilasciato da AgID nei rapporti commerciali del fornitore.

L'eliminazione della soluzione dal marketplace SaaS è comunicata a tutte le PA che abbiano stipulato contratti ancora attivi alla data del provvedimento di revoca da parte dell'Agenzia.

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

Si specifica, inoltre, che in caso di aggiornamento del software che incide su almeno uno dei requisiti di cui all'art. 4, il soggetto interessato deve procedere a presentare una nuova richiesta di qualificazione della soluzione SaaS. In tal caso, al fine di semplificare il nuovo processo di qualificazione, l'Agenzia potrà tenere conto della documentazione già presentata e procedere alla sola verifica dei nuovi requisiti.

2.1.9 Articolo 7 – Utilizzo della qualificazione SaaS.

Ai soggetti la cui soluzione SaaS ha ricevuto esito positivo nell'istruttoria di qualificazione sarà rilasciato da AgID apposito "Attestato di qualificazione SaaS" con specifico *logo* appositamente registrato.

Tali soggetti potranno utilizzare la qualificazione della soluzione SaaS nei propri rapporti commerciali con le Pubbliche amministrazioni o gli altri soggetti – clienti.

2.1.10 Articolo 8 - Contributo per la procedura di qualificazione

Al fine del ristoro dei costi sostenuti dall'Agenzia, per ciascuna richiesta di qualificazione delle soluzioni SaaS è dovuto il pagamento di un contributo. L'Agenzia determina entro il mese di aprile di ogni anno il valore del corrispettivo dovuto per richiesta. Il mancato pagamento entro i termini prescritti dall'Agenzia, comporta il decadimento della richiesta presentata e/o la revoca della qualificazione SaaS.

2.1.11 Articolo 9 - Disposizioni transitorie e finali

La presente Circolare entra in vigore alla data di pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Le PA che intendono approvvigionarsi delle soluzioni SaaS qualificate dall'Agenzia consultano il marketplace SaaS a partire dalla data di rilascio in esercizio della *piattaforma AgID dedicata *di cui all'art.2 della presente Circolare.

La data di attivazione della *piattaforma dedicata e del marketplace SaaS *sarà comunicata insieme alle modalità operative della procedura di qualificazione sul sito dell'Agenzia.

Nelle more dell'attivazione della *piattaforma dedicata*, i soggetti che intendono avviare il processo di qualificazione possono inviare formale manifestazione d'interesse all'Agenzia, tramite posta elettronica certificata.

Le richieste di qualificazione pervenute nei 12 (dodici) mesi successivi alla pubblicazione nella Gazzetta Ufficiale della Repubblica italiana della presente Circolare non sono soggette al contributo di cui all'art.8.

Nelle more dell'attivazione della procedura di qualificazione dei CSP, solo per il caso a) di cui all'art.2, non sarà oggetto di valutazione il criterio di ammissibilità di cui all'art.3 punto ii) e la qualificazione della soluzione SaaS sarà rilasciata con riserva nell'attesa che il soggetto consegua la necessaria qualifica CSP da AgID, ai sensi del Piano Triennale.

2.1.12 Allegati

ALLEGATO A "Requisiti per la qualificazione di soluzioni SaaS nell'ambito del *Cloud della PA*"

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

IL DIRETTORE GENERALE

Note

Nota: Il documento rappresenta lo schema della Circolare AgID sui «Criteri per la qualificazione di servizi SaaS per il Cloud della PA». Lo schema della circolare è in consultazione e aperto ai commenti **fino al 1 Marzo 2018**.

Nota: Inserisci il tuo contributo: scegli l'argomento cliccando su una delle voci dell'indice e inserisci i tuoi commenti usando il link apposito.

Allegato alla CIRCOLARE N. XX del YY gennaio 2018

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

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 da Cloud SPC, dai PSN e dagli altri CSP che saranno qualificati come compatibili con i requisiti Cloud 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
CSP-S	Cloud Service Provider fornitore di servizi applicativi in modalità cloud
CSP-I	Cloud Service Provider fornitore di servizi infrastrutturali di tipo Cloud (IaaS e PaaS), su cui è possibile erogare servizi Cloud di tipo applicativo (SaaS)
CSC	Cloud Service Consumer acquirente e fruitore di servizi erogati in modalità Cloud.
Fornitore	Soggetto richiedente la qualificazione SaaS
Giorni	Giorni solari
Marketplace SaaS	Piattaforma digitale che permette la selezione e l'acquisto di applicazioni software erogate in Cloud secondo il modello Software-as-a-Service
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.

Continued on next page

Tabella 2.2 – continued from previous page

Termine o abbreviazione	Descrizione
Software as a Service	Tra i modelli di servizio offerti dalle piattaforme di Cloud computing, il Software as a Service (SaaS) è il servizio fully-managed in cui il gestore del servizio si occupa della predisposizione, configurazione, messa in esercizio e manutenzione dello stesso, lasciando al fruitore del servizio (PA) il solo ruolo di utilizzatore delle funzionalità offerte e che, quindi, non senza oneri di gestione, gestisce o controlla l'infrastruttura cloud necessaria all'erogazione del servizio sottostante.
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 del livello di 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 sulla "Qualificazione dei servizi SaaS per il Cloud della PA".
MePA	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.

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

2.2.2 Introduzione

Il presente documento allegato alla Circolare è stato redatto al fine di definire nel dettaglio i requisiti di cui all'art. 3 della Circolare che i CSP devono rispettare per ottenere la qualificazione AgID della propria soluzione SaaS.

Come previsto dalla Circolare la procedura di qualificazione inizia mediante la richiesta del CSP interessato ad ottenere la qualificazione e prevede verifiche amministrative e tecniche di cui il presente allegato fornisce modalità e specifiche.

Le soluzioni SaaS soggette a qualificazione riguardano applicativi software erogati secondo il paradigma SaaS e compatibili con una o più infrastrutture Cloud di tipo *public* o *community*. 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.

2.2.2.1 Modelli architetturali delle soluzioni SaaS

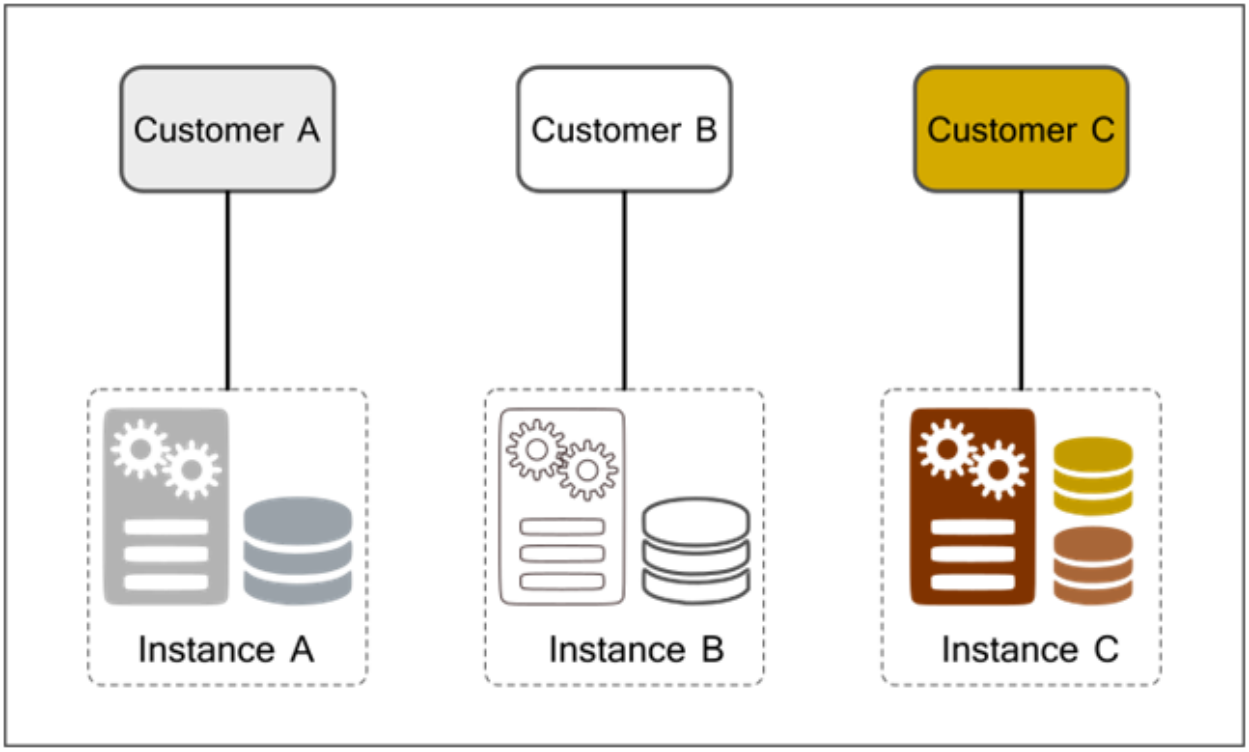
Esistono diversi modelli architetturali per l'erogazione delle soluzioni SaaS che si sono sviluppati nel tempo e a cui i fornitori di soluzioni software fanno tipicamente riferimento durante l'implementazione o il porting del loro software in modalità SaaS. Tali modelli architetturali sono riepilogati 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.



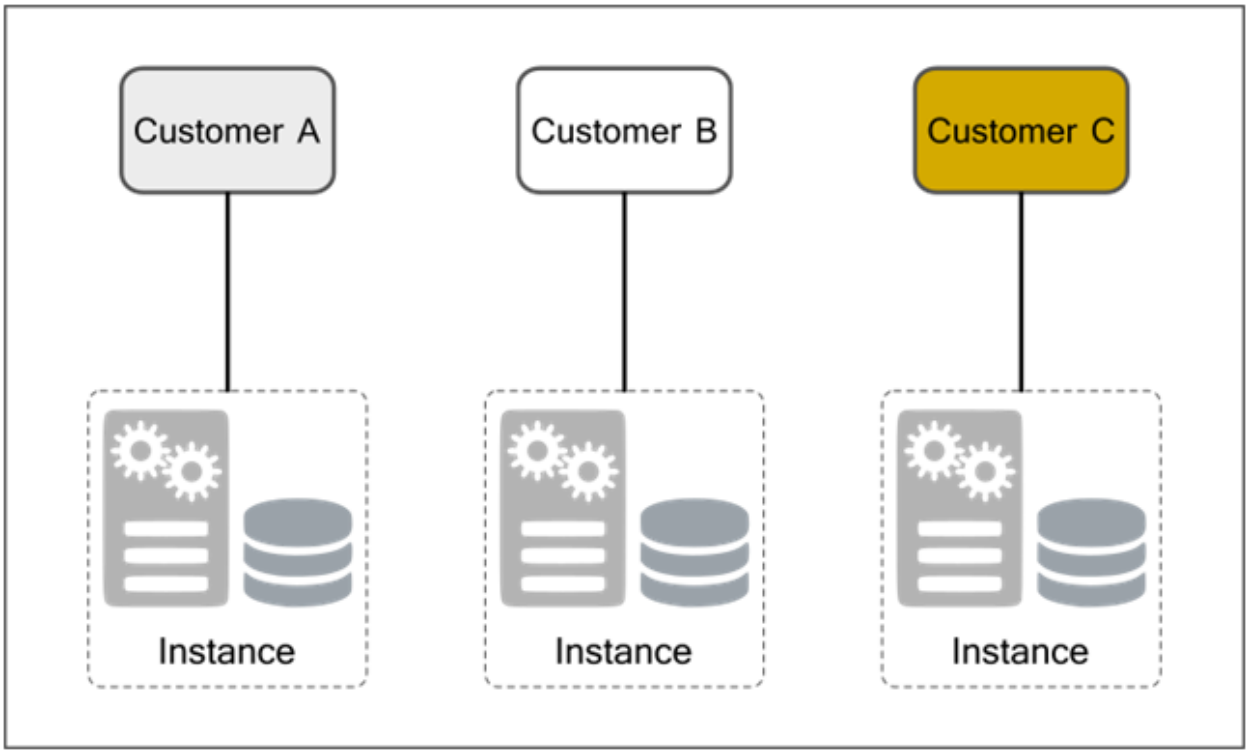
Fanno riferimento a questo modello le applicazioni preesistenti presso il fornitore, oppure presso l'acquirente, di cui viene fatto il porting verso il paradigma Cloud minimizzando gli interventi di adattamento e di re-factoring dell'applicazione. Le applicazioni che vengono esplicitamente pensate per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

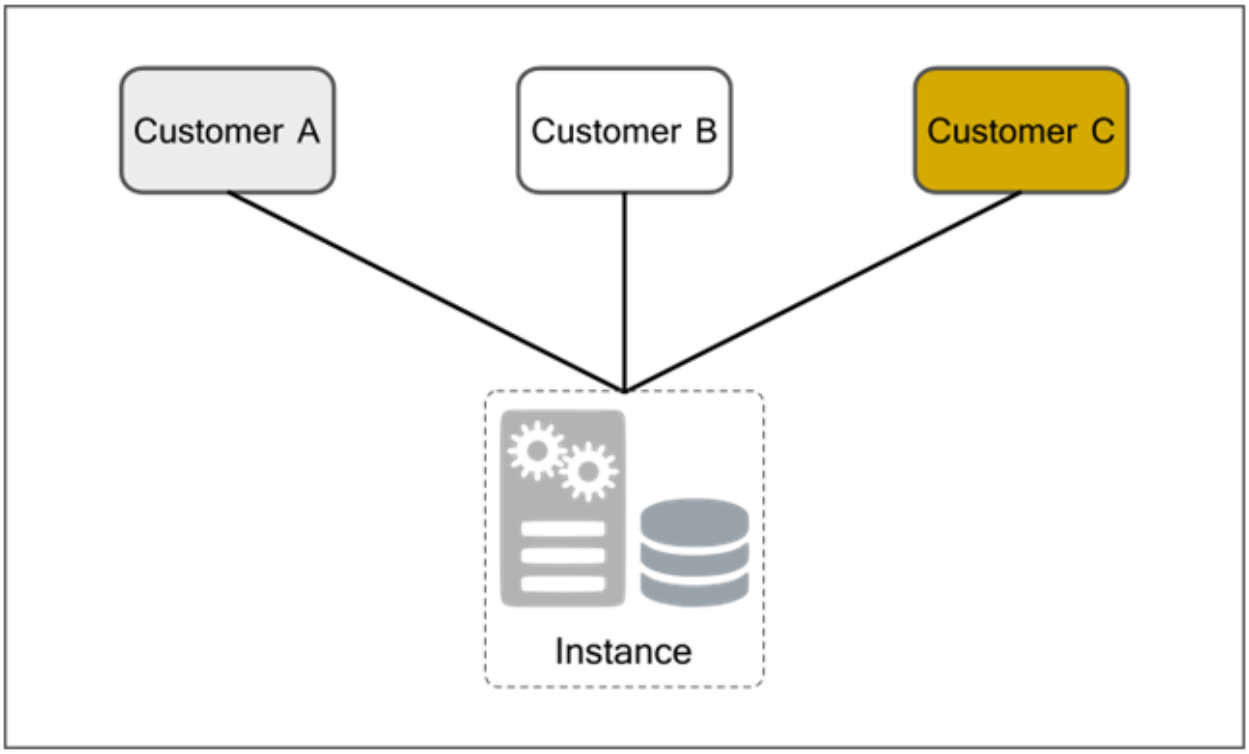
In questo modello l'applicazione risulta essere più standardizzata pur permettendo un certo livello di personalizzazione ("configurazione" di aspetto e comportamento), ma viene comunque dispiegata ed eseguita su risorse virtuali dedicate ed indipendenti. Un tipico esempio è quello dei servizi software 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.

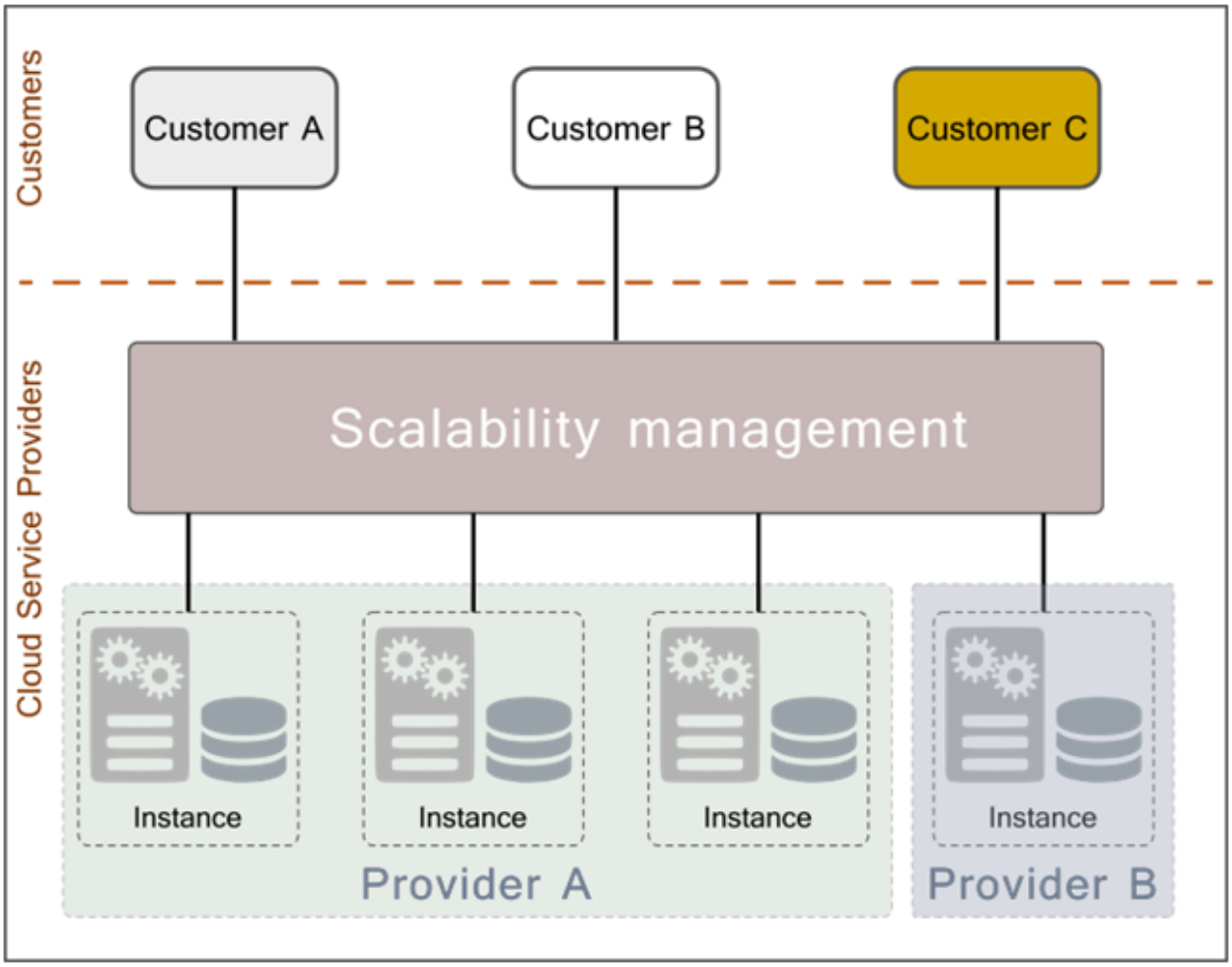


In questo modello viene esaltato l'uso efficiente delle risorse software, computazionali e di storage, con l'evidente vantaggio di riuscire a servire un maggior numero di clienti da parte dei provider. Efficienze che si riflettono anche nella possibilità di abbassare i costi di esercizio e di vendita. 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.

2.2.3 Requisiti delle soluzioni SaaS

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

- Requisiti preliminari (RP),
- 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).

2.2.4 Tipologie di verifiche previste

Nelle sezioni che seguono sono definiti tutti i requisiti previsti per le soluzioni SaaS secondo la classificazione sopra richiamata. Per ciascun requisito è prevista l'effettuazione di una o più verifiche durante la procedura di qualificazione, al fine di accertare il possesso del requisito stesso da parte della soluzione SaaS e/o del Fornitore.

Le tipologie di verifiche previste sono:

- **Dichiarazione del Fornitore SaaS** - il cui accertamento consiste nell'acquisizione di un atto formale in cui il Fornitore SaaS dichiara quanto specificato nel requisito e/o si assume l'obbligo di agire secondo quanto richiesto dal requisito al verificarsi di determinate condizioni. Nel caso in cui sia previsto un obbligo di agire, la verifica consiste nell'accertare che l'obbligo sia stato riportato correttamente, ad esempio, nel contratto di fornitura (NOTE: Si veda la tabella "Clausole contrattuali" riportata in Appendice 1 in cui sono riepilogate le clausole contrattuali oggetto di verifica.). Nel caso in cui sia richiesto di dichiarare informazioni puntuali e/o descrittive, la verifica consiste nell'acquisizione delle specifiche informazioni tramite compilazione da parte del Fornitore SaaS dei moduli di registrazione (form) presenti sulla piattaforma informatica che supporta il processo di qualificazione e della *scheda tecnica del servizio* (NOTE: Si veda l'Appendice 2.).
- **Verifica documentale** - il cui accertamento consiste nella verifica del possesso da parte del Fornitore SaaS di documentazione comprovante il possesso del requisito, di cui viene richiesta la produzione in atti durante la sottomissione della richiesta di qualificazione. La verifica documentale comprende anche il caso in cui al Fornitore SaaS sia richiesto di produrre una documentazione tecnica (manualistica, guida operativa, ecc.) o una certificazione tecnica da consegnare all'Acquirente SaaS nella fase di avvio della fornitura.
- **Verifica tecnica** - nei casi previsti dall'art. 4 (Fase 3) della Circolare viene eseguita una verifica tecnica del requisito nell'ambito di una complessiva attività di collaudo in cui il servizio viene posto in esercizio in un apposito ambiente messo a disposizione da AgID e le cui caratteristiche sono omogenee con quanto previsto per l'ambiente SPC Cloud Lotto 1.

2.2.5 Requisiti preliminari

Nelle soluzioni SaaS che utilizzano PSN o Cloud SPC I fornitori dovranno indicare il livello di automazione di cui l'applicazione dispone per ogni fase del ciclo di vita dell'applicazione. È necessario che le soluzioni SaaS siano in grado di interagire mediante API (Application Programming Interface) con la piattaforma Cloud su cui risiedono e che tale capacità di interazione consenta di sfruttare appieno le potenzialità e i servizi della piattaforma Cloud ospitante.

Le soluzioni SaaS devono poter disporre dinamicamente delle risorse di calcolo, di storage e di rete di tipo IaaS/PaaS, sia per l'attivazione dei servizi (durante le fasi di provisioning e deployment) che, in seguito, per l'adattamento alle variazioni di carico, alle necessità di ripristino da eventuali malfunzionamenti e per la disattivazione dei servizi (cioè nelle fasi di esercizio, manutenzione e disattivazione).

Tipicamente queste funzionalità sono accessibili in modalità programmatica usando le API che le piattaforme Cloud mettono a disposizione. A livello applicativo sarà quindi necessario utilizzare le chiamate API messe a disposizione dalla piattaforma Cloud sottostante relativamente a funzionalità IaaS/PaaS quali: autenticazione, gestione di risorse computazionali, risorse di storage, risorse di rete, funzionalità di logging, acquisizione di metriche/KPIs, eccetera.

Il Fornitore della soluzione SaaS, operando in qualità di amministratore delle risorse Cloud (PaaS/IaaS) deve garantire il corretto funzionamento e la **massima trasparenza** di tutti i processi e le interazioni tra la piattaforma Cloud e l'applicazione SaaS.

Nelle soluzioni SaaS che utilizzano risorse cloud erogate basate su PSN o Cloud SPC il fornitore deve rendere disponibili tutte le informazioni relative all'implementazione ed erogazione del servizio. Tali informazioni vengono dichiarate dal Fornitore SaaS e acquisite da AgID tramite la piattaforma informatica di supporto al processo di qualificazione SaaS.

La produzione di tali informazioni è obbligatoria per il Fornitore SaaS e costituisce un requisito preliminare per la qualificazione (requisito RP5) qualora il Fornitore faccia richiesta di test e collaudo della soluzione SaaS (si veda l'art. 4 (Fase 3) della Circolare).

Elenco dettagliato dei requisiti preliminari:

Codice Requisito	Requisito	Elementi di riscontro
Piena capacità di interfacciarsi con la piattaforma Cloud		
RP1	È necessario specificare se la soluzione SaaS è in grado operare, mediante processi di automazione, funzionalità infrastrutturali della piattaforma Cloud consentendo di: · instanziare le risorse infrastrutturali (IaaS/PaaS) utili ad erogare il servizio; · dismettere risorse (IaaS/PaaS) non più necessarie per l'erogazione del servizio e di conseguenza evitare consumi inutili di tali risorse; · implementare (se richiesto dall'Acquirente) una soluzione ad elevata disponibilità utilizzando risorse della piattaforma Cloud utili alla realizzazione di questa funzionalità.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RP2	Specificare se la soluzione SaaS è in grado di estrarre autonomamente dalla piattaforma IaaS/PaaS le metriche e i KPI utili a controllare l'erogazione del servizio, in particolare per non eccedere i limiti prefissati di consumo delle risorse computazionali, di storage e di rete (banda e accessi); nonché per esporre trasparentemente all'Acquirente i dati sui consumi di tali risorse. Il Fornitore deve dichiarare se e quali KPI/ metriche vengono estratte e in che modo sono utilizzate.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RP3	Specificare se la soluzione SaaS in grado di accedere a funzionalità di recupero del logging/tracing relativo all'esecuzione di processi di sistema erogati dalla piattaforma Cloud, utili nella risoluzione di potenziali problemi connessi ai servizi erogati.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RP4	Specificare se la soluzione SaaS è in grado di gestire compartimenti logici e/o fisici che garantiscono la segregazione delle risorse tra più istanze del servizio in uso a diversi Acquirenti. Si applica solo nel caso di soluzione SaaS multi-tenant.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
Produzione delle informazioni necessarie per l'istruttoria di qualificazione		

Continued on next page

Tabella 2.3 – continued from previous page

Codice Requisito	Requisito	Elementi di riscontro
RP5	Il Fornitore SaaS deve dichiarare: i requisiti necessari per poter garantire l'esecuzione dell'applicazione su piattaforma Cloud, espressi direttamente in termini di caratteristiche delle istanze IaaS e/o PaaS sottostanti che dovranno essere attivate e configurate in fase di provisioning; l'organizzazione architetturale dei moduli e componenti principali della soluzione SaaS; lo stack software su cui è basata la soluzione applicativa, includendo il sistema operativo, il middleware, gli SDK o framework di programmazione, le librerie e le API di terze parti eventualmente utilizzate; le modalità principali di fruizione del servizio (client Web, client Mobile, Thin client, ecc); le modalità programmatiche di fruizione del servizio (Web service REST, Web service SOAP, ecc.); Più in generale, il Fornitore SaaS deve fornire tutte le informazioni richieste nella scheda tecnica del servizio. Inoltre, deve indicare esplicitamente le tipologie di licenze software di eventuali librerie, API e componenti software di terze parti utilizzati. Questo requisito è richiesto solo nel caso la soluzione sia installata su PSN o Cloud SPC.	Dichiarazione Fornitore SaaS Verifica documentale
RP6	Il Fornitore SaaS deve rendere disponibile un account di test ed un URL utilizzabili da AgID per effettuare ogni tipo di verifica (anche a campione) che si renderà necessaria per il rilascio ed il mantenimento della qualificazione.	Dichiarazione Fornitore SaaS
Amministrazione delle risorse Infrastrutturali IaaS/PaaS		
RP7	Il Fornitore SaaS, durante tutto il ciclo di vita della soluzione SaaS opera in qualità di amministratore unico di tutte le risorse Cloud di tipo PaaS/IaaS utilizzate dal servizio che eroga.	Dichiarazione Fornitore SaaS Verifica documentale

2.2.6 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:

Codice Requisito	Requisito	Elementi di riscontro
Supporto clienti e assistenza tecnica		

Continued on next page

Tabella 2.4 – continued from previous page

Codice Requisito	Requisito	Elementi di riscontro
RO1	Il Fornitore SaaS deve mettere 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 deve assicurare delle procedure chiare e con tempistiche garantite per la presa in carico e gestione delle segnalazioni, garantendo all'Acquirente piena visibilità dei processi di tracking e supporto. SLI previsti: SLI09, SLI10	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RO2	Il Fornitore SaaS deve assicurare la disponibilità di manuali tecnici e guide d'uso e/o altro materiale di supporto aggiornati, ivi compresa la documentazione tecnica delle API e delle interfacce SOAP/REST, specificando se disponibili anche in lingua italiana.	Dichiarazione Fornitore SaaS Verifica documentale
Aggiornamento del software		
RO3	Il Fornitore SaaS si assume l'onere di eseguire un monitoraggio del contesto tecnologico e operativo riferibile all'erogazione del servizio, atto a individuare e implementare migliorie e aggiornamenti dello stesso.	Dichiarazione Fornitore SaaS
RO4	Il Fornitore SaaS descrive, mediante documentazione opportuna, il processo e le modalità di aggiornamento dell'applicazione SaaS, indicando in maniera trasparente e chiara l'impatto di ogni operazione sulle funzionalità del servizio.	Dichiarazione Fornitore SaaS
RO5	Il Fornitore SaaS deve garantire una comunicazione puntuale all'utenza dei cambiamenti e delle migliorie introdotti in seguito ad aggiornamento del software.	Dichiarazione Fornitore SaaS
RO6	Il Fornitore SaaS deve garantire la produzione di documentazione e manualistica aggiornata da rendere disponibile in seguito agli aggiornamenti del software.	Dichiarazione Fornitore SaaS
Adozione di best practice e trasparenza		
RO7	Il Fornitore SaaS deve dichiarare i livelli di servizio offerti utilizzando le metriche descritte nella tabella degli indicatori per i livelli di servizio. I livelli di servizio devono essere espressi rispetto a parametri tecnici oggettivi e misurabili.	Dichiarazione Fornitore SaaS Verifica documentale
RO8	Il Fornitore SaaS deve dichiarare i livelli di servizio garantiti per quanto riguarda la disponibilità del servizio e le tempistiche di gestione dei malfunzionamenti che compromettono l'utilizzabilità del servizio da parte dell'Acquirente. SLI previsti: SLI01, SLI12, SLI20	Dichiarazione Fornitore SaaS Verifica documentale

Continued on next page

Tabella 2.4 – continued from previous page

Codice Requisito	Requisito	Elementi di riscontro
RO9	Il Fornitore SaaS deve dichiarare livelli di servizio garantiti per quanto riguarda la gestione delle richieste di assistenza tecnica e la risoluzione delle problematiche segnalate (eventualmente differenziate in base alla loro gravità). SLI previsti SLI11, SLI12	Dichiarazione Fornitore SaaS Verifica documentale
RO10	Il Fornitore SaaS deve documentare e rendere disponibile l'accesso a strumenti di monitoraggio e di logging del servizio SaaS, filtrando e restringendo opportunamente i risultati agli eventi di interesse dell'Acquirente.	Dichiarazione Fornitore SaaS Verifica documentale Verifica tecnica (se prevista)
RO11	Il calcolo dei costi imputati all'Acquirente deve essere trasparente e accurato, rispettare le condizioni contrattuali ed essere monitorabile dall'Acquirente in tempo reale. In particolare il Fornitore SaaS dovrà rendere disponibile all'Acquirente un set minimo di funzioni (API) che permettano di acquisire le informazioni sulle metriche di "billing" (Show back / Charge Back).	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RO12	Il Fornitore SaaS deve dichiarare se possiede o meno la certificazione ISO 27001 in ambito compatibile con quello previsto per l'erogazione del servizio oggetto di qualificazione. In assenza della certificazione ISO 27001 devono essere descritte in dettaglio le buone pratiche utilizzate per implementare il Sistema di Gestione della Sicurezza delle Informazioni.	Dichiarazione Fornitore SaaS Verifica documentale

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.

2.2.7 Requisiti specifici

I requisiti specifici riguardano le seguenti tematiche:

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

2.2.8 Sicurezza

Il Fornitore SaaS, prima della messa in esercizio della soluzione 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 può utilizzare componenti software realizzate da terze parti per implementare la propria applicazione (middleware, librerie o una qualsiasi delle componenti dello stack applicativo). In questi casi egli deve necessariamente rendersi garante anche della sicurezza di queste componenti. Deve essere quindi garantita la sicurezza dell'intera supply chain relativa all'applicazione SaaS (includendo anche il sistema operativo).

Deve essere presente un sistema di Identity & Access Management con una o più figure di amministrazione e diverse figure con privilegi di accesso differenziati e gerarchici. Il trattamento sicuro dei dati è indispensabile per prevenire

possibili perdite di dati oppure l'accesso non protetto ai dati da parte di persone non autorizzate. Una gestione accurata delle credenziali di accesso permette di evitare la compromissione dell'applicazione stessa o dell'ambiente in cui è ospitata. Le informazioni in transito tra le varie componenti del sistema devono essere adeguatamente protette e cifrate.

Le risorse IaaS/PaaS e i software ospitati nella piattaforma Cloud (di base, middleware e applicativi) devono essere protetti dal traffico di rete indesiderato e/o dannoso, garantendo la sicurezza dei dati, del software e degli account utente, nonché prestazioni di rete non degradate.

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 e delle verifiche previste durante la procedura di qualificazione.

Codice Requisito	Requisito	Elementi di riscontro
Sicurezza del codice e delle interfacce		
RS1	Il Fornitore SaaS deve indicare se la soluzione SaaS è stata sottoposta e ha superato i test OWASP.	Dichiarazione Fornitore SaaS
RS2	Il codice binario ed eventualmente il codice sorgente (se disponibile) devono essere sottoposti a verifiche che tendono ad identificare eventuali vulnerabilità o la presenza di codice malevolo (worm, trojans, ecc.) prima della messa in esercizio della soluzione SaaS. Le medesime verifiche vanno ripetute in occasione di operazioni di manutenzione del servizio (aggiornamenti e modifiche).	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RS3	Il Fornitore SaaS può utilizzare componenti software realizzate da terze parti per implementare la propria applicazione (middleware, librerie, componenti da cui l'applicazione dipende). In questi casi egli deve necessariamente rendersi garante anche della sicurezza di queste componenti. Deve essere in sostanza garantita la sicurezza dell'intera supply chain relativa alla soluzione SaaS (includendo anche il sistema operativo).	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RS4	Occorre scegliere accuratamente le componenti di terze parti da utilizzare, assicurarsi di aver utilizzato la fonte originale del software e che non ci siano stati passaggi intermedi capaci di alterare il contenuto originale. Accertarsi che non siano presenti vulnerabilità note nel software utilizzato o che queste siano state opportunamente gestite e neutralizzate. Ripetere periodicamente i controlli e le verifiche sulle componenti software di terze parti e apportare prontamente i fix necessari e/o rimuovere le dipendenze da componenti con accertate vulnerabilità.	Dichiarazione Fornitore SaaS
RS5	È necessario prevedere per gli endpoint del servizio SaaS (ad esempio di tipo REST oppure di tipo SOAP) le stesse misure di autenticazione e autorizzazione previste per gli eventuali client Web o Mobile. Inoltre è necessario garantire la sicurezza delle comunicazioni con tali interfacce tramite l'adozione del protocollo HTTPS.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)

Continued on next page

Tabella 2.5 – continued from previous page

Codice Requisito	Requisito	Elementi di riscontro
Sicurezza del traffico di rete		
RS6	Le risorse IaaS/PaaS e i software ospitati nella piattaforma Cloud (di base, middleware e applicativi) devono essere protetti dal traffico di rete indesiderato e/o dannoso, garantendo la sicurezza dei dati, del software e degli account utente, nonché prestazioni di rete non degradate.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RS7	Il Fornitore SaaS deve mettere in atto misure di network e domain isolation (firewall, ACL, controller di dominio) per mantenere l'isolamento tra i diversi domini applicativi.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RS8	Devono essere attuate da parte del Fornitore SaaS misure per prevenire e contrastare le intrusioni nella rete e la congestione della stessa (intrusion detection, monitoraggio e filtering del traffico di rete anomalo), evitando che possano avere successo eventuali attacchi di denial of service (DoS) o distributed denial of service (DDoS).	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RS9	Nella gestione e monitoraggio del traffico di rete di cui al requisito RS8 devono essere inclusi meccanismi per bloccare il traffico di rete da e verso URL presenti in una blacklist. Il Fornitore SaaS deve curare l'aggiornamento periodico della blacklist.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
Trattamento sicuro dei dati e delle credenziali		
RS10	Il Fornitore SaaS deve assicurare una attenta gestione delle chiavi e dei codici di accesso usati per la soluzione SaaS e le sue componenti costitutive (database, sistemi di code e messaggi, servizi accessori, ecc.).	Dichiarazione Fornitore SaaS
RS11	Qualora la soluzione SaaS, oppure alcune delle sue componenti, effettuino degli accessi amministrativi alle risorse IaaS/PaaS sottostanti per motivi di monitoraggio o di gestione elastica delle stesse deve essere garantita una gestione accurata sia delle credenziali di amministratore dell'applicazione SaaS che delle credenziali amministrative della piattaforma IaaS/PaaS sottostante, evitando in tal modo la compromissione delle risorse Cloud utilizzate.	Dichiarazione Fornitore SaaS
RS12	Nel caso di applicazione che accorpa più acquirenti sullo stesso sistema, separati logicamente gli uni dagli altri (multi-tenant), occorre impedire che un acquirente possa accedere ai dati degli altri accidentalmente oppure aggirando i controlli (data isolation).	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)

Continued on next page

Tabella 2.5 – continued from previous page

Codice Requisito	Requisito	Elementi di riscontro
RS13	Le informazioni in transito tra le varie componenti del sistema devono essere adeguatamente protette e cifrate. Lo stesso principio vale per le informazioni in transito tra il front-end e il back-end dell'applicazione (ad esempio tra il browser dell'utente e il back-end applicativo, oppure tra il client Mobile e il back-end applicativo). Quando la natura della soluzione SaaS o i dati trattati lo richiedono deve essere implementata anche la cifratura lato client (client-side encryption).	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
Gestione sicura delle identità e degli accessi		
RS14	Il Fornitore SaaS deve garantire che non si possano verificare abusi nell'uso delle funzionalità dell'applicazione e nell'accesso ai dati (eventualmente in grado di compromettere la sicurezza), inoltre la soluzione SaaS deve essere associata ad un sistema di gestione delle identità e degli accessi.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RS15	Il sistema di Identity & Access Management deve prevedere una o più figure di amministrazione e diverse figure con privilegi di accesso differenziati e gerarchici.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RS16	Deve essere implementato il tracciamento degli accessi al servizio e dell'accesso ai dati (transaction audit) con monitoraggio continuo delle informazioni per rilevare in tempo reale eventuali attività sospette.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
Gestione degli incidenti e degli aggiornamenti di sicurezza		
RS17	Il Fornitore SaaS deve definire le modalità e i tempi di risposta e gestione di ad eventuali incidenti che hanno impatto sul servizio offerto. SLI previsti: SLI13, SLI14, SLI15, SLI16	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RS18	Deve essere sempre attivo un sistema di monitoraggio e di alerting relativo a possibili incidenti di sicurezza e/o di violazioni delle policy. Questo sistema deve prevedere la pronta applicazione delle necessarie contromisure in maniera automatica e/o tramite l'intervento di un operatore.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RS19	Le informazioni relative alle problematiche occorse devono essere registrate, insieme alle attività poste in essere per rimediarvi, e devono essere messe a disposizione degli acquirenti dei servizi.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RS20	Qualora le risorse IaaS/PasS, i dati e/o i software ospitati, oppure le loro configurazioni dovessero risultare alterati o utilizzati impropriamente a seguito di un incidente di sicurezza occorre mettere in atto le opportune attività di security assessment and audit prima di porre il servizio nuovamente in esercizio, al fine di valutare lo stato complessivo della sicurezza e la possibilità di procedere con l'utilizzo del servizio in modo protetto e sicuro.	Dichiarazione Fornitore SaaS

Continued on next page

Tabella 2.5 – continued from previous page

Codice Requisito	Requisito	Elementi di riscontro
RS21	Il Fornitore SaaS deve documentare le attività sulle patch di sicurezza applicate, relative a aggiornamenti del software, alle procedure e politiche di sicurezza, rendendo disponibile tale documentazione agli acquirenti dei servizi per la consultazione.	Dichiarazione Fornitore SaaS Verifica documentale

2.2.9 Performance e scalabilità

Il Fornitore SaaS è tenuto a dichiarare prima la qualità e l'affidabilità del servizio offerto durante tutto il ciclo di vita della soluzione SaaS. Le pattuizioni relative alla qualità del servizio costituiscono parte integrante del contratto di fornitura, all'interno del quale deve essere ricompresa una specifica sezione relativa ai "livelli di servizio garantiti" ovvero al Service Level Agreement (SLA).

Gli accordi relativi ai *livelli di servizio garantiti* (SLA) devono essere 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). Il Fornitore SaaS si impegna a rispettare gli obietti inoltre a monitorare costantemente tali indicatori e a fornire all'Acquirente l'accesso ad opportuni strumenti di monitoraggio.

La sezione del contratto di fornitura relativa ai *livelli di servizio garantiti* deve includere le *penali compensative* che il Fornitore SaaS dovrà corrispondere 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 devono essere inclusi nel contratto ed essere allineati ai valori e alle condizioni di mercato riscontrabili per servizi analoghi o appartenenti alla medesima categoria.

Inoltre, per quanto concerne i livelli di servizio garantiti (SLA) nel loro complesso, devono essere osservate le seguenti prescrizioni:

- 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 deve produrre e inviare al consumatore 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 deve implementare delle politiche e dei piani operativi per garantire la continuità del servizio (business continuity). Inoltre deve gestire tempestivamente il ripristino dell'operatività del servizio in seguito ad eventi catastrofici o imprevisti (disaster recovery).

Il Fornitore SaaS deve dichiarare 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 deve specificare e garantire quali sono le condizioni e i tempi di attivazione delle istanze aggiuntive.

Codice Requisito	Requisito	Elementi di riscontro
Disponibilità e continuità del servizio		
RPS1	La disponibilità del servizio è adeguata all'utilizzo previsto e corrispondente a quella dichiarata dal Fornitore SaaS. Il Fornitore SaaS deve assicurare la disponibilità e fruibilità del servizio nella sua interezza: non possono esserci parti di servizio non disponibili o non utilizzabili appieno. SLI previsto: SLI01	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RPS2	Devono essere presenti funzionalità automatiche e su richiesta di backup e ripristino dei dati e delle configurazioni software. SLI previsti: SLI17, SLI18, SLI19	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RPS3	Il Fornitore SaaS deve disporre di un piano di continuità operativa (business continuity) in cui sono previste azioni orientate al ripristino dell'operatività del servizio (disaster recovery) al verificarsi di eventi catastrofici/imprevisti. Il piano di ripristino raccoglie tutte le procedure necessarie al ripristino del servizio e dei dati ad esso relativi.	Dichiarazione Fornitore SaaS Verifica documentale
RPS4	Il Fornitore SaaS deve descrivere il comportamento della soluzione SaaS nell'eventualità di un evento catastrofico, fornendo una valutazione del rischio relativamente ai seguenti eventi: perdita o inconsistenze di dati alterazioni o non accessibilità di dati perdita delle transazioni perdita delle chiavi crittografiche per decifrare i dati impossibilità di ripristinare il servizio da un backup precedente impossibilità di operare il servizio nella sua pienezza	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
Tempi di risposta del servizio		
RPS5	I tempi di risposta del servizio sono corrispondenti a quelli dichiarati dal Fornitore SaaS e non sono presenti scostamenti significativi, e comunque entro precisi limiti prevedibili e noti a priori, al variare del numero di utenti connessi e del carico di lavoro sottoposto al servizio.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
Capacità di elaborazione		
RPS6	Le capacità di elaborazione e di evadere completamente le richieste sottoposte dagli utilizzatori al servizio devono essere adeguate all'utilizzo previsto per la soluzione SaaS e corrispondenti a quelle dichiarate dal Fornitore SaaS.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RPS7	Nel caso di servizio dispiegato in configurazione multitenant, la capacità di elaborazione deve mantenersi inalterata (o comunque entro precisi limiti prevedibili e noti a priori) al variare del numero di tenant attivi.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
Scalabilità del servizio		
RPS9	Il Fornitore SaaS deve dichiarare quali sono le condizioni massime di carico sopportabili dal servizio sia in termini di numero di utenti concorrenti e/o numero di richieste processabili (oppure volume di dati processabili).	Dichiarazione Fornitore SaaS

Continued on next page

Tabella 2.6 – continued from previous page

Codice Requisito	Requisito	Elementi di riscontro
RPS10	Nel caso in cui sia prevista la scalabilità automatica della soluzione SaaS, il Fornitore SaaS deve specificare e garantire quali siano le condizioni e i tempi di attivazione delle istanze aggiuntive che vengono attivate per sopportare i maggiori carichi. SLI previsti: SLI06	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RPS11	La scalabilità automatica o semi-automatica del servizio deve attivarsi correttamente al verificarsi delle condizioni operative prestabilite e deve garantire che non si verifichino interruzioni apprezzabili nell'erogazione del servizio.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RPS12	I precedenti requisiti di scalabilità devono essere garantiti sia nel caso di scalabilità crescente che nel caso di decrescita delle risorse allocate. In particolare in fase di decrescita le istanze SaaS/PaaS/IaaS non più necessarie devono risultare correttamente disattivate in modo da non comportare costi di utilizzo.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
Performance dei dispositivi client		
RPS13	I requisiti di performance precedenti devono valere per tutti i tipi di dispositivi client supportati (PC, tablet, mobile, ecc.).	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)

Dettaglio degli indicatori dei livelli di servizio garantiti:

Codice SLI	Indicatore	Descrizione
SLI01	Nome: Availability Origine: ISO/IEC 19086-1 / 19086-2	La disponibilità può essere calcolata come il tempo totale su un insieme di intervalli temporali definiti meno il tempo di inattività totale.
SLI13	Nome: Time to Service recovery Origine: ISO/IEC 19086-1	Il tempo che intercorre tra l'interruzione del servizio e il suo ripristino.
SLI14	Nome: Mean Time to Service recovery Origine: ISO/IEC 19086-1	Il valore medio su un determinato periodo di tempo di una serie di valori "Time to Service recovery"
SLI15	Nome: Maximum Time to Service recovery Origine: ISO/IEC 19086-1	Il valore massimo su un determinato periodo di tempo di una serie di valori "Time to Service recovery"
SLI16	Nome: Numero di Service Failures Origine: ISO/IEC 19086-1	Il numero totale di interruzioni di servizio su un arco temporale.
SLI05	Nome: Service Bandwidth Origine: ISO/IEC 19086-1	La quantità di dati che possono essere trasferiti in un determinato periodo di tempo.
SLI06	Nome: Elasticity speed Origine: ISO/IEC 19086-1	Questa quantità descrive quanto velocemente reagisce il servizio alla richiesta di nuove risorse.
SLI07	Nome: Data retention period Origine: ISO/IEC 19086-1	Il periodo di tempo in cui i dati del cliente vengono mantenuti dopo la notifica di cessazione del servizio.
SLI08	Nome: Log retention period Origine: ISO/IEC 19086-1	l periodo di tempo in cui i file di log relativi al servizio vengono conservati dopo la notifica di cessazione del servizio.
SLI09	Nome: Support hours Origine: ISO/IEC 19086-1	Le ore di funzionamento per ogni piano di supporto.

Continued on next page

Tabella 2.7 – continued from previous page

Codice SLI	Indicatore	Descrizione
SLI10	Nome: Service Incident Support hours Origine: ISO/IEC 19086-1	Le ore durante le quali il cliente può ottenere supporto specificamente per incidenti legati al servizio.
SLI11	Nome: Maximum First Support Response Time Origine: ISO/IEC 19086-1	Il tempo massimo tra la segnalazione del cliente e la risposta iniziale del fornitore.
SLI12	Nome: Maximum Incident Resolution Time Origine: ISO/IEC 19086-1	Il tempo massimo per risolvere un incidente
SLI17	Nome: Backup Interval Origine: ISO/IEC 19086-1	Il tempo che intercorre tra un backup e l'altro
SLI18	Nome: Retention period of backup data Origine: ISO/IEC 19086-1	Il periodo di tempo in cui vengono mantenuti i backup da parte del fornitore
SLI19	Nome: Backup restoration testing Origine: ISO/IEC 19086-1	Il numero di test di restore eseguiti durante un determinato periodo di tempo.
SLI20	Nome: Recovery Time Objective Origine: ISO/IEC 19086-1	Il tempo massimo necessario a ripristinare completamente il servizio dopo un'interruzione

2.2.10 Interoperabilità e portabilità

Le soluzioni 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 le soluzioni SaaS devo 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.

Il Fornitore SaaS deve dichiarare se la soluzione SaaS è interoperabile con i servizi pubblici SPID e PagoPA.

Deve essere sempre possibile la migrazione dell'Acquirente verso un altro Fornitore SaaS con conseguente eliminazione permanentemente dei dati di proprietà dell'Ente al termine della procedura di migrazione. In aggiunta, per quanto coerente con la piattaforma Cloud su cui sarà dispiegato il servizio, il Fornitore SaaS dovrà garantire che la portabilità della soluzione SaaS (o reversibilità) sia conforme con i criteri e gli scenari delineati nel documento "Piattaforma SPC Cloud e Reversibilità" (disponibile online all'indirizzo https://www.cloudspc.it/files/pdf/SPC-Cloud-Reversibility-signed.pdf). Inoltre, il Fornitore SaaS dovrà predisporre e consegnare all'Acquirente un dettagliato *piano di reversibilità*.

La proprietà dei dati deve essere mantenuta dall'Acquirente durante tutto il ciclo di vita del servizio, anche in seguito ad operazioni di acquisizione o fallimento del fornitore.

Codice Requisito	Requisito	Elementi di riscontro
Interoperabilità del servizio		
RIP1	La soluzione SaaS deve esporre opportune Application Programming Interface (API) di tipo SOAP e/o REST associate alle funzionalità applicative, di gestione e configurazione del servizio.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RIP2	Il Fornitore SaaS deve rendere disponibile una adeguata documentazione tecnica delle API che ne chiarisca l'utilizzo.	Dichiarazione Fornitore SaaS Verifica documentale

Continued on next page

Tabella 2.8 – continued from previous page

Codice Requisito	Requisito	Elementi di riscontro
RIP3	In caso di aggiornamento delle funzionalità del servizio e/o delle relative API deve essere possibile 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.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RIP4	Devono essere implementate delle limitazioni sul numero di richieste che è possibile sottomettere alle API, collegate alle caratteristiche delle API stesse e della classe di utilizzatori (throttling).	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RIP5	Deve essere implementata la tracciabilità delle richieste SOAP/REST ricevute e del loro esito (logging e accounting), anche al fine della non ripudiabilità della comunicazione.	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RIP6	Il Fornitore SaaS deve dichiarare se la soluzione SaaS è interoperabile con i servizi pubblici SPID e PagoPA. La dichiarazione di compatibilità con tali servizi può essere rilasciata solo se il Fornitore SaaS ha già superato le eventuali verifiche tecniche previste dalle normative e/o linee guida in vigore per tali servizi pubblici.	Dichiarazione Fornitore SaaS
Portabilità del servizio e dei dati		
RIP7	Deve essere sempre possibile da parte dell'Acquirente, su richiesta oppure in modalità self-service, l'estrazione di una copia completa dei dati memorizzati e gestiti dal servizio (in formato standard, non proprietario e riutilizzabile), ivi compresi i dati derivati quali log e statistiche di utilizzo, nonché le configurazioni del servizio. Tali prerogative devono essere garantite per un periodo di almeno due mesi (phase out) a partire dalla cessazione della fornitura (anche nel caso in cui la cessazione sia stata determinata dalla revoca della qualifica da parte di AgID). SLI previsti: SLI07 e SLI08	Dichiarazione Fornitore SaaS Verifica tecnica (se prevista)
RIP8	Deve essere sempre possibile la migrazione dei dati del servizio verso un altro Fornitore SaaS con conseguente eliminazione permanente dei dati di proprietà dell'Acquirente al termine della procedura di migrazione (inclusi i dati derivati e i dati di backup).	Dichiarazione Fornitore SaaS
RIP9	La proprietà dei dati deve essere mantenuta dall'Acquirente anche in seguito ad operazioni di acquisizione o fallimento del Fornitore SaaS. In caso di fallimento, chiusura dell'attività o dismissione del servizio, il Fornitore SaaS deve garantire all'Acquirente di poter recuperare i dati (in formato standard, non proprietario e riutilizzabile) e di poter migrare il servizio. Il periodo di tempo a disposizione dell'Acquirente dovrà consentirgli di completare il recupero dei dati e la migrazione del servizio e non potrà comunque essere inferiore a due mesi. SLI previsti: SLI07 e SLI08	Dichiarazione Fornitore SaaS

Continued on next page

Tabella 2.8 – continued from previous page

Codice Requisito	Requisito	Elementi di riscontro
RIP10	Il Fornitore SaaS deve predisporre un dettagliato piano di reversibilità, contenente le procedure e le modalità per migrare il servizio SaaS e tutti i dati pertinenti (anche derivati).	Dichiarazione Fornitore SaaS Verifica documentale

2.2.11 Conformità legislativa

In funzione del dominio applicativo in cui la soluzione SaaS si colloca, essa dovrà risultare conforme a tutte le normative e i regolamenti del settore, relativamente ai dati trattati e alle funzionalità implementate (ad esempio, settore sanitario, settore bancario, ecc.). In aggiunta, devono essere 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.

Nello specifico, il Fornitore SaaS dovrà mettere a disposizione dell'Acquirente tutti gli strumenti necessari per consentirgli di essere conforme alla legislazione corrente.

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 per la conformità legislativa:

Codice Requisito	Requisito	Tipo di verifica
Riservatezza dei dati		
RCL1	Tutti i dati trattati e memorizzati dal servizio devono sottostare ai regolamenti e alle normative vigenti in materia di trattamento e riservatezza dei dati (D.Lgs. n. 196 del 2003, detto Testo unico sulla Privacy).	Dichiarazione Fornitore SaaS
RCL2	Se nell'ambito delle attività della soluzione SaaS è previsto il trattamento di dati sensibili dei dipendenti dell'amministrazione e/o dei cittadini devono essere implementate le procedure e le funzioni opportune per consentire all'Acquirente di espletare tutte le incombenze e obbligazioni che da ciò ne derivano (ad es. consultazione da parte dell'interessato, cancellazione, ecc.).	Dichiarazione Fornitore SaaS
RCL3	Il Fornitore SaaS deve indicare per quali aspetti la soluzione SaaS proposta è conforme agli obblighi e agli adempimenti previsti dal GDPR (General Data Protection Regulation- Regolamento UE 2016/679).	Dichiarazione Fornitore SaaS
RCL4	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 SaaS e/o all'interno dei quali transiteranno anche temporaneamente i dati gestiti dal servizio (ivi compresi i siti di disaster recovery e di backup).	Dichiarazione Fornitore SaaS
RCL5	Il Fornitore SaaS, nei casi applicabili, dichiara la conformità ad accordi bilaterali (Privacy Shield EU-USA ecc.) volti alla salvaguardia dei dati elaborati, conservati ed a vario titolo gestiti per erogare il servizio.	Dichiarazione Fornitore SaaS

Continued on next page

Tabella 2.9 – continued from previous page

Codice Requisito	Requisito	Tipo di verifica
Normative specifiche per il settore di attività		
RCL6	Qualora siano previste delle norme derivanti da leggi o regolamenti specifici per il settore di attività in cui si colloca il servizio SaaS, il Fornitore SaaS deve garantire la conformità a tutti gli adempimenti e gli obblighi che ne conseguono e/o sono funzionali alla sua erogazione ed utilizzo da parte dell'Acquirente.	Dichiarazione Fornitore SaaS

2.2.12 Livelli della qualificazione SaaS

Sono previsti tre differenti livelli di qualificazione denominati L1, L2 e L3. Tutti i servizi che ottengono la qualificazione SaaS devono soddisfare obbligatoriamente tutti i requisiti di cui alla colonna L1 del seguente prospetto. Qualora soddisfino anche tutti o parte dei requisiti L2 e/o L3 potranno ottenere un differente livello di qualificazione corrispondente. All'interno della sezione dedicata del catalogo MePA sarà possibile consultare il dettaglio dei requisiti opzionali che i servizi SaaS soddisfano, in modo tale che gli acquirenti siano messi in grado di selezionare i servizi che meglio si adattano alle proprie particolari esigenze.

	Bronze (oppure L1)	Silver (oppure L2)	Gold (oppure L3)
Preliminari	X	X	X
Organizzativi	X	X	X
Sicurezza	X	X	X
Interoperabilità (da RIP1 a RIP6)	X	X	X
Portabilità (da RIP7 a RIP10)	X	X	X
Conformità Legislativa	X	X	X
Performance (da RPS1 a RPS8)	X	X	X
Scalabilità (da RPS9 a RPS13)		X	X
Multi-tenancy			X

2.2.13 Appendice 1 - Impegni contrattuali

Nella tabella che segue si riepilogano i requisiti dai quali scaturiscono specifici impegni contrattuali e adempimenti formali che dovranno governare il rapporto di fornitura tra Fornitore SaaS e Acquirente SaaS. Per rispettare appieno i requisiti di qualificazione di cui al presente allegato, le clausole contrattuali presenti nei contratti di fornitura dovranno essere conformi ai principi e agli impegni di seguito richiamati.

Clausola	Requisiti	Adempimenti aggiuntivi
CL1	RP7 – Dichiarazione del fornitore che si impegna ad operare come amministratore dell'infrastruttura IaaS/PaaS utilizzata. Deve essere indicata l'infrastruttura che si utilizza. Nel caso in cui il Fornitore SaaS utilizzi delle risorse IaaS/PaaS acquisite da un Cloud pubblico gestito da un CSP qualificato, oppure acquisite tramite Cloud SPC Lotto 1	Documento formale allegato al contratto

Continued on next page

Tabella 2.10 – continued from previous page

Clausola	Requisiti	Adempimenti aggiuntivi
CL2	RO3 – Monitoraggio del contesto tecnologico e implementazione di migliorie del servizio RO4 – Aggiornamenti del software che non introducono problemi e vulnerabilità RO5 – Comunicazione tempestiva di aggiornamenti e modifiche al servizio RO6 – Aggiornamento tempestivo della documentazione e della manualistica	
CL3	RO7 – Livelli di servizio garantiti relativi a disponibilità e performance RO8 – Livelli di servizio garantiti relativamente alla gestione degli incidenti di sicurezza RO9 – Livelli di servizio garantiti relativamente alla gestione delle richieste di assistenza	
CL4	RO10 – Accesso a strumenti di monitoraggio e di logging opportunamente documentato	
CL5	RO11 – Monitoraggio in tempo reale delle risorse utilizzate e dei costi imputati	
CL6	RS1 – Sicurezza del codice applicativo RS2 – Verifiche di sicurezza preliminari e periodiche del codice binario e dei sorgenti RS3 – Garanzia di sicurezza dell'intera supply chain della soluzione SaaS RS4 – Controlli periodici sulle componenti software di terze parti	
CL7	RS10 – Gestione in sicurezza delle chiavi e dei codici di accesso RS11 – Gestione in sicurezza delle risorse Cloud utilizzate per erogare il servizio RS12 – Impedire l'accesso ai dati di altri utenti (ambiente multi-tenant)	
CL8	RS19 – Registrazione delle informazioni sugli incidenti di sicurezza e sui rimedi attuati RS20 – Attività di security assessment and audit prima di porre il servizio nuovamente in esercizio in seguito ad incidente di sicurezza RS21 – Documentare le patch di sicurezza applicate, gli aggiornamenti del software e le procedure e politiche di sicurezza	
CL9	RPS3 – Piano di continuità operativa	Documento tecnico facente parte della fornitura
CL10	RPS4 – Responsabilità del Fornitore SaaS nel caso di perdita o inconsistenza dei dati a seguito di ripristino da un evento catastrofico o a seguito di migrazione del servizio per altri motivi	
CL11	RPS5 – Tempi di risposta del servizio che non subiscono fluttuazioni al di fuori degli intervalli dichiarati, al variare del numero di utenti e del carico di lavoro.	Scheda tecnica servizio SaaS

Continued on next page

Tabella 2.10 – continued from previous page

Clausola	Requisiti	Adempimenti aggiuntivi
CL12	RPS7 – Capacità di processamento del servizio che non subisce fluttuazioni al di fuori degli intervalli dichiarati, al variare del numero di utenti e del carico di lavoro. RPS8 – Capacità di processamento del servizio che non subisce fluttuazioni al di fuori degli intervalli dichiarati, al variare del numero di tenant attivi (nel caso di configurazione multi-tenant)	
CL13	RPS9 – Condizioni massime di esercizio del servizio RPS10 – Tempi di attivazione delle istanze RPS11 – Scalabilità automatica del servizio RPS12 – Scalabilità decrescente accurata	Scheda tecnica servizio SaaS
CL14	RPS13 – Performance garantite per tutti i tipi di dispositivi client supportati	
CL15	RIP1 – Presenza API di tipo SOAP/REST RIP2 – Documentazione tecnica API RIP3 – Versioning delle API RIP4 – Limitazioni volumetriche per l'utilizzo delle API RIP5 – Tracciabilità delle richieste SOAP/REST	Documento tecnico facente parte della fornitura
CL16	RIP6 – Possibilità di estrarre i dati gestiti dal servizio in qualsiasi momento, anche dopo il termine della fornitura (periodo di phase-out di almeno due mesi) RIP7 – Migrazione dei dati del servizio (reversibilità) RIP8 – Garanzie sulla proprietà e disponibilità dei dati in caso di fallimento/acquisizione del Fornitore SaaS	
CL17	RIP9 – Piano di reversibilità	Documento tecnico facente parte della fornitura
CL18	RCL1 – Trattamento dei dati conforme al Testo unico sulla Privacy RCL2 – Adempimenti derivanti dal trattamento di dati sensibili	
CL19	RCL3 – Ambiti conformi al regolamento GDPR	
CL20	RCL4 – Comunicazione degli eventuali stati esteri in cui risiedono i/il data center attraverso cui si eroga il servizio	
CL21	RCL5 – Conformità a tutte le normative specifiche per il settore di attività	

2.2.14 Appendice 2 - Scheda tecnica del Servizio SaaS

La seguente scheda tecnica è esemplificativa. Il formato definitivo sarà disponibile sulla piattaforma dedicata di qualificazione.

Scheda tecnica del Servizio SaaS	
Nome del servizio	
Descrizione generale	
Max 800 caratteri	
Elenco delle caratteristiche funzionali e dei benefici	
10 + 5 punti elenco	

Continued on next page

Tabella 2.11 – continued from previous page

Scheda tecnica del Servizio SaaS	
Ambito di applicazione	
Enti destinatari del servizio	
Cloud deployment model	Public/Private/Hybrid
Cloud platform	Openstack/Amazon AWS/Microsoft Azure/Google Cloud/IBM Bluemix/. . . ..
Single tenant/Multi tenant	
Software e Servizi correlati	
Dipendenze e prerequisiti	
Supporto Clienti	
e-mail	
Online ticketing	
Telefono	
Web chat	
Disponibilità del supporto clienti (giorni/orari)	
Tempi di risposta e di risoluzione garantiti	
Assistenza on site	(descrivere se prevista)
Assistenza remota	(descrivere se prevista)
Attivazione e disattivazione del servizio	
Tempi di attivazione	
Processo di attivazione	
Processo di disattivazione	
Estrazione dei dati a seguito di disattivazione	
Formati in cui i dati saranno disponibili	
Piattaforme abilitanti	PagoPAi: Si/No SPID: Si/No Altro: (elenco di eventuali altre piattaforme abilitanti rispetto alle quali il servizio è compatibile)
Reti sulle quali è fruibile il servizio:	
Rete SPC	Si/No
GARR	Si/No
Internet	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	
Documentazione	
API	URL: Autenticazione: Altro:
Funzionalità invocabili tramite API e funzionalità che non sono accessibili via API	
Documentazione delle API	URL Web: PDF:
Presenza 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)

Continued on next page

Tabella 2.11 – continued from previous page

Scheda tecnica del Servizio SaaS	
Metriche e statistiche di utilizzo	
Metriche disponibili	
Statistiche disponibili	
Report disponibili	
Conformità legislativa	
Localizzazione dei data centers	Italia/EU/Extra EU Elenco nazioni estere
Adempimenti Testo unico Privacy	Si/No
Conformità GDPR	Si/No Tempistiche di adeguamento previste
Portabilità dei dati del servizio	
Dati esportabili	
Formati dei dati esportabili	
Dati derivati (configurazioni, template, log, ecc.)	
Livelli di servizio garantiti	
Disponibilità di monitoraggio in tempo reale dello stato del servizio	Si/No
Disponibilità di notifiche via SMS/email degli eventi di indisponibilità del servizio	Si/No
Elenco degli SLA garantiti	L'elenco contiene gli indicatori SLI e gli obiettivi SLO previsti dalla Tabella XYZ rispetto ai quali il Fornitore SaaS si impegna a fornire delle garanzie contrattuali Possono essere previsti SLA aggiuntivi non rientranti nella tabella.
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	
Approcci utilizzati per la protezione dei dati in transito nelle reti interne	
Meccanismi di autenticazione degli utenti supportati	
Possibilità di configurazione/ customizzazione dei meccanismi di autenticazione	Si/No (eventuale descrizione)
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

Continued on next page

Tabella 2.11 – continued from previous page

Scheda tecnica del Servizio SaaS	
Standard e certificazioni	
Elenco standard	
Elenco certificazioni possedute	
Prezzi e imputazione dei costi	
Prezzo del servizio	
Unità di misura	
Altre condizioni	

2.3 Archivio dei commenti alla circolare «Qualificazione Servizi SaaS per il Cloud della PA»

2.3.1 Archivio dei commenti a «Criteri per la qualificazione di servizi SaaS per il Cloud della PA»

In questa sezione è presente l'archivio dei commenti alla Circolare «Qualificazione Servizi SaaS per il Cloud della PA» pubblicati in precedenza.

Abbiamo migliorato il sistema dei commenti: la discussione ora continua su Forum Italia.

2.3.2 Archivio dei commenti a «Requisiti per la qualificazione di servizi SaaS per il Cloud della PA»

In questa sezione è presente l'archivio dei commenti all'allegato della Circolare SaaS pubblicati in precedenza.

Abbiamo migliorato il sistema dei commenti: la discussione ora continua su Forum Italia.

Nota: Circolare in consultazione pubblica fino al 01/03/2018

CAPITOLO 3

Cloud Service Provider

Nota: Il documento rappresenta lo schema della Circolare AgID sui «Criteri per la qualificazione dei Cloud Service Provider per la PA». Lo schema della circolare è in consultazione e aperto ai commenti fino **al 1 Marzo 2018**.

Nota: Inserisci il tuo contributo: scegli l'argomento cliccando su una delle voci dell'indice e inserisci i tuoi commenti usando il link apposito.

CIRCOLARE N. XX del YY gennaio 2018

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

3.1.1 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 per l'inserimento dei CSP tra i soggetti 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/PaaS erogati da Cloud SPC, dai PSN e dai CSP qualificati ai sensi di quanto disposto da questa Circolare.).

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 Cloud Service Provider nell'ambito della strategia di evoluzione del modello *Cloud della PA*.

Tale procedura consentirà alle Amministrazioni di utilizzare, nell'ambito del *Cloud della PA*, soluzioni IaaS e PaaS fornite dai CSP qualificati o altresì servizi SaaS basati su tali soluzioni di cui alla Circolare n. XX del YYY "Criteri per la qualificazione di servizi SaaS per il *Cloud della PA"*.

A tale scopo verrà realizzato il catalogo dei CSP qualificati da AgID per l'acquisizione di soluzioni IaaS e PaaS da parte della PA mediante gli strumenti del mercato elettronico, convenzioni, accordi quadro, secondo quanto previsto nelle *Disposizioni per il procurement dei servizi IaaS, PaaS e SaaS per il Cloud della PA*, che saranno redatte da CONSIP.

3.1.2 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)
CSP	Cloud Service Provider, fornitore di servizi Cloud
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 CSP, Fornitore	Soggetto richiedente la qualificazione CSP
Giorni	Giorni solari
Marketplace Cloud	Piattaforma digitale che permette la selezione e l'acquisto di servizi IaaS e PaaS offerti dai CSP qualificati da AgID ai sensi della presente Circolare, nonchè i servizi SaaS qualificati ai sensi della Circolare AgID "Criteri per la qualificazione di 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.

Continued on next page

Tabella 3.1 – continued from previous page

Software as a Service, SaaS	Tra i modelli di servizio offerti dalle piattaforme di Cloud computing, il Software as a Service (SaaS) è il servizio fully-managed in cui il gestore del servizio si occupa della predisposizione, configurazione, messa in esercizio e manutenzione dello stesso, lasciando al fruitore del servizio il solo ruolo di utilizzatore delle funzionalità offerte e che, quindi, non senza oneri di gestione, gestisce o controlla l'infrastruttura cloud necessaria all'erogazione del servizio sottostante.
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.
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).
PagoPA	Sistema di pagamenti elettronici verso la Pubblica Amministrazione.
SLI	Service Level Indicator, una misura quantitativa definita di un determinato aspetto del livello di 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 dei Cloud Service Provider pubblici per la "PA".
MePA	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.

3.1.3 Articolo 1 - Ambito di applicazione

La presente circolare definisce i requisiti di qualificazione per i fornitori Cloud Privati, nonché la relativa procedura di qualificazione e si applica a tutti i fornitori Cloud privati che hanno interesse a proporre servizi Cloud in modalità IaaS, PaaS alle Pubbliche amministrazioni, ai sensi di quanto disposto dal Piano Triennale.

3.1.4 Articolo 2 – Il processo di qualificazione

I soggetti interessati ad offrire servizi Cloud per la PA devono seguire uno specifico processo di qualificazione, articolato in tre fasi.

È possibile che il soggetto richiedente sia:

1. un fornitore privato di soluzioni Cloud che intende ottenere da AgID la qualificazione per erogare servizi di tipo Public Cloud (IaaS o PaaS) per la PA;
2. un fornitore privato di soluzioni Cloud SaaS che intende ottenere da AgID la qualificazione delle proprie soluzioni SaaS ai sensi della Circolare AgID "Criteri per la qualificazione di servizi SaaS per il *Cloud della PA"* per erogare servizi sfruttando la propria infrastruttura Cloud.

Nella tabella successiva sono riportati tutti gli attori coinvolti nel processo di qualificazione ed il loro ruolo in termini di responsabilità (RACI). Negli articoli seguenti sono previste le eccezioni di processo, in relazione alle fasi ed ai casi sopra elencati.

N.	Fasi del processo di qualificazione	Soggetto	AgID	CONSIP	Clienti (PA)
1	Richiesta di qualificazione	R, A	I	I	O
2	Istruttoria documentale	I	R, A	C	O
3	Mantenimento della qualificazione (Monitoraggio)	C	R, A	C	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 della *piattaforma AgID dedicata* alla gestione del workflow di cui all'articolo 2 della Circolare AgID "Criteri per la qualificazione di servizi SaaS per il *Cloud della PA"* 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 anche mediante la sottomissione di un'unica richiesta valida sia ai fini della presente Circolare sia ai fini della richiesta di cui alla Circolare AgID "Criteri per la qualificazione di servizi SaaS per il *Cloud della PA*. Le modalità operative di trasmissione saranno definite in apposita comunicazione pubblicata sul sito AgID.

3.1.5 Articolo 3 - Criteri di ammissibilità e requisiti della qualificazione

La richiesta di qualificazione è ammissibile, se all'atto della presentazione della richiesta di qualificazione, il fornitore privato è abilitato da Consip sui propri sistemi d'acquisto.

I requisiti per la qualificazione si suddividono in:

1. Requisiti preliminari;
2. Requisiti organizzativi;
3. Requisiti specifici.

Il dettaglio di tali requisiti 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.

3.1.6 Articolo 4 - Fasi del processo di qualificazione.

3.1.6.1 Fase 1 - Richiesta di qualificazione

Il soggetto interessato alla qualificazione CSP provvede ad inserire sulla *piattaforma AgID dedicata* apposita richiesta, fornendo le informazioni e la documentazione relativa sia ai criteri di ammissibilità sia al possesso dei requisiti di cui all'allegato "A" alla presente Circolare.

All'atto della presentazione della richiesta di qualificazione CSP, il soggetto richiedente dovrà dichiarare che, conseguita la qualificazione, si impegna a rispettare, in maniera integrale e incondizionata, senza eccezione, deroga o riserva alcuna, per tutta la durata dei contratti di fornitura stipulati con le Amministrazioni clienti, quanto previsto all'appendice 1 dell'Allegato "A" alla presente Circolare.

Il soggetto richiedente dovrà altresì dichiarare che si impegna ad accettare nei contratti con le Amministrazioni clienti la clausola di risoluzione anticipata in caso di revoca della qualificazione da parte di AgID ed a sottoporsi a qualsiasi verifica che l'Agenzia potrà disporre a garanzia del rispetto degli impegni assunti e del mantenimento dei requisiti e dei criteri di ammissibilità richiesti.

3.1.6.2 Fase 2 - Istruttoria documentale

La fase istruttoria inizia con la verifica preliminare delle informazioni e della documentazione fornita dai soggetti richiedenti, relative al possesso del criterio di ammissibilità di cui all'articolo 3 della presente Circolare.

L'eventuale esito negativo di tale verifica preliminare viene notificato telematicamente da AgID al soggetto interessato, secondo le modalità operative di trasmissione definite in apposita comunicazione, entro 30 giorni dalla ricezione della richiesta di qualificazione. Il silenzio dell'Agenzia nel termine indicato equivale all'ammissione della richiesta di qualificazione per come proposta.

Per le richieste ammesse, AgID effettua la verifica delle informazioni e della documentazione fornita dai soggetti richiedenti rispetto ai requisiti di cui all'art.3, per come dettagliati all'Allegato "A" della presente Circolare.

L'esito della verifica potrà essere:

1. **Positivo**: la richiesta di qualificazione rispetta i requisiti oggetto di verifica;
2. **Negativo con riserva**: a seguito della verifica della documentazione e delle informazioni dichiarate dal soggetto, AgID trasmette l'esito negativo con riserva e contestuale richiesta di documentazione ed informazioni ad integrazione e completamento di quanto inserito nella *piattaforma AgID dedicata*. Il soggetto fornisce i documenti e le informazioni richieste dall'Agenzia entro 20 giorni dalla ricezione della richiesta, in caso contrario la richiesta di qualificazione si intenderà respinta. Qualora il soggetto richiedente abbia invece inviato nei termini i documenti e le informazioni richieste, l'Agenzia, previa verifica, comunica l'esito dell'istruttoria. (Positivo o Negativo);
3. **Negativo**: la richiesta di qualificazione è respinta. Il soggetto non può presentare una nuova richiesta se non siano cessate le cause che hanno determinato il mancato accoglimento della richiesta e comunque non prima di 90 giorni.

Il provvedimento avente per oggetto l'esito della verifica viene notificato telematicamente al soggetto interessato da AgID, in apposita comunicazione, entro 60 giorni dalla ricezione della richiesta. Nel caso di esito negativo con riserva, il termine di 60 giorni si intende interrotto.

3.1.6.3 Fase 3 – Mantenimento della qualificazione (Monitoraggio)

L'Agenzia verifica la persistenza del possesso dei criteri di ammissibilità e dei requisiti previsti per la qualificazione e di quanto dichiarato nel corso della procedura di qualificazione.

La verifica è svolta anche con l'esecuzione di attività ispettive e/o richieste di test da parte di AgID, o di soggetti terzi dalla stessa incaricati, anche su segnalazione formale all'Agenzia da parte delle Amministrazioni clienti/utenti.

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

L'Agenzia si riserva, inoltre, la facoltà di richiedere al soggetto ogni ulteriore documento correlato all'espletamento del processo di qualificazione, che consideri necessario per poter svolgere le previste attività di verifica. Le difformità riscontrate nel corso dell'attività di verifica sono comunicate al soggetto interessato con indicazione delle modalità e del termine per la loro risoluzione. 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.

3.1.7 Articolo 5 - Revoca della qualificazione

L'Agenzia dispone la revoca della qualificazione, con provvedimento motivato nel caso di:

- perdita del criterio di ammissibilità;
- mancato rispetto del termine assegnato, ove non sussistano adeguati motivi di proroga, per l'eliminazione delle difformità riscontrate;
- riscontro da parte dei competenti organi di violazioni di norme relative all'attività oggetto di qualificazione;
- mancata presentazione di una richiesta di rinnovo della qualificazione entro la scadenza dell'Attestato di qualificazione di cui all'art. 6 della presente Circolare. La richiesta di rinnovo della qualificazione equivale alla richiesta di qualificazione di cui alla Fase 1 dell'art. 4 della presente Circolare.

La revoca della qualificazione comporta l'eliminazione della soluzione dal marketplace Cloud.

La revoca della qualificazione sarà comunicata a Consip e a tutte le PA che abbiano stipulato contratti ancora attivi alla data del provvedimento di revoca da parte dell'Agenzia.

Nei casi di revoca, il soggetto interessato non può presentare una nuova richiesta di qualificazione all'Agenzia se non siano cessate le cause che hanno determinato la revoca, pena l'inammissibilità della richiesta.

3.1.8 Articolo 6 – Utilizzo della qualificazione

Ai soggetti che hanno ottenuto esito positivo dell'istruttoria, sarà rilasciato da AgID apposito "Attestato di Qualificazione di Fornitore di Public Cloud della PA". Tale attestato ha una validità temporale di 24 mesi dalla data di rilascio.

Tali soggetti potranno utilizzare la suddetta qualificazione nei propri rapporti commerciali con le pubbliche amministrazioni.

Consip provvede ad abilitare l'accesso agli strumenti del mercato elettronico/convenzioni/accordi quadro ai Cloud Service Provider qualificati da AgID.

3.1.9 Articolo 7 - Contributo per la procedura di qualificazione

Al fine del ristoro dei costi sostenuti dall'Agenzia, per ciascuna richiesta di qualificazione è dovuto il pagamento di un contributo. L'Agenzia determina entro il mese di aprile di ogni anno il valore del corrispettivo dovuto per ciascuna richiesta. Il mancato pagamento entro i termini prescritti dall'Agenzia, comporta il decadimento della richiesta presentata e/o la revoca della qualificazione.

3.1.10 Articolo 8 - Disposizioni transitorie e finali

La presente Circolare entra in vigore alla data di pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Le PA che intendono approvvigionarsi dei servizi IaaS e PaaS offerti dai CSP qualificati dall'Agenzia consultano il marketplace Cloud a partire dalla data di rilascio in esercizio della *piattaforma AgID dedicata *di cui all'art.2 della presente Circolare.

La data di attivazione della *piattaforma AgID dedicata* e del Marketplace Cloud sarà comunicata insieme alle modalità operative della procedura di qualificazione sul sito dell'Agenzia.

Nelle more dell'attivazione della *piattaforma AgID dedicata*, i soggetti che intendono avviare il processo di qualificazione possono inviare formale manifestazione d'interesse all'Agenzia, tramite posta elettronica certificata.

Le richieste di qualificazione pervenute nei 12 (dodici) mesi successivi alla pubblicazione nella Gazzetta Ufficiale della Repubblica italiana della presente Circolare non sono soggette al contributo di cui all'art.7.

3.1.11 Allegati

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

ALLEGATO B "Disposizioni per il procurement dei servizi IaaS, PaaS e SaaS per il *Cloud della PA*"

IL DIRETTORE GENERALE

Nota: Il documento rappresenta lo schema della Circolare AgID sui «Criteri per la qualificazione dei Cloud Service Provider per la PA». Lo schema della circolare è in consultazione e aperto ai commenti **fino al 1 Marzo 2018**.

Nota: Inserisci il tuo contributo: scegli l'argomento cliccando su una delle voci dell'indice e inserisci i tuoi commenti usando il link apposito.

Allegato alla CIRCOLARE N. XX del YY gennaio 2018

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

3.2.1 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 da Cloud SPC, dai PSN e dagli altri CSP che saranno qualificati come compatibili con i requisiti Cloud 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)

Continued on next page

Tabella 3.2 – continued from previous page

CSP	Cloud Service Provider, fornitore di servizi Cloud
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 richiedente la qualificazione CSP
Giorni	Giorni solari
Marketplace SaaS	Piattaforma digitale che permette la selezione e l'acquisto di applicazioni software erogate in Cloud secondo il modello Software-as-a-Service
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.
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.
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 del livello di 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 pubblici per la PA".

Continued on next page

Tabella 3.2 – continued from previous page

MePA	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.

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.

3.2.2 Introduzione

Il presente documento definisce nel dettaglio i requisiti, di cui all'art. 3 della Circolare, che il Fornitore Cloud e le soluzioni IaaS/PaaS da esso proposte 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 può includere uno o più servizi Cloud. 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).

Vengono qualificati quei Cloud Service Provider che intendono offrire alla Pubblica Amministrazione uno o più servizi Cloud appartenenti alle seguenti categorie:

- IaaS
- PaaS

La procedura di qualificazione inizia con la richiesta da parte del Fornitore Cloud o un suo Partner e procede per mezzo di verifiche amministrative e documentali descritte nel presente allegato.

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

- *Fornitore Cloud o CSP*, che fornisce, gestisce e amministra i servizi Cloud infrastrutturali di tipologia IaaS e/o PaaS, che sono oggetto della qualificazione;
- *Acquirente o CSC*, PA che acquisisce e/o utilizza i servizi Cloud in maniera diretta o indiretta mediante l'acquisto di soluzioni SaaS di terzi o dello stesso Fornitore Cloud.
- *Partner o CSN*, è un soggetto terzo che può svolgere attività di supporto e/o di consulenza per conto del CSP o del CSC. 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.

3.2.3 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 preliminari (RP),
- 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).

3.2.3.1 Tipologie di verifiche previste

Nelle sezioni che seguono sono definiti tutti i requisiti previsti per le soluzioni IaaS/PaaS secondo la classificazione sopra richiamata.

Le tipologie di verifiche previste sono:

- *Dichiarazione del Fornitore Cloud* - il cui accertamento consiste nell'acquisizione da parte di AgID di un atto formale nel quale il Fornitore Cloud (a seconda dei casi):
  - dichiara espressamente la sussistenza di quanto specificato nel requisito;
  - si assume l'obbligo di agire secondo quanto richiesto dal requisito al verificarsi di determinate condizioni.

  Nel caso in cui sia previsto un obbligo di agire, la verifica può consistere nell'accertare che l'obbligo sia stato riportato correttamente in uno o più atti formali (ad esempio, nel contratto di fornitura). Nel caso in cui sia richiesto di dichiarare informazioni puntuali e/o descrittive, la verifica consiste nell'acquisizione delle specifiche informazioni tramite compilazione da parte del Fornitore Cloud dei moduli di registrazione (form) presenti sulla piattaforma informatica che supporta il processo di qualificazione.
- *Verifica documentale* - il cui accertamento consiste nella verifica del possesso da parte del Fornitore Cloud di idonea documentazione comprovante il soddisfacimento del requisito. Durante la sottomissione della richiesta di qualificazione verrà espressamente richiesta la produzione di tale documentazione. La verifica documentale comprende anche il caso in cui al Fornitore Cloud sia richiesto di produrre una documentazione tecnica (manualistica, guida operativa, ecc.) o una certificazione tecnica da consegnare all'Acquirente nella fase di avvio della fornitura.

3.2.4 Requisiti preliminari

Al Fornitore Cloud viene richiesto di produrre la documentazione necessaria al fine di dimostrare:

- 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.

La tabella seguente riporta i requisiti preliminari e il tipo di verifica richiesta per ognuno di essi.

Codice Requisito	Requisito	Elementi di riscontro
Informazioni necessarie per l'istruttoria		
RP1	Produrre l'elenco dei servizi per i quali si richiede la qualificazione, fornendo le informazioni di dettaglio richieste nella "scheda tecnica del servizio" e negli ulteriori requisiti che prevedono una dichiarazione da parte del Fornitore.	Dichiarazione Fornitore Cloud

Continued on next page

Tabella 3.3 – continued from previous page

Esperienza del Fornitore Cloud nell'ambito dei servizi IaaS/PaaS		
RP2	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.	Dichiarazione Fornitore Cloud, Verifica documentale
RP3	Specificare il sistema e le procedure adottate per la gestione della qualità aziendale che vengono applicati anche ai servizi oggetto di qualificazione.	Dichiarazione Fornitore Cloud Verifica Documentale

3.2.5 Requisiti organizzativi

Per quanto concerne le soluzioni IaaS/PaaS oggetto di qualificazione, al Fornitore Cloud viene richiesto di produrre la documentazione necessaria al fine di dimostrare il possesso dei seguenti requisiti organizzativi,:

- 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 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 tutto il processo. Tali prerogative dovranno essere rese disponibili almeno attraverso:

- uno strumento (console o pannello) fruibile in modalità Web-based e con accesso sicuro;
- la disponibilità di API invocabili da remoto in modalità SOAP/REST.

Analoghi strumenti, possibilmente integrati con i precedenti e tra di loro, dovranno essere messi a disposizione al fine di consentire all'Acquirente il monitoraggio delle performance e dell'utilizzo delle risorse (compreso l'accesso ai log), nonché per la gestione amministrativa degli ordini e il controllo dei costi. Si vedano a tal proposito i requisiti RO11 e RO12.

La tabella seguente riporta i requisiti organizzativi e il tipo di verifica richiesta per ognuno di essi.

Codice Requisito	Requisito	Elementi di riscontro
Supporto clienti e assistenza tecnica		

Continued on next page

Tabella 3.4 – continued from previous page

RO1	Il Fornitore Cloud deve mettere a disposizione dell'Acquirente un servizio di supporto tecnico disponibile 24/7 e accessibile mediante opportuni e diversificati canali di comunicazione e adeguati sistemi di gestione (issue tracking), al fine di consentire all'Acquirente di effettuare le eventuali segnalazioni di malfunzionamenti e potenziali pericoli per la sicurezza e la fruibilità del servizio, in completa autonomia.	Dichiarazione Fornitore Cloud
RO2	Il Fornitore Cloud deve assicurare la massima trasparenza nella gestione delle segnalazioni, garantendo all'Acquirente piena 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. SLI previsti: SLI09, SLI10, SLI11, SLI12	Dichiarazione, Fornitore Cloud
RO3	I servizi proposti devono essere accompagnati dalla documentazione tecnica, dalle 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.	Dichiarazione Fornitore Cloud, Verifica documentale
Gestione del cambiamento (change management)		
RO4	Al fine di garantire che vengano utilizzate procedure e metodi standard per la gestione tempestiva ed efficiente di ogni cambiamento applicativo e di infrastruttura, il Fornitore Cloud deve garantire e dare evidenza del fatto che i servizi offerti siano sottoposti ad un ben definito processo di gestione del cambiamento. Quanto dichiarato deve essere coerente con le certificazioni e le best practises richieste in ambito della sicurezza (ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018)	Dichiarazione Fornitore Cloud, Verifica documentale
RO5	Il Fornitore Cloud deve garantire una comunicazione puntuale all'Acquirente dei cambiamenti e delle migliorie introdotti in seguito ad aggiornamenti apportati alle modalità di funzionamento e fruizione dei servizi Cloud erogati.	Dichiarazione Fornitore Cloud
RO6	Il Fornitore Cloud deve garantire che la documentazione tecnica sia prontamente aggiornata e resa disponibile in seguito ad aggiornamenti apportati ai servizi Cloud.	Dichiarazione Fornitore Cloud
Gestione della configurazione (configuration management)		
RO7	Il Fornitore Cloud deve garantire 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 (hardware e software) del servizio. Quanto dichiarato deve essere coerente con le certificazioni e le best practises richieste in ambito della sicurezza (ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018)	Dichiarazione Fornitore Cloud
Gestione degli Incidenti (incident & problem management)		

Continued on next page

Tabella 3.4 – continued from previous page

RO8	Il Fornitore Cloud deve garantire che la gestione degli incidenti avvenga mediante procedure standard coerenti con gli standard di sicurezza internazionali. (p.e. ISO/IEC 27002, ISO/IEC 27035). Quanto dichiarato deve essere coerente con le certificazioni e le best practises richieste in ambito della sicurezza (ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018)	Dichiarazione Fornitore Cloud
Best practice e trasparenza		
RO9	Il Fornitore Cloud nell'ambito del contratto con l'Acquirente deve dichiarare tutti i livelli di servizio offerti utilizzando le metriche descritte nella tabella degli indicatori per i livelli di servizio che trovano applicazione. I livelli di servizio devono essere espressi rispetto a parametri tecnici oggettivi e misurabili.	Dichiarazione Fornitore Cloud, Verifica documentale
RO10	Il Fornitore Cloud deve obbligatoriamente dichiarare i livelli di servizio garantiti per quanto riguarda la disponibilità del servizio, le performance e le tempistiche di gestione dei malfunzionamenti che possano compromettere l'utilizzabilità del servizio da parte dell'Acquirente. SLI previsti: SLI01, SLI12, SLI20	Dichiarazione Fornitore Cloud, Verifica documentale
RO11	Il Fornitore Cloud deve documentare e rendere disponibile l'accesso a strumenti di monitoraggio e di logging, filtrando e restringendo opportunamente i risultati agli eventi di interesse dell'Acquirente.	Dichiarazione Fornitore Cloud, Verifica documentale
RO12	Il calcolo dei costi imputati all'Acquirente deve essere trasparente e accurato, rispettare le condizioni contrattuali ed essere monitorabile dall'Acquirente in tempo reale. In aggiunta il Fornitore Cloud dovrà rendere disponibile all'Acquirente un set minimo di funzioni (API) che permettano di acquisire le informazioni sulle metriche di "billing".	Dichiarazione Fornitore Cloud

Il fornitore potrà dichiarare e documentare il possesso di ulteriori requisiti di tipo organizzativo e/o altre certificazioni tecniche che abbiano attinenza con i servizi Cloud sottoposti alla procedura di qualificazione.

3.2.6 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).

3.2.6.1 Sicurezza, Privacy e protezione dei dati

Di seguito è riportato il dettaglio dei requisiti di sicurezza, privacy e protezione dei dati e delle verifiche previste durante la procedura di qualificazione.

Codice Requisito	Requisito	Elementi di riscontro
RSI1	I servizi Cloud offerti devono essere certificati secondo lo standard ISO/IEC 27001.	Dichiarazione Fornitore Cloud, Verifica documentale
RSI2	Al fine di garantire adeguati livelli di sicurezza e riservatezza dei dati per i servizi Cloud della PA, il Fornitore Cloud deve rendere coerenti i servizi offerti alle best practices proposte dallo standard ISO/IEC 27017. (ISO/IEC 27017 è uno standard "auditabile", il certificato di conformità deve essere rilasciato da un ente terzo)	Dichiarazione Fornitore Cloud, Verifica documentale
RSI3	Al fine di garantire adeguati livelli di sicurezza e riservatezza dei dati per i servizi Cloud della PA, il Fornitore Cloud deve rendere coerenti i servizi offerti alle best practices proposte dallo standard ISO/IEC 27018. (ISO/IEC 27018 è uno standard "auditabile", il certificato di conformità deve essere rilasciato da un ente terzo)	Dichiarazione Fornitore Cloud, Verifica documentale

3.2.6.2 Performance

Il Fornitore Cloud è tenuto a definire la qualità e l'affidabilità del servizio durante tutto il suo ciclo di vita. Le pattuizioni relative alla qualità del servizio costituiscono parte integrante del contratto di fornitura, all'interno del quale deve essere compresa una specifica sezione relativa ai "livelli di servizio garantiti" ovvero il Service Level Agreement (SLA).

I livelli di servizio sono definiti dagli *indicatori del livello di servizio* (**SLI**), ovvero delle metriche che quantificano e/o qualificano alcune grandezze specifiche del servizio. Si definiscono invece *obiettivi del livello di servizio* (**SLO**) i valori (o intervalli) massimi e/o minimi degli indicatori (SLI) che si intendono come garantiti dal servizio.

Gli accordi contrattuali relativi ai *livelli di servizio* (**SLA**) vengono definiti tramite un'opportuna combinazione degli *obiettivi* (SLO) che il fornitore intende mantenere per ogni indicatore (SLI).

Il Fornitore Cloud si impegna a monitorare costantemente tali indicatori ed a fornire all'Acquirente l'accesso ad opportuni strumenti di monitoraggio.

La sezione del contratto di fornitura relativa ai *livelli di servizio garantiti* deve includere le *penali compensative* che il Fornitore Cloud dovrà corrispondere 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 devono essere inclusi nel contratto ed essere allineati ai valori e alle condizioni di mercato riscontrabili per servizi analoghi o appartenenti alla medesima categoria.

Inoltre, per quanto concerne i livelli di servizio garantiti (SLA) nel loro complesso, devono essere osservate le seguenti prescrizioni:

- deve essere inclusa la definizione chiara e non ambigua di tutti gli indicatori (SLI) e dei relativi valori obiettivo (SLO);
- il 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 deve dichiarare esplicitamente e preventivamente il periodo di tempo minimo e massimo di conservazione dei dati di monitoraggio degli SLI associati a ciascun servizio erogato;

- il Fornitore Cloud deve produrre e inviare al consumatore un report periodico (con periodicità almeno 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 Cloud deve implementare delle politiche e dei piani operativi per garantire la continuità del servizio (business continuity). Inoltre deve gestire tempestivamente il ripristino dell'operatività del servizio in seguito ad eventi catastrofici o imprevisti (disaster recovery).

Il Fornitore Cloud deve dichiarare 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.

Codice Requisito	Requisito	Elementi di riscontro
Disponibilità e continuità del servizio		
RPE1	La disponibilità del servizio deve essere adeguata all'utilizzo previsto e corrispondente a quella dichiarata dal Fornitore Cloud. Il Fornitore Cloud deve assicurare la disponibilità e fruibilità del servizio nella sua interezza: non possono esserci parti di servizio non disponibili o non utilizzabili appieno. SLI previsti: SLI01, SLI02, SLI03	Dichiarazione, Fornitore Cloud
Tempi di risposta del servizio		
RPE2	I tempi di risposta del servizio devono essere corrispondenti a quelli dichiarati dal Fornitore senza scostamenti significativi, e comunque entro precisi limiti prevedibili e noti a priori, al variare del numero di utenti connessi e del carico di lavoro sottoposto al servizio. SLI previsti: SLI04, SLI05	Dichiarazione Fornitore Cloud
Performance delle componenti Infrastructure		
RPE3	Servizi che includono la componente Compute Il Fornitore deve dichiarare i valori dei seguenti indicatori per i quali è previsto un livello di servizio garantito: disponibilità, massima durata dei periodi di indisponibilità (outage length), tempo medio e massimo di reboot delle VM SLI previsti: SLI01, SLI13	Dichiarazione Fornitore Cloud
RPE4	Servizi che includono la componente Network Il Fornitore deve dichiarare i valori dei seguenti indicatori per i quali è previsto un livello di servizio garantito: disponibilità, numero massimo di pacchetti persi (packet loss), larghezza di banda (bandwith), latenza massima, variazione minima e massima della latenza con cui vengono ricevuti i pacchetti SLI previsti: SLI01, SLI05	Dichiarazione Fornitore Cloud
RPE5	Servizi che includono la componente Storage Il Fornitore deve dichiarare i valori dei seguenti indicatori per i quali è previsto un livello di servizio garantito: disponibilità, quantità di dati trasferibili al secondo (sia in input che in output), tempo massimo di ripristino dei dati (max restore time)(*) latenza massima rispetto alle risorse compute(**) SLI previsti: SLI01, SLI05 * nel caso di risorse storage utilizzate per servizi di backup ** nel caso di risorse storage utilizzate in associazione a risorse compute	Dichiarazione Fornitore Cloud
Performance delle componenti Platform		

Continued on next page

Tabella 3.6 – continued from previous page

RPE6	Il Fornitore deve dichiarare i valori dei seguenti indicatori per i quali è previsto un livello di servizio garantito: disponibilità (oppure tempo cumulativo di indisponibilità mensile), tempi massimi di risposta delle componenti PaaS (ad es. database, load balancer, componenti DevOps, middleware),	Dichiarazione Fornitore Cloud
RPE7	Nel caso in cui sia prevista la scalabilità automatica della soluzione PaaS (o di alcune sue componenti), il Fornitore deve specificare e garantire quali siano le condizioni e i tempi di attivazione delle istanze aggiuntive che vengono attivate. SLI previsti: SLI06	Dichiarazione Fornitore Cloud
RPE8	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.	Dichiarazione Fornitore Cloud
RPE9	I precedenti requisiti di scalabilità (RPE7 e RPE8) devono essere garantiti sia nel caso di scalabilità crescente che nel caso di decrescita delle risorse allocate. In particolare in fase di decrescita le istanze PaaS/IaaS non più necessarie devono risultare correttamente disattivate in modo da non comportare costi di utilizzo.	Dichiarazione Fornitore Cloud

Dettaglio degli indicatori dei livelli di servizio garantiti:

Codice SLI	Indicatore	Descrizione
SLI01	Nome: Availability Origine: ISO/IEC 19086-1 / 19086-2	La disponibilità può essere calcolata come il tempo totale su un insieme di intervalli temporali definiti meno il tempo di inattività totale.
SLI13	Nome: Time to Service recovery Origine: ISO/IEC 19086-1	Il tempo che intercorre tra l'interruzione del servizio e il suo ripristino.
SLI14	Nome: Mean Time to Service recovery Origine: ISO/IEC 19086-1	Il valore medio su un determinato periodo di tempo di una serie di valori "Time to Service recovery"
SLI15	Nome: Maximum Time to Service recovery Origine: ISO/IEC 19086-1	Il valore massimo su un determinato periodo di tempo di una serie di valori "Time to Service recovery"
SLI16	Nome: Numero di Service Failures Origine: ISO/IEC 19086-1	Il numero totale di interruzioni di servizio su un arco temporale.
SLI05	Nome: Service Bandwidth Origine: ISO/IEC 19086-1	La quantità di dati che possono essere trasferiti in un determinato periodo di tempo.
SLI06	Nome: Elasticity speed Origine: ISO/IEC 19086-1	Questa quantità descrive quanto velocemente reagisce il servizio alla richiesta di nuove risorse.
SLI07	Nome: Data retention period Origine: ISO/IEC 19086-1	Il periodo di tempo in cui i dati del cliente vengono mantenuti dopo la notifica di cessazione del servizio.
SLI08	Nome: Log retention period Origine: ISO/IEC 19086-1	l periodo di tempo in cui i file di log relativi al servizio vengono conservati dopo la notifica di cessazione del servizio.
SLI09	Nome: Support hours Origine: ISO/IEC 19086-1	Le ore di funzionamento per ogni piano di supporto.

Continued on next page

Tabella 3.7 – continued from previous page

SLI10	Nome: Service Incident Support hours Origine: ISO/IEC 19086-1	Le ore durante le quali il cliente può ottenere supporto specificamente per incidenti legati al servizio.
SLI11	Nome: Maximum First Support Response Time Origine: ISO/IEC 19086-1	Il tempo massimo tra la segnalazione del cliente e la risposta iniziale del fornitore.
SLI12	Nome: Maximum Incident Resolution Time Origine: ISO/IEC 19086-1	Il tempo massimo per risolvere un incidente
SLI17	Nome: Backup Interval Origine: ISO/IEC 19086-1	Il tempo che intercorre tra un backup e l'altro
SLI18	Nome: Retention period of backup data Origine: ISO/IEC 19086-1	Il periodo di tempo in cui vengono mantenuti i backup da parte del fornitore
SLI19	Nome: Backup restoration testing Origine: ISO/IEC 19086-1	Il numero di test di restore eseguiti durante un determinato periodo di tempo.
SLI20	Nome: Recovery Time Objective Origine: ISO/IEC 19086-1	Il tempo massimo necessario a ripristinare completamente il servizio dopo un'interruzione

3.2.6.3 Interoperabilità e portabilità

Le soluzioni IaaS e PaaS devono consentire l'interoperabilità dei sistemi tra diversi ambienti Cloud in uso presso il medesimo Acquirente. Devono inoltre essere presenti caratteristiche di portabilità atte ad evitare il lock-in dell'Acquirente rispetto al Fornitore Cloud, nonché rispetto a specifici servizi (oppure feature) offerti.

A tal proposito i servizi che erogano virtual machines devono prevedere opportuni meccanismi di compatibilità e/o convertibilità da e verso formati basati su standard (ad es. Open Virtualization Format). Gli strumenti di importazione/esportazione e i tool di conversione devono essere messi a disposizione dal Fornitore Cloud ed essere corredati da opportuna documentazione.

Anche per quanto riguarda i servizi basati su virtualizzazione di tipo "Container", occorre evitare il lock-in e garantire la massima portabilità, attuando i seguenti principi:

- stack tecnologico per i container non strettamente correlato ad altre componenti a corredo quali orchestration engine, container catalogue, ecc.
- stack tecnologico non strettamente legato ad un particolare fornitore commerciale
- container interoperabili e compatibili con un'ampia varietà di sistemi operativi, architetture hardware, public Clouds.

I servizi Cloud 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 Cloud. L'Acquirente deve essere messo nella condizione di poter estrarre ed eventualmente eliminare permanentemente i propri dati in qualsiasi momento mediante interfaccia di gestione e mediante API.

La proprietà dei dati deve essere mantenuta dall'Acquirente durante tutto il ciclo di vita del servizio, anche in seguito ad operazioni di acquisizione o fallimento del Fornitore.

Codice Requisito	Requisito	Elementi di riscontro
Interoperabilità del servizio		

Continued on next page

Tabella 3.8 – continued from previous page

RIP1	Le soluzioni IaaS/PaaS devono esporre opportune Application Programming Interface (API) di tipo SOAP e/o REST associate alle funzionalità del servizio, per la gestione e la configurazione del servizio.	Dichiarazione Fornitore Cloud
RIP2	Il Fornitore Cloud deve rendere disponibile una adeguata documentazione tecnica delle API che ne chiarisca l'utilizzo.	Dichiarazione Fornitore Cloud Verifica documentale
RIP3	In caso di aggiornamento delle funzionalità del servizio e/o delle relative API deve essere possibile 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.	Dichiarazione Fornitore Cloud
RIP4	Devono essere implementate delle limitazioni sul numero di richieste che è possibile sottomettere alle API, collegate alle caratteristiche delle API stesse e della classe di utilizzatori (throttling).	Dichiarazione Fornitore Cloud
RIP5	Deve essere implementata la tracciabilità delle richieste SOAP/REST ricevute e del loro esito (logging e accounting), anche al fine della non ripudiabilità della comunicazione.	Dichiarazione Fornitore Cloud
Portabilità del servizio e dei dati		
RIP7	Deve essere sempre possibile da parte dell'Acquirente, su richiesta oppure in modalità self-service, l'estrazione di una copia completa dei dati memorizzati e gestiti dal servizio (in formato standard, non proprietario e riutilizzabile), ivi compresi i dati derivati quali log e statistiche di utilizzo, nonché le configurazioni del servizio. Tali prerogative devono essere garantite per un periodo di almeno due mesi (phase out) a partire dalla cessazione della fornitura (anche nel caso in cui la cessazione sia stata determinata dalla revoca della qualifica da parte di AgID). SLI previsti: SLI07 e SLI08	Dichiarazione Fornitore Cloud
RIP8	Deve essere sempre possibile la migrazione dei dati del servizio verso un altro Fornitore Cloud con conseguente eliminazione permanente dei dati di proprietà dell'Acquirente al termine della procedura di migrazione (inclusi i dati derivati e i dati di backup).	Dichiarazione Fornitore Cloud
RIP9	La proprietà dei dati deve essere mantenuta dall'Acquirente anche in seguito ad operazioni di acquisizione o fallimento del Fornitore Cloud. In caso di fallimento, chiusura dell'attività o dismissione del servizio, il Fornitore Cloud deve garantire all'Acquirente di poter recuperare i dati (in formato standard, non proprietario e riutilizzabile) e di poter migrare il servizio. Il periodo di tempo a disposizione dell'Acquirente dovrà consentirgli di completare il recupero dei dati e la migrazione del servizio e non potrà comunque essere inferiore a due mesi. SLI previsti: SLI07 e SLI08	Dichiarazione Fornitore Cloud

3.2.6.4 Conformità legislativa

Il Fornitore Cloud dovrà mettere a disposizione dell'Acquirente tutti gli strumenti necessari per consentirgli di essere conforme alla legislazione corrente.

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

Dettaglio dei requisiti per la conformità legislativa:

Codice Requisito	Requisito	Tipo di verifica
Riservatezza dei dati		
RCL1	Il Fornitore Cloud deve indicare per quali aspetti il servizio offerto è conforme al regolamento GDPR (General Data Protection Regulation - Regolamento UE 2017/679)	Dichiarazione Fornitore Cloud
RCL2	Il Fornitore Cloud deve rendere noti gli eventuali Stati esteri in cui sono dislocati i 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).	Dichiarazione Fornitore Cloud
RCL3	Il Fornitore Cloud, nei casi applicabili, dichiara la conformità ad accordi bilaterali (Privacy Shield EU-USA ecc.) volti alla salvaguardia dei dati elaborati, conservati ed a vario titolo gestiti per erogare il servizio.	Dichiarazione Fornitore Cloud

3.2.7 Appendice 1 - Impegni contrattuali

Nella tabella che segue si riepilogano i requisiti dai quali scaturiscono specifici impegni contrattuali e adempimenti formali che dovranno governare il rapporto di fornitura tra Fornitore Cloud e Acquirente. Per rispettare appieno i requisiti di qualificazione di cui al presente allegato, le clausole contrattuali presenti nei contratti di fornitura dovranno essere conformi ai principi e agli impegni di seguito richiamati.

Clausola	Requisiti	Adempimenti aggiuntivi
CL2	RO5 – Comunicazione tempestiva di aggiornamenti e modifiche al servizio RO6 – Aggiornamento tempestivo della documentazione e della manualistica	
CL3	RO9 – Dichiarazione di tutti i livelli di servizio garantiti che trovano applicazione RO10 – Livelli di servizio garantiti relativamente a disponibilità, performance e gestione malfunzionamenti RO2 – Livelli di servizio garantiti relativamente alla gestione delle richieste di assistenza	
CL4	RO11 – Accesso a strumenti di monitoraggio e di logging opportunamente documentato	
CL5	RO12 – Monitoraggio in tempo reale delle risorse utilizzate e dei costi imputati	
CL9	RPS3 – Piano di continuità operativa	Documento tecnico facente parte della fornitura

Continued on next page

Tabella 3.10 – continued from previous page

CL10	RPS4 – Responsabilità del Fornitore Cloud nel caso di perdita o inconsistenza dei dati a seguito di ripristino da un evento catastrofico o a seguito di migrazione del servizio per altri motivi	
CL11	RPE – Tempi di risposta del servizio che non subiscono fluttuazioni eccessive al variare del numero di utenti e del carico di lavoro	Scheda tecnica del servizio
CL12	RPS7 – Capacità di processamento del servizio che non subisce fluttuazioni eccessive al variare del numero di utenti e del carico di lavoro RPS8 – Capacità di processamento del servizio che non subisce fluttuazioni eccessive al variare del numero di tenant attivi (nel caso di configurazione multi-tenant)	
CL15	RIP1 – Presenza API di tipo SOAP/REST RIP2 – Documentazione tecnica API RIP3 – Versioning delle API RIP4 – Limitazioni volumetriche per l'utilizzo delle API RIP5 – Tracciabilità delle richieste SOAP/REST	Documento tecnico facente parte della fornitura
CL16	RIP6 – Possibilità di estrarre i dati gestiti dal servizio in qualsiasi momento, anche dopo il termine della fornitura (periodo di phase-out di almeno due mesi) RIP7 – Migrazione dei dati del servizio (reversibilità) RIP8 – Garanzie sulla proprietà e disponibilità dei dati in caso di fallimento/acquisizione del Fornitore Cloud	
CL19	RCL1 – Conformità rispetto al regolamento GDPR	
CL20	RCL2 – Comunicazione degli eventuali stati esteri in cui risiedono i data center attraverso cui si eroga il servizio	

3.2.8 Appendice 2 - Scheda tecnica del Servizio

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) / CSN delegato da un CSP
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	
Tempi di risposta e di risoluzione garantiti	
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 i dati saranno disponibili	
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	
Accesso via SSH	
Accesso via RDP	
Altro tipo di accesso	
Documentazione	
API	URL Autenticazione Altre info
Funzionalità invocabili tramite API e funzionalità che non sono accessibili via API	
Documentazione delle API	URL Web PDF
Presenza 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)

Metriche e statistiche di utilizzo	
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

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

Livelli di servizio garantiti	
Disponibilità	
Tempi di risposta	
Capacità di processa mento/carico	
Altri indicatori	Elencare:
Scostamenti massimi tollerabili	(per ciascun indicatore per cui sono previsti)
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)
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	

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

3.3 Archivio dei commenti alla circolare «Qualificazione dei Cloud Service Provider per servizi IaaS/PaaS»

In questa sezione è presente l'archivio dei commenti alla Circolare «Qualificazione dei Cloud Service Provider per servizi IaaS/PaaS» pubblicati in precedenza.

Abbiamo migliorato il sistema dei commenti: la discussione ora continua su Forum Italia.

Nota: Circolare in consultazione pubblica fino al 01/03/2018

Nota: Le circolari rimarranno in consultazione pubblica fino al 01/03/2018