Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

CIRCOLARE N. 2 del 9 aprile 2018

Criteri per la qualificazione dei Cloud Service Provider per la PA

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 affinché le infrastrutture e i servizi IaaS e PaaS erogati dal fornitore possano ricevere la qualificazione "CSP" nell'ambito del "Cloud della PA"[1].

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

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

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

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

[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 e PaaS erogati da Cloud SPC, dai PSN e dai CSP qualificati ai sensi di quanto disposto da questa Circolare.

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

Definizioni

Termine o abbreviazione	Descrizione
AgID, Agenzia	Agenzia per l'Italia Digitale
Codice /Codice dell'Amministrazione Digitale/CAD	Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i.
Cloud della PA	Il Cloud della PA è composto dalle infrastrutture e servizi IaaS/PaaS erogati da Cloud SPC, dai PSN e dagli altri CSP qualificati da AgID ai sensi della presente Circolare
Cloud	Insieme di infrastrutture tecnologiche remote utilizzate come risorsa virtuale per la memorizzazione e/o l'elaborazione nell'ambito di un servizio
Cloud SPC o SPC Cloud	Contratto Quadro stipulato da CONSIP con il RTI aggiudicatario della Gara SPC Cloud Lotto 1 (https://www.cloudspc.it)
Fornitore Cloud, CSP, Fornitore	Soggetto titolare dell'infrastruttura e dei servizi IaaS e PaaS o Pubblica Amministrazione interessata ad erogare servizi IaaS e PaaS ad altre PA
Giorni	Giorni solari
Marketplace Cloud	Piattaforma digitale che espone il catalogo dei servizi IaaS e PaaS qualificati ai sensi della presente Circolare, nonchè i servizi SaaS qualificati da AgID ai sensi della circolare "Criteri per la qualificazione dei servizi SaaS per il Cloud della PA"

Pubbliche amministrazioni/ Amministrazioni/ PA	Le Amministrazioni, come meglio definite all'art. 2, comma 2 del Codice dell'Amministrazione Digitale
PSN	Soggetto titolare dell'insieme di infrastrutture IT (centralizzate o distribuite), ad alta disponibilità, di proprietà pubblica, eletto a Polo Strategico Nazionale dalla Presidenza del Consiglio dei Ministri, e qualificato da AgID ad erogare ad altre amministrazioni, in maniera continuativa e sistematica, servizi infrastrutturali on-demand, servizi di disaster recovery e business continuity, servizi di gestione della sicurezza IT ed assistenza ai fruitori dei servizi erogati
Software as a Service/SaaS	Tra i modelli di servizio offerti dalle piattaforme di Cloud computing, il Software as a Service (SaaS) identifica una classe di servizi fully-managed in cui il gestore del servizio (CSP) si occupa della predisposizione, configurazione, messa in esercizio e manutenzione dello stesso (utilizzando un'infrastruttura cloud propria o di terzi), lasciando al fruitore del servizio (PA) il solo ruolo di utilizzatore delle funzionalità offerte
Platform as a Service/PaaS	Una categoria di servizi cloud in cui le funzionalità cloud offerte sono di tipo programmatico ovvero il CSC può amministrare, dispiegare ed eseguire applicazioni Cloud utilizzando uno o più linguaggi di programmazione, uno o più ambienti di sviluppo/esecuzione supportati dal CSP e i relativi componenti software a corredo (code di messaggi, database, ecc.)
Infrastructure as a Service/IaaS	Una categoria di servizi cloud in cui le funzionalità cloud offerte sono di tipo infrastrutturale, tali funzionalità consentono al CSP 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)
Circolare	Circolare AgID "Criteri per la qualificazione dei Cloud Service Provider per la PA".
Mercato elettronico	Il Mercato Elettronico della P.A. (MePA) è il mercato digitale gestito da CONSIP in cui le Amministrazioni abilitate possono acquistare per valori inferiori alla soglia comunitaria, i beni e servizi offerti da fornitori abilitati a presentare i propri cataloghi sul sistema.
SLI	Service Level Indicator, una misura quantitativa definita di un determinato aspetto della qualità del servizio (ad es. numero di richieste al secondo, latency, throughput, availability, etc)

Articolo 1 - Oggetto ed ambito di applicazione

La presente circolare definisce i requisiti e la procedura per la qualificazione dell'infrastruttura e dei servizi IaaS e PaaS dei Cloud Service Provider. Le disposizioni ivi contenute si applicano sia ai fornitori interessati ad offrire servizi IaaS e PaaS alle PA, sia alle amministrazioni che intendono acquisire servizi IaaS e PaaS erogati dai CSP nell'ambito del Cloud della PA.
In particolare, come previsto dal Piano Triennale per l'informatica della PA 2017 - 2019, Consip provvede ad abilitare l'accesso agli strumenti del mercato elettronico / convenzioni / accordi quadro ai soli Cloud Service Provider che erogano servizi IaaS e PaaS qualificati da AgID.

Articolo 2 – Il processo di qualificazione

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

- erogare servizi di tipo Public Cloud (IaaS o PaaS) per la PA - *Richiesta "Tipo A"*;

- erogare servizi SaaS da qualificare ai sensi della Circolare AgID "*Criteri per la qualificazione di servizi SaaS per il Cloud della PA*" utilizzando la propria infrastruttura Cloud - *Richiesta "Tipo B"*;
- erogare tutti i servizi previsti nei punti precedenti - *Richiesta "Tipo C"*.

Il processo di qualificazione è articolato in tre fasi:

- Richiesta di qualificazione
- Conseguimento della qualificazione
- Mantenimento della qualificazione (Monitoraggio)

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

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

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

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

Articolo 3 - Requisiti della qualificazione

I requisiti per la qualificazione si suddividono in:

- Requisiti organizzativi;
- Requisiti specifici.

Il dettaglio di tali requisiti differenziati per tipologia di richiesta (di cui all'art.2) è fornito all'interno dell'allegato "A" alla presente Circolare, denominato "*Requisiti per la qualificazione dei Cloud Service Provider della PA*".
AgID si riserva la facoltà di modificare/aggiornare/integrare tali requisiti sulla base dell'evoluzione del contesto e delle tecnologie.

Articolo 4 - Fasi del processo di qualificazione

Fase 1 - Richiesta di qualificazione
Il fornitore interessato alla qualificazione CSP provvede a trasmettere tramite la piattaforma AgID dedicata apposita richiesta, fornendo le informazioni e la documentazione in lingua italiana relative al possesso dei requisiti di cui all'allegato "A" alla presente Circolare. Per l'eventuale documentazione d'accompagnamento presentata in lingua straniera dovrà essere allegata idonea traduzione, anche per estratto.
Nel caso in cui un fornitore non abbia alcuna rappresentanza diretta o indiretta in Italia, l'Agenzia per l'Italia Digitale su segnalazione di un'amministrazione proponente, acquisisce le informazioni necessarie alla qualificazione e potrà avviare d'ufficio la procedura mediante la piattaforma AgID dedicata alla qualificazione, secondo le modalità pubblicate sul sito Cloud Italia all'indirizzo: https://cloud.italia.it/
Fase 2 - Conseguimento qualificazione
Il conseguimento della qualificazione CSP coincide con la corretta acquisizione tramite la piattaforma AgID dedicata della richiesta di qualificazione.
L'Agenzia si riserva di effettuare le verifiche necessarie di cui alla fase successiva del presente processo.
I servizi IaaS e PaaS qualificati da AgID sono inseriti nel Marketplace Cloud.
I CSP qualificati sono inseriti in apposito registro pubblico nell'ambito di Marketplace Cloud.
Fase 3 – Mantenimento della qualificazione
L'Agenzia potrà verificare in ogni momento il possesso del criterio d'ammissibilità e dei requisiti previsti per la qualificazione CSP.

Le verifiche potranno essere avviate anche sulla base di segnalazioni formali indirizzate all'Agenzia da parte dell'Amministrazione cliente/utente del CSP qualificato.
L'Agenzia si riserva la facoltà di avvalersi di soggetti terzi per l'espletamento delle attività di verifica.
Al fine del mantenimento della qualifica, il soggetto richiedente si impegna a comunicare tempestivamente all'Agenzia, tramite la piattaforma dedicata, ogni evento che modifichi il rispetto dei requisiti di cui all'allegato "A" alla presente Circolare.
La perdita del possesso del/i criterio/i d'ammissibilità e/o di almeno uno dei requisiti di cui all'allegato A, comporta la revoca della qualificazione, ai sensi del successivo art. 5.
Qualora durante le attività di verifica dovessero emergere elementi relativi a possibili violazioni della normativa sulla privacy, l'Agenzia ne informa tempestivamente il Garante per la protezione dei dati personali.

Articolo 5 - Revoca della qualificazione

Nel caso di:

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

l'Agenzia comunica al fornitore il preavviso di revoca della qualificazione CSP con previsione di un termine per le eventuali controdeduzioni.

Nel caso di infruttuoso esperimento del termine o mancato accoglimento delle controdeduzioni presentate, l'Agenzia procede alla revoca della qualificazione CSP con provvedimento motivato, disponendone la contestuale eliminazione dei servizi IaaS e PaaS dal Marketplace Cloud, nonchè la relativa annotazione della cancellazione del fornitore dal registro pubblico dei CSP qualificati, dandone adeguata pubblicità.
Nei casi di revoca della qualificazione CSP, il fornitore non può presentare una nuova richiesta di qualificazione all'Agenzia se non siano venute meno le cause che hanno determinato la revoca.

Articolo 6 – Durata della qualificazione CSP

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

Articolo 7 - Disposizioni transitorie

Nelle more dell'attivazione della piattaforma dedicata la richiesta di qualificazione potrà essere sottomessa mediante le modalità pubblicate sul sito https://cloud.italia.it
Nelle more dell'attivazione del Marketplace Cloud l'elenco dei servizi IaaS/PaaS dei CSP qualificati sarà pubblicato sul sito https://cloud.italia.it

Articolo 8 - Disposizioni finali

La presente Circolare entra in vigore a partire da 30 giorni dalla data di pubblicazione nella Gazzetta Ufficiale della Repubblica Italiana.
A decorrere da sei mesi dall'entrata in vigore della presente Circolare, le Amministrazioni acquisiscono esclusivamente servizi IaaS e PaaS qualificati e pubblicati sul Marketplace Cloud.
Nei contratti aventi ad oggetto servizi IaaS e PaaS qualificati, le Amministrazioni prevedono gli SLI obbligatori presenti nella tabella "Indicatori della Qualità del Servizio" di cui all'Allegato A.
La data di attivazione della piattaforma dedicata e del Marketplace Cloud sarà comunicata insieme alle modalità operative della procedura di qualificazione sul sito https://cloud.italia.it.

Allegati

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

IL DIRETTORE GENERALE

ANTONIO SAMARITANI

Firmato digitalmente da
ANTONIO SAMARITANI
Data: 2018.04.09
19:20:09 +02'00'

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Allegato A alla CIRCOLARE N. 2 del 9 aprile 2018

Requisiti per la qualificazione dei Cloud Service Provider per la PA

Acronimi e definizioni

Termine o abbreviazione	Descrizione
AgID, Agenzia	Agenzia per l'Italia Digitale
Codice /Codice dell'Amministrazione Digitale/CAD	Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i.
Cloud della PA	Il Cloud della PA è composto dalle infrastrutture e servizi IaaS/PaaS erogati da Cloud SPC, dai PSN e dai CSP qualificati da AgID ai sensi della presente Circolare
Cloud	Insieme di infrastrutture tecnologiche remote utilizzate come risorsa virtuale per la memorizzazione e/o l'elaborazione nell'ambito di un servizio
Cloud SPC o SPC Cloud	Contratto Quadro stipulato da CONSIP con il RTI aggiudicatario della Gara SPC Cloud Lotto 1 (https://www.cloudspc.it)
CSC	Cloud Service Consumer acquirente e fruitore di servizi erogati in modalità Cloud
CSN	Cloud Service Partner, è un soggetto terzo che può svolgere attività di supporto o di consulenza per conto del CSP, del CSC o di entrambi
Fornitore Cloud, CSP, Fornitore	Soggetto titolare dell'infrastruttura e dei servizi IaaS e PaaS o Pubblica Amministrazione

	interessata ad erogare servizi IaaS e PaaS ad altre PA
Giorni	Giorni solari
Marketplace Cloud	Piattaforma digitale che espone il catalogo dei servizi IaaS e PaaS qualificati ai sensi della presente Circolare, nonchè i servizi SaaS qualificati da AgID ai sensi della circolare "Criteri per la qualificazione dei servizi SaaS per il Cloud della PA"
Provisioning	Predisposizione delle risorse Cloud infrastrutturali funzionale all'erogazione di servizi Cloud. Le attività di predisposizione sono eseguite a cura del Fornitore Cloud, tipicamente si tratta di attività automatizzate su risorse virtuali di tipo computazionale, di storage e di rete che vengono attivate e configurate opportunamente
Pubbliche amministrazioni/ Amministrazioni/PA	Le Amministrazioni, come meglio definite all'art. 2, comma 2 del Codice dell'Amministrazione Digitale
PSN	Soggetto titolare dell'insieme di infrastrutture IT (centralizzate o distribuite), ad alta disponibilità, di proprietà pubblica, eletto a Polo Strategico Nazionale dalla Presidenza del Consiglio dei Ministri, e qualificato da AgID ad erogare ad altre amministrazioni, in maniera continuativa e sistematica, servizi infrastrutturali on-demand, servizi di disaster recovery e business continuity, servizi di gestione della sicurezza IT ed assistenza ai fruitori dei servizi erogati
Platform as a Service, PaaS	Una categoria di servizi cloud in cui le funzionalità cloud offerte sono di tipo programmatico ovvero il CSC può amministrare, dispiegare ed eseguire applicazioni Cloud utilizzando uno o più linguaggi

	di programmazione, uno o più ambienti di sviluppo/esecuzione supportati dal CSP e i relativi componenti software a corredo (code di messaggi, database, ecc.)
Infrastructure as a Service, IaaS	Una categoria di servizi cloud in cui le funzionalità cloud offerte sono di tipo infrastrutturale, tali funzionalità consentono al CSC di disporre autonomamente in modo programmatico di risorse di computing, di storage e networking
SLI	Service Level Indicator, una misura quantitativa definita di un determinato aspetto della qualità del servizio (ad es. numero di richieste al secondo, latency, throughput, availability, etc)
SLO	Service Level Objective, un valore o un intervallo di valori di riferimento per un livello di servizio misurato da un indicatore (SLI)
SLA	Service Level Agreement, un accordo formale che prevede le conseguenze del mancato raggiungimento degli obiettivi (SLO) prefissati relativamente alla qualità del servizio
Dati derivati	Dati che risiedono sotto il controllo del Cloud Service Provider, originati dall'interazione con il servizio Cloud da parte del Cloud Service Customer. I dati derivati includono tipicamente dati di logging, contenenti informazioni su chi ha utilizzato il servizio, quando lo ha utilizzato e che funzionalità ha utilizzato; possono anche includere informazioni circa il numero di utenti autorizzati e le loro identità; includono tutte le configurazioni e customizzazioni supportate dal servizio.
Circolare	Circolare AgID sui "Criteri per la qualificazione dei Cloud Service Provider per la PA"

Autocertificazione	Dichiarazione sostitutiva resa ai sensi del DPR 28 dicembre 2000 n. 445

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

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

Introduzione

Il presente documento definisce nel dettaglio i requisiti, di cui all'art. 3 della Circolare, che le infrastrutture ed i servizi IaaS e PaaS del Fornitore Cloud devono rispettare per ottenere la qualificazione da parte di AgID quale "CSP qualificato per il *Cloud della PA*". Nella richiesta di qualificazione il Fornitore Cloud include le informazioni relative alla propria infrastruttura e può includere uno o più servizi IaaS/PaaS. Resta inteso che tutti i servizi per i quali è stata fatta richiesta di qualificazione devono possedere i requisiti di cui al presente allegato e dovranno essere conformi alla vigente disciplina nazionale e europea in materia di protezione dei dati personali (regolamento GDPR - General Data Protection Regulation - Regolamento UE 2016/679).

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

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

- AgID o Agenzia, Agenzia per l'Italia Digitale in qualità di soggetto responsabile della procedura di qualificazione.

Requisiti delle soluzioni Cloud

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

- Requisiti organizzativi (RO),
- Requisiti specifici.

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

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

Requisiti organizzativi

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

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

Gli standard di riferimento per questo insieme di requisiti sono quelli che appartengono alla famiglia ISO/IEC 20000, in particolare gli standard ISO/IEC 20000-1 e ISO/IEC TR 20000-9.
Al fine di garantire un'adeguata gestione della fornitura il Fornitore Cloud deve permettere all'Acquirente di amministrare in maniera strutturata e automatizzata le fasi di acquisto e di gestione/configurazione di ciascun servizio e, ove applicabile, di tutte le risorse/elementi/funzionalità associate (ad es. selezione dei template PaaS, configurazione dei server virtuali, gestione delle risorse di rete, ecc.), garantendo controlli di coerenza durante il processo.

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

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

Supporto clienti e assistenza tecnica

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

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

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

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

Gestione del cambiamento (change management)

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

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

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

Gestione della configurazione (configuration management)

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

Gestione degli Incidenti (incident & problem management)

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

Livelli di servizio e trasparenza

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

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

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

Requisiti specifici

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

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

Sicurezza, Privacy e protezione dei dati

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

Performance

Il Fornitore Cloud è tenuto a dichiarare la qualità offerta e l'affidabilità del servizio durante tutto il ciclo di vita. Le Amministrazioni Acquirenti sono tenute a verificare che le pattuizioni relative alla qualità del servizio costituiscano parte integrante del contratto di fornitura, all'interno del quale dovrà essere ricompresa una specifica sezione relativa ai "livelli di servizio garantiti" ovvero al Service Level Agreement (SLA).
Le Amministrazioni acquirenti assicurano che gli accordi relativi ai *livelli di servizio garantiti* (SLA) siano specificati mediante la quantificazione di un insieme di valori *obiettivo* (SLO) o intervalli di valori riferibili ad altrettanti specifici *indicatori* di performance, affidabilità, risultato (SLI). Sulla base di tali accordi il Fornitore Cloud risulterà impegnato a rispettare gli obiettivi dichiarati che dovranno essere monitorabili dall'Acquirente.

La sezione del contratto di fornitura relativa ai *livelli di servizio garantiti* include le *penali compensative* che il Fornitore Cloud corrisponde all'Acquirente in caso di mancato rispetto di uno o più valori obiettivo (SLO). I metodi di quantificazione e le condizioni di riconoscimento delle penali compensative sono inclusi nel contratto e sono allineati ai valori e alle condizioni di mercato riscontrabili per servizi analoghi o appartenenti alla medesima categoria.
Si richiama inoltre quanto previsto dallo standard ISO/IEC 19086-1:2016 per quanto concerne i livelli di servizio garantiti (SLA):

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

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

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

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

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

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

Interoperabilità e portabilità

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

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

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

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

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

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

RIP5 - Il Fornitore Cloud garantisce all'Acquirente la possibilità di estrarre in qualsiasi momento una copia completa dei dati e metadati memorizzati (in formato pubblico e

aperto) come, a titolo esemplificativo ma non esaustivo: volumi, object e block storage, dump di DB, ecc.

Conformità legislativa

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

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

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

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

Appendice 1

Tabella 1.1 - Indicatori della Qualità del Servizio

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

SLI6	*Cloud Service Throughput*	Il numero di input o insieme di input correlati tra di loro (transazione) che possono essere processati in ciascuna unità di tempo dal servizio.
SLI7	*Elasticity Speed*	Descrive quanto velocemente reagisce il servizio alla richiesta di nuove risorse allorquando: • viene effettuata una richiesta di ri-allocazione (nel caso di elasticità manuale), oppure • il carico di lavoro cambia (in caso di elasticità automatica).
SLI8	*Maximum Time to Service Recovery*	Il massimo tempo che intercorre tra l'indisponibilità del servizio dovuta a malfunzionamento di una delle sue componenti e il ripristino della sua normale operatività.
SLI9	*Backup Interval*	Il tempo che intercorre tra un backup e l'altro.
SLI10	*Retention period of backup data*	Il periodo di tempo in cui vengono mantenuti i backup da parte del CSP.
SLI11	*Backup restoration testing*	Il numero di test di restore (a partire dai dati di backup) eseguiti durante un determinato periodo di tempo.
SLI12	*Recovery Time Objective (RTO)*	Il tempo massimo necessario a ripristinare completamente il servizio dopo un'interruzione dovuta ad un "evento catastrofico" che ha innescato l'attivazione di un ambiente di erogazione secondario (disaster recovery).
SLI13	*Recovery Point Objective (RPO)*	L'intervallo massimo di tempo che precede un "evento catastrofico" rispetto al quale si può verificare la perdita delle modifiche ai dati come conseguenza delle attività di ripristino del servizio (disaster recovery).
SLI14	*Data retention period*	Il periodo di tempo in cui i dati del cliente vengono mantenuti dal CSP dopo la notifica di cessazione del servizio.

SLI15	*Log retention period*	Il periodo di tempo in cui i file di log relativi al servizio vengono conservati dopo la notifica di cessazione del servizio.

Tabella 1.2 - Riepilogo applicabilità requisiti e adempimenti previsti

Requisito	Applicabilità alla richiesta di qualificazione	Adempimenti previsti
Requisiti organizzativi		
RO1	Tipo A Tipo B Tipo C	Autocertificazione Produzione documentazione
RO2	Tipo A Tipo B Tipo C	Autocertificazione Produzione documentazione
RO3	Tipo A Tipo C	Autocertificazione
RO4	Tipo A Tipo C	Autocertificazione Produzione documentazione
RO5	Tipo A Tipo C	Autocertificazione Produzione documentazione
RO6	Tipo A Tipo B Tipo C	Autocertificazione Produzione documentazione
RO7	Tipo A Tipo C	Autocertificazione
RO8	Tipo A Tipo C	Autocertificazione
RO9	Tipo A Tipo C	Autocertificazione Produzione documentazione
RO10	Tipo A Tipo B Tipo C	Autocertificazione Produzione documentazione
RO11	Tipo A Tipo C	Autocertificazione
RO12	Tipo A Tipo C	Autocertificazione
RO13	Tipo A Tipo C	Autocertificazione

Sicurezza		
RSI1	Tipo A Tipo B Tipo C	Autocertificazione Produzione documentazione
Performance		
RPE1	Tipo A Tipo C	Autocertificazione
RPE2	Tipo A Tipo C	Autocertificazione
RPE3	Tipo A Tipo C	Autocertificazione
RPE4	Tipo A Tipo C	Autocertificazione
Interoperabilità e Portabilità		
RIP1	Tipo A Tipo C	Autocertificazione
RIP2	Tipo A Tipo C	Autocertificazione Produzione documentazione
RIP3	Tipo A Tipo C	Autocertificazione
RIP4	Tipo A Tipo C	Autocertificazione
RIP5	Tipo A Tipo C	Autocertificazione
Conformità legislative		
RCL1	Tipo A Tipo B Tipo C	Autocertificazione
RCL2	Tipo A Tipo B Tipo C	Autocertificazione
RCL3	Tipo A Tipo B Tipo C	Autocertificazione

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Appendice 2

Scheda tecnica del Servizio

La scheda tecnica del servizio riporta alcune delle informazioni acquisite durante la richiesta di qualificazione tramite la *piattaforma AgID dedicata*. Dette informazioni potranno confluire nel Marketplace Cloud quale corredo descrittivo del servizio. La scheda tecnica che segue è riportata in versione preliminare e potrà subire successive modifiche e integrazioni che saranno visibili direttamente sulla piattaforma AgID dedicata.

Nome del servizio

Descrizione generale

Max 800 caratteri

Elenco delle caratteristiche funzionali

10 punti elenco + max 200 caratteri

Ambito di applicazione

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

Supporto Clienti

e-mail	

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

Attivazione e disattivazione del servizio

Tempi di attivazione e disattivazione	
Processo di attivazione	
Processo di disattivazione	
Estrazione dei dati a seguito di disattivazione	(descrivere tempistiche e modalità)

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

Reti pubbliche disponibili

Rete SPC	Si/No
GARR	Si/No
Altro	

Utilizzo del servizio

Web Browser	Si/No
Browser supportati	(elenco dei browser supportati)
Applicativo da installare	Si/No
App Mobile	Si/No

Differenze nella fruizione del servizio tra la versione Mobile e la versione Desktop	
Altro tipo di fruizione	(se prevista)
Accesso via SSH	(se applicabile)
Accesso via RDP	(se applicabile)
Altro tipo di accesso	(se previsto)
Documentazione utente	
Elenco delle lingue in cui è resa disponibile la documentazione utente	
API	URL Autenticazione Altre info
Funzionalità invocabili tramite API e funzionalità che non sono accessibili via API	

Documentazione delle API	URL Web PDF Altro
Disponibilità di un ambiente di test delle API (sandbox)	URL Autenticazione Altro

Scalabilità

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

Trasparenza, metriche e statistiche di utilizzo

Strumenti di monitoraggio delle risorse utilizzate, dei costi, e della qualità del servizio	
Metriche disponibili	

Statistiche disponibili	
Report disponibili	

Conformità legislative

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

Portabilità dei dati del servizio

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

Livelli di servizio garantiti

Availability	
Support hours	
Maximum First Support Response Time	
Altri indicatori	Elenco indicatori
Disponibilità di monitoraggio in tempo reale sullo stato del servizio	Si/No

Disponibilità di notifiche via SMS/email degli eventi di indisponibilità del servizio	Si/No

Misure di sicurezza e protezione dei dati

Controllo da parte dell'utilizzatore sulla localizzazione dei siti in cui verranno memorizzati e processati i dati	Si/No
Standard di sicurezza dei data center utilizzati per erogare il servizio	Elenco
Approccio utilizzato per eseguire test di penetrazione	
Frequenza con cui sono eseguiti i test di penetrazione	
Approcci utilizzati per proteggere i dati memorizzati dal servizio	

Presenza di procedure per la cancellazione permanente dei dati	Si/No
Approcci utilizzati per la protezione dei dati in transito nelle reti esterne	(Ad es. VPN, IPSEC, HTTPS, ecc.)
Approcci utilizzati per la protezione dei dati in transito nelle reti interne	(Ad es. VPN, IPSEC, HTTPS, ecc.)
Meccanismi di autenticazione degli utenti supportati	
Possibilità di configurazione/ customizzazione dei meccanismi di autenticazione	Si/No (eventuale descrizione, anche con riferimento alla possibilità di federazione delle identità)
Disponibilità di autenticazione a 2 fattori	Si/No
Politiche di accesso alle informazioni di audit	In tempo reale (Si/No) Differenziata tra utilizzatori e fornitore (Si/No) Tempo minimo e massimo di conservazione delle informazioni di audit Tempo minimo e massimo di conservazione dei log del servizio

Standard e certificazioni

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

Prezzi e modalità di imputazione dei costi

Prezzo del servizio	
Unità di misura	
Altre condizioni	