QUALIFICAZIONE SERVIZI CLOUD

SUGGERIMENTI PER UNA CORRETTA SOTTOMISSIONE DELLE QUALIFICAZIONI CSP O SAAS

UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale

Agenzia per la Coesione Territoriale

Dipartimento della Funzione Pubblica

PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020

AGID Agenzia per l'Italia Digitale

INDICE CONTENUTI

1. INTRODUZIONE

1.1 - PREMESSA

Tra le linee d'azione del Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017 - 2019, approvato con DPCM del 31 maggio 2017, nell'ambito della strategia di evoluzione del modello Cloud della PA, è prevista la definizione di regole e procedure per la qualificazione di Cloud Service Provider (CSP) pubblici.

L'Agenzia per l'Italia Digitale in data 09 Aprile 2018 ha emesso due Circolari operative, una, la numero 2, per la qualificazione dei CSP per la PA (servizi IaaS e PaaS) e l'altra, la numero 3, per la qualificazione di servizi SaaS per il Cloud della PA.

Le Circolari definiscono i requisiti e la procedura per la qualificazione dei Cloud Service Provider, articolata in tre fasi:

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

Per ottenere la qualificazione della propria infrastruttura cloud o dei propri servizi cloud un Fornitore deve autenticarsi tramite SPID al portale AgID "Qualificazione dei Cloud Service Provider e dei Servizi Cloud" all'indirizzo:

https://cloud.italia.it/marketplace/supplier/landing/landing_page.html

La procedura guidata richiede di inserire le informazioni e di produrre la documentazione di cui agli allegati tecnici delle Circolari. La piattaforma permette di trasmettere per via telematica la richiesta di qualificazione ai sensi dell'art. 65 del Codice dell'amministrazione digitale (D.Lgs. 7 marzo 2005, n. 82). La richiesta di qualificazione (istanza), le dichiarazioni ivi contenute e la documentazione prodotta costituiscono pertanto una "dichiarazione sostituiva di atto di notorietà" resa ai sensi dell'art. 47 del DPR n. 445/2000.

Il Fornitore Cloud può trasmettere la richiesta di qualificazione direttamente oppure tramite soggetti terzi (ossia una società che opera in Italia in qualità di rappresentante, distributore commerciale, ecc.). In questi casi il soggetto richiedente assume il ruolo di "partner" del fornitore. La piattaforma richiede al soggetto partner di produrre un opportuno atto di delega che lo autorizzi ad agire in nome e per conto del fornitore ai sensi della normativa vigente.

Tutti i servizi qualificati da AgID saranno pubblicati all'interno del "Catalogo dei servizi Cloud per la PA qualificati":

https://cloud.italia.it/marketplace/supplier/market/index.html

AgID si riserva di effettuare tutte le verifiche necessarie in merito alle dichiarazioni e le informazioni fornite, anche dopo il conseguimento della qualificazione CSP e/o della qualificazione SaaS.

1.2 - SCOPI

Lo scopo del documento, indirizzato a quei Fornitori interessati alla qualificazione della propria infrastruttura cloud o dei propri servizi cloud (IaaS, PaaS, SaaS), è quello di fornire alcuni suggerimenti utili per una corretta sottomissione dei dati e dei documenti richiesti da AgID (per ottemperare agli adempimenti previsti dalle circolari nr. 2 e 3 del 09 Aprile 2018) all'interno del portale di "Qualificazione dei Cloud Service Provider e dei Servizi Cloud" all'indirizzo:

https://cloud.italia.it/marketplace/supplier/landing/landing_page.html

Il presente documento si aggiunge agli altri strumenti a supporto:

- le FAQ, reperibili agli indirizzi:
  - https://cloud.italia.it/marketplace/supplier/landing/domande_frequenti.html
  - https://cloud.italia.it/projects/cloud-italia-docs/it/latest/domande-frequenti.html#circolare-qualificazione-cloud-service-provider

- l'Assistenza tecnica e il supporto mail, attraverso l'indirizzo:

  qualificazione-cloud@agid.gov.it

- gli incontri periodici con i fornitori eseguiti dall'amministrazione, assimilabili ad altrettanti eventi formativi, in cui viene descritto il processo di sottomissione nei suoi diversi aspetti:
  - scopi
  - aspettative
  - modalità

1.3 - RIFERIMENTI

Identificativo	Titolo/Descrizione
AgID, Circolare nr. 2 del 09 aprile 2018	Documento contenente la circolare AgID ed il relativo allegato tecnico (Allegato A) del 09 aprile 2018 che definisce i criteri per la qualificazione dei Cloud Service Provider per la PA
AgID, Circolare nr. 3 del 09 aprile 2018	Documento contenente la circolare AgID ed il relativo allegato tecnico (Allegato A) del 09 aprile 2018 che definisce i criteri per la qualificazione dei Cloud Service Provider per la PA

1.4 - ACRONIMI E GLOSSARIO

Definizione / Acronimo	Descrizione
AgID	Agenzia per l'Italia Digitale
CSP	Cloud Service Provider
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
SPC	Sistema Pubblico di Connettività

2. I NOSTRI SUGGERIMENTI

Il documento si articola in due sezioni distinte, una dedicata ai Cloud Service Provider e servizi cloud (IaaS e PaaS), la seconda che tratta i servizi cloud di tipo SaaS.

In ognuna di esse, sono presenti i requisiti che a nostro parere richiedono alcune specificazioni ulteriori, rispetto a quanto già documentato. In particolare, vengono fornite alcune informazioni aggiuntive da prevedere all'atto della sottomissione del servizio, riguardanti:

- i processi di Change, Configuration, Incident e Problem Management,
- le diverse forme di certificazione che vengono richieste,
- la documentazione tecnica da fornire a corredo,
- la conformità con gli obblighi e gli adempimenti normativi in materia del trattamento dei dati personali.

Ciascun requisito preso in esame, è descritto attraverso una scheda in cui vengono riportati:

- la definizione, così come è stata espressa nelle circolari di riferimento,
- l'obiettivo per cui si richiede il suo inserimento,
- il posizionamento nel form di sottomissione e le sue caratteristiche ovvero se si tratta di:
    - una descrizione sintetica;
    - il caricamento di un documento o di un certificato;
    - gli elementi di un elenco;
    - le opzioni possibili legate a qualche aspetto particolare del servizio;
    - un'autocertificazione,
- infine i nostri suggerimenti, ossia le informazioni, che riteniamo sia opportuno vengano fornite per completare il contesto descrittivo del servizio, in una forma che rimane prevalentemente di autocertificazione.

2.1 CLOUD SERVICE PROVIDER E SERVIZI CLOUD (IaaS e PaaS)

Di seguito i requisiti relativi alla sottomissione di Cloud Service Provider e servizi Cloud, che sono stati selezionati:

- RO1 (Test Most Mortem o Disaster Recovery)
- RO2 (Certificazione ISO 9001)
- RO5 (Documentazione tecnica e di supporto)
- RO6 (Processo di Change Management
- RO9 (Processo di Configuration Management)
- RO10 (Processi di Incident e Problem Management)
- RSI1 (Certificazione ISO/IEC 27001)
- RIP2 (Documentazione tecnica API)

2.1.1 RO1 – Test Port Mortem o Disaster Recovery

Requisito	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.
Obiettivi	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.
Caratteristiche e posizione nella scheda	▪ Alla sez. 4.2 sono richieste informazioni relative a documenti specifici, così articolate: ○ Una descrizione sintetica della documentazione da produrre ○ Il tipo di documenti prodotti, case studies di eventi critici o test di DR ○ I singoli documenti prodotti, che saranno allegati alla sottomissione ▪ Alla sez. 4.5, al punto uno delle "Dichiarazioni", è richiesta l'autocertificazione che non si siano verificati eventi critici negli ultimi 24 mesi
Cosa prevedere	La descrizione deve essere strettamente attinente a quanto richiesto. Nel caso in cui si siano verificati situazioni critiche negli ultimi 24 mesi, vanno prodotti almeno due case studies che devono includere: ▪ il riferimento ad un piano di ripristino; ▪ i requisiti di ripristino contenuti nel piano; ▪ le procedure operative di ripristino contenute nel piano; ▪ la cronologia degli eventi; ▪ l'esito del ripristino rispetto ai requisiti. Se non si sono registrate situazioni critiche negli ultimi 24 mesi, va prodotta analoga documentazione riferita ai test di Disaster Recovery. Questa deve contenere almeno: ▪ il riferimento ad un piano di ripristino; ▪ i requisiti di ripristino contenuti nel piano; ▪ la procedura operativa di ripristino oggetto di test; ▪ la cronologia del test; ▪ l'esito del test rispetto ai requisiti.

2.1.2 RO2 – Certificazione ISO 9001

Requisito	Il Fornitore Cloud deve essere in possesso della certificazione ISO 9001 per la gestione della qualità aziendale.
Obiettivi	Dimostrare di utilizzare un adeguato sistema di gestione della qualità, applicato all'erogazione dei servizi offerti.
Caratteristiche e posizione nella scheda	▪ Alla sez. 4.2 sono richieste informazioni relative alla certificazione ISO 9001, così articolate: ○ il numero della certificazione ○ la data scadenza nel formato gg/mm/aaaa ○ il link alla banca dati online o al registro pubblico dell'organismo nazionale di accreditamento dal quale risulta il conseguimento e la validità della certificazione ○ una copia del certificato da allegare alla sottomissione ▪ Alla sez. 4.5, al punto due delle "Dichiarazioni", è richiesta l'autocertificazione che l'azienda sia in possesso della certificazione ISO 9001 e che tale certificazione sia stata rilasciata da un organismo di accreditamento riconosciuto dalla Unione Europea
Cosa prevedere	Sottolineando che il fornitore deve essere in possesso del certificato ISO 9001 all'atto della sottomissione, questo deve rispettare le seguenti condizioni: ▪ oggetto e versione del certificato devono essere inerenti alla norma ▪ in caso di ente certificatore italiano, questo deve compreso in quelli riconosciuti da Accredia ▪ parimenti gli enti certificatori europei devono essere accreditati presso gli enti analoghi ad Accredia presenti nei vari stati e membri dell'European Accreditation (http://www.european-accreditation.org/) ▪ data di validità del certificato non inferiore alla data di richiesta di sottomissione del servizio da qualificare Le informazioni inserite dal CSP all'atto della sottomissione, devono essere consistenti rispetto a quelle presenti e consultabili sul sito dell'ente certificatore.

2.1.3 RO5 – Documentazione tecnica e di supporto

Requisito	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.
Obiettivo	Fornire gli elementi utili circa la presenza di documentazione tecnica al servizio e alle relative modalità di fruizione.
Caratteristiche e posizione nella scheda	▪ Alla sez. 5.1.3, dedicata alle informazioni riguardanti l'utilizzo del servizio, viene richiesto di inserire una breve descrizione della documentazione tecnica fornita a corredo. Questa può includere: ○ le API dei servizi ○ un'eventuale GUI del servizio ○ un'eventuale GUI del servizio vanno poi inseriti ○ il link alla pagina web, se la documentazione è pubblicata in rete ○ i formati cui è resa disponibile, se consultabile offline ○ l'elenco delle lingue in cui è fruibile.
Cosa prevedere	Nella descrizione richiesta, va riportato un elenco dei documenti che sono disponibili a corredo del servizio, insieme ad una loro breve descrizione. Le pagine referenziate dai link, devono riguardare il servizio cloud oggetto di sottomissione ed i contenuti devono essere di natura tecnica utili ad accompagnare l'utilizzo del servizio da parte degli utenti della PA.

2.1.4 RO6 – Processo di Change Management

Requisito	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.
Obiettivi	Dare evidenza che vengono utilizzate procedure formali che disciplinano la gestione del cambiamento. Il processo di change management che viene utilizzato, è indipendente dal singolo servizio che viene inserito nella sottomissione. L'autocertificazione circa l'adozione del processo è un adempimento richiesto anche sul singolo servizio.
Caratteristiche e posizione nella scheda	▪ Alla sez. 4.2 sono richieste informazioni relative a documenti specifici, così articolate: ○ Una descrizione sintetica della documentazione da produrre, da cui sia possibile ricavare che il fornitore Cloud applica adeguati e consolidati processi di change management, evidenziando in particolare la presenza di un CAB e la sua composizione, le tematiche sottoposte all'attenzione del CAB, la frequenza con cui si riunisce ○ I singoli documenti prodotti, che saranno allegati alla sottomissione ▪ Alla sez. 4.5, al punto tre delle "Dichiarazioni", è richiesta l'autocertificazione che l'azienda applichi regolarmente i processi di change management, secondo le modalità operative descritte nel paragrafo 4.2 ▪ Alla sez. 5.2, al punto cinque delle dichiarazioni relative ai requisiti organizzativi che descrivono il singolo servizio, è richiesta l'autocertificazione che le procedure e i metodi standard relativamente alla gestione tempestiva ed efficiente di ogni cambiamento, siano applicate nell'ambito del servizio Cloud secondo quanto inserito alla sez. 4.2.
Cosa prevedere	La documentazione allegata o di riferimento deve essere in italiano, ovvero deve essere resa disponibile una traduzione, anche per estratto. Il documento deve esprimere almeno i seguenti elementi: ▪ l'esistenza di un processo formale contestualizzato sulla realtà del fornitore ▪ la categorizzazione dei change ▪ il processo di comunicazione ▪ il processo di tracciatura dei change Non sono ritenute attinenti esclusive descrizioni generiche del processo, riferite alle definizioni di standard internazionali, quali ad esempio ITIL, senza che essi siano declinati rispetto al servizio cloud da qualificare.

2.1.5 RO9 – Processo di Configuration Management

Requisito	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.
Obiettivi	Porre in risalto l'adozione di procedure formali che disciplinano la gestione delle configurazioni. L'autocertificazione circa l'adozione del processo è un adempimento richiesto sul singolo servizio.
Caratteristiche e posizione nella scheda	▪ Alla sez. 5.2 sono richieste informazioni relative a documenti specifici, così articolate: ○ Una descrizione sintetica della documentazione da produrre, che dimostri l'adozione da parte del fornitore di procedure standard e relativi tool attraverso cui viene eseguito il controllo di tutte le componenti rilevanti del servizio. La documentazione deve essere coerente con le buone pratiche presenti nello standard ISO/IEC 20000-2. Se in possesso della certificazione ISO/IEC 20000-2, è possibile indicare il numero e la scadenza, nonché allegarla alla documentazione a corredo ○ I singoli documenti prodotti, che saranno allegati alla sottomissione ▪ Alla sez. 5.2, al punto nove delle dichiarazioni relative ai requisiti organizzativi che descrivono il singolo servizio, è richiesta l'autocertificazione che i processi della configurazione, siano conformi alle buone pratiche presenti nello standard ISO/IEC 20000-2.
Cosa prevedere	La documentazione allegata o di riferimento deve essere in italiano, ovvero deve essere resa disponibile una traduzione, anche per estratto. Il documento deve esprimere almeno i seguenti elementi: ▪ l'esistenza di un processo formale, contestualizzato sulla realtà del fornitore ▪ la categorizzazione degli asset ▪ il processo di comunicazione ▪ un sistema di tracciatura delle informazioni relative agli asset Non sono ritenute attinenti esclusive descrizioni generiche del processo, riferite alle definizioni di standard internazionali, quali ad esempio ITIL, senza che essi siano declinati rispetto al servizio cloud da qualificare.

2.1.6 RO10 – Processo di Incident e Problem Management

Requisito	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).
Obiettivi	Evidenziare l'adozione di procedure formali che disciplinano la gestione degli incident, legati alla sicurezza e ai componenti dell'infrastruttura. Il processo di incident management è indipendente dal singolo servizio che viene inserito nella sottomissione. L'autocertificazione circa l'adozione del processo è però richiesta anche sul singolo servizio.
Caratteristiche e posizione nella scheda	▪ Alla sez. 4.2 sono richieste informazioni relative a documenti specifici, così articolate: ○ Una descrizione sintetica della documentazione da produrre, in cui il Fornitore Cloud illustra i processi adottati per la gestione degli incident nell'ambito dell'infrastruttura Cloud (incident & problem management). La documentazione deve rispettare gli standard di sicurezza internazionali (p.e. ISO/IEC 27002, ISO/IEC 27035). Se in possesso di tali certificazioni, è possibile indicarne il numero, la scadenza e allegarle alla documentazione ○ I singoli documenti che saranno acclusi alla sottomissione ▪ Alla sez. 4.5, al punto quattro delle "Dichiarazioni", è richiesta l'autocertificazione che l'azienda adotti processi di gestione degli incidenti coerenti con quanto raccomandato dagli standard di sicurezza internazionali (ad es. ISO/IEC 27002, ISO/IEC 27035), secondo quanto inserito alla sez. 4.2 ▪ Alla sez. 5.2, al punto dieci delle dichiarazioni relative ai requisiti organizzativi che descrivono il singolo servizio, è richiesta l'autocertificazione che i processi di gestione degli incident siano coerenti con quanto raccomandato dagli standard di sicurezza internazionali (ad es. ISO/IEC 27002, ISO/IEC 27035), secondo quanto inserito alla sez. 4.2.
Cosa prevedere	La documentazione allegata o di riferimento deve essere in italiano, ovvero deve essere resa disponibile una traduzione, anche per estratto. Il documento deve esprimere almeno i seguenti elementi: ▪ l'esistenza di un processo formale, contestualizzato sulla realtà del fornitore ▪ la categorizzazione degli incident per severità ▪ il sistema di tracciatura delle azioni di risoluzione ▪ un esempio di stesura di un Report Post-Mortem completo ▪ il processo di Problem Management e Continuous Improvement Non sono ritenute attinenti esclusive descrizioni generiche del processo, riferite alle definizioni di standard internazionali, quali ad esempio ITIL, senza che essi siano declinati rispetto al servizio cloud da qualificare.

2.1.7 RSI 1 – Certificazione ISO/IEC 27001

Requisito	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.
Obiettivi	Dimostrare di essere in grado di erogare i servizi proposti dal punto di vista tecnologico, rispettando i requisiti specifici concernenti sicurezza, privacy e protezione dei dati.
Caratteristiche e posizione nella scheda	▪ Alla sez. 4.1, viene richiesto: ○ L'elenco degli standard di sicurezza riferiti al Data Center ○ Una descrizione dell'approccio utilizzato per eseguire i penetration test ○ La frequenza con cui sono eseguiti i penetration test ▪ Alla sez. 4.3, dedicato alla sicurezza, è previsto: ○ Il numero della certificazione ISO/IEC 27001 ○ La scadenza del certificato ○ Il link alla banca dati online o al registro pubblico dell'organismo nazionale di accreditamento dal quale risulta il conseguimento e la validità della certificazione ○ il caricamento del certificato ISO/IEC 27001, con l'estensione dei controlli standard ISO/IEC 27017 e ISO/IEC 27018 relativamente all'infrastruttura Cloud ▪ Alla sez. 4.5, al punto cinque delle "Dichiarazioni", l'autocertificazione che il fornitore sia in possesso della ISO/IEC 27001 estesa con i controlli degli standard ISO/IEC 27017 e ISO/IEC 27018; e che questa sia stata rilasciata da un organismo di accreditamento riconosciuto dalla Unione Europea.
Cosa prevedere	Sottolineando che il fornitore deve essere in possesso del certificato ISO 27001 all'atto della sottomissione, questo deve rispettare le seguenti condizioni: ▪ oggetto e versione del certificato devono essere inerenti alla norma ISO 27001 ▪ in caso di ente certificatore italiano, questo deve compreso in quelli riconosciuti da Accredia ▪ parimenti gli enti certificatori europei devono essere accreditati presso gli enti analoghi ad Accredia presenti nei vari stati e membri del dell'European Accreditation (http://www.european-accreditation.org/). ▪ data di validità del certificato non inferiore alla data della sottomissione Le informazioni inserite dal CSP all'atto della sottomissione, devono essere consistenti rispetto a quelle presenti e consultabili sul sito dell'ente certificatore.

2.1.8 RIP2 – Documentazione tecnica API

Requisito	Il Fornitore Cloud rende disponibile una adeguata documentazione tecnica delle API che ne chiarisce l'utilizzo.
Obiettivi	Fornire i riferimenti della documentazione tecnica delle API in formato WEB o in altro formato.
Caratteristiche e posizione nella scheda	▪ Alla sez. 5.1.3, dedicato alle informazioni riguardanti l'utilizzo del servizio, vanno indicate tutte le opzioni soddisfatte tra quelle previste: ○ L'elenco degli standard di sicurezza riferiti al Data Center ○ Una descrizione dell'approccio utilizzato per eseguire i penetration test ○ La frequenza con cui sono eseguiti i penetration test ▪ Alla sez. 4.3, dedicato alla sicurezza, è previsto: ○ url degli endpoint SOAP e/o REST ○ presenza di meccanismi di autenticazione ○ url della documentazione consultabile sulla rete, se disponibile ○ disponibilità di documentazione in altri formati ○ disponibilità di un ambiente di test delle API Vanno poi specificate le funzionalità invocabili tramite API di tipo SOAP/ REST e le eventuali funzionalità che non sono accessibili per mezzo di tali API ▪ Alla sez. 5.3, al punto due delle "Dichiarazioni" relative ai requisiti di Interoperabilità e Portabilità, l'autocertificazione che la documentazione tecnica aggiornata delle API verrà rilasciata e resa disponibile alla PA acquirente contestualmente ad ogni rilascio di nuove versioni delle API medesime.
Cosa prevedere	Gli allegati che vengono forniti devono prevedere: ▪ i metodi espliciti di chiamata alle API ▪ ogni istruzione sia descritta nella sua funzionalità ▪ esempi pratici di utilizzo e relativo output atteso ▪ informazioni di supporto alla risoluzione di problemi nell'utilizzo delle API.

2.2 SERVIZI CLOUD DI TIPO SaaS

Nell'ambito dei servizi di tipo SaaS, sono stati individuati i seguenti requisiti:

- RO3 (Documentazione tecnica)
- RO6 (Informazioni tecniche su Monitoraggio e Logging)
- RS2 (Certificazione ISO/IEC 27001 o CSA Star Self-Assessment2)
- RIP1 (Funzionalità API)
- RIP5 (Procedure di reversibilità)
- RCL1 (Conformità GDPR)

2.2.1 RO3 – Documentazione tecnica

Requisito	Il Fornitore SaaS assicura la disponibilità di manuali tecnici e guide d'uso (e/o altro materiale di supporto), ivi compresa la documentazione tecnica delle API e delle interfacce SOAP/REST, specificando se disponibili anche in lingua italiana.
Obiettivi	Fornire i riferimenti alla documentazione tecnica del servizio resa disponibile dal fornitore.
Caratteristiche e posizione nella scheda	▪ Alla sez. 3.1.3, dedicato alle informazioni riguardanti l'utilizzo del servizio, vanno indicate tutte le opzioni soddisfatte tra quelle previste: ○ url della documentazione consultabile sulla rete in modalità pubblica ○ eventuale disponibilità di documentazione in altri formati ○ l'elenco delle lingue in cui è disponibile la documentazione tecnica Per quanto riguarda le API: ○ o url degli endpoint SOAP e/o REST ○ o presenza di meccanismi di autenticazione ○ o url della documentazione consultabile sulla rete, se disponibile ○ o disponibilità di documentazione in altri formati ○ o disponibilità di un ambiente di test Vanno poi specificate le funzionalità invocabili tramite API di tipo SOAP/REST e le funzionalità che non sono accessibili per mezzo di tali API ▪ Alla sez. 3.2, al punto cinque delle dichiarazioni relative ai requisiti organizzativi, l'autocertificazione che la documentazione tecnica messa a disposizione della PA acquirente è sempre aggiornata e coerente con la versione del servizio in esercizio.
Cosa prevedere	È necessario specificare almeno una lingua in cui è resa disponibile la documentazione tecnica. Se fruibili on line, i manuali che espongono il funzionamento delle API e delle interfacce SOAP/REST oltre ad alcuni esempi di utilizzo, devono contenere una descrizione chiara: ▪ delle istruzioni ammesse ▪ dei metodi di chiamata ▪ dei parametri di input ▪ dei messaggi di risposta.

2.2.2 RO6 – Informazioni tecniche su monitoraggio e logging

Requisito	Il Fornitore SaaS rende disponibile l'accesso a strumenti di monitoraggio e di logging, consentendo all'Acquirente di filtrare e limitare i risultati agli eventi di suo interesse
Obiettivi	Rendere disponibile al fruitore, gli strumenti relativi al monitoraggio delle risorse, dei costi e della qualità del servizio.
Caratteristiche e posizione nella scheda	▪ Alla sez. 3.1.5, in cui vanno inserite le informazioni relative a trasparenza, metriche e statistiche di utilizzo riguardanti l'utilizzo, vanno indicate le seguenti informazioni: ○ descrizione degli strumenti di monitoraggio messi a disposizione ○ metriche e statistiche disponibili relativi al funzionamento del servizio, inclusi gli elementi che fanno riferimento agli strumenti di monitoraggio ○ elenco e breve descrizione dei report ▪ Alla sez. 3.2, al punto nove delle dichiarazioni relative ai requisiti organizzativi, l'autocertificazione che viene reso disponibile 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 la PA acquirente.
Cosa prevedere	Gli strumenti, le relative metriche e i report messi a disposizione devono riguardare il monitoraggio di: ▪ risorse ▪ costi ▪ funzionamento del servizio L'elenco dei report messi a disposizione può riportare anche le url se consultabili in rete e/o la periodicità in cui vengono prodotti.

2.2.3 RS2 – Certificazione ISO/IEC 27001 o CSA Star Self-Assessment2

Requisito	Il Fornitore SaaS 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. In alternativa, il Fornitore SaaS effettua il CSA STAR Self-Assessment2 con riferimento al servizio che intende qualificare (nella versione denominata CAIQ), ne produce la relativa documentazione e la rende pubblicamente consultabile sul proprio sito Web.
Obiettivi	Dimostrare di essere in grado di erogare i servizi proposti dal punto di vista tecnologico, rispettando i requisiti specifici concernenti sicurezza, privacy e protezione dei dati.
Caratteristiche e posizione nella scheda	▪ Alla sez. 3.2, Requisiti Organizzativi e di Sicurezza, va selezionata una delle due opzioni: ○ se si è in possesso della certificazione secondo lo standard ISO/IEC 27001 estesa con i controlli degli standard ISO/IEC 27017 e ISO/IEC 27018 ○ se è stato effettuato CSA STAR Self-Assessment relativo alla sicurezza Cloud Sulla base della selezione effettuata, va caricato il file che attesta la relativa certificazione e nel caso di CSA STAR Self-Assessment, anche la url del sito del fornitore presso cui è reperibile il certificato.
Cosa prevedere	Nel caso in cui si fornisca la certificazione ISO/IEC 27001, estesa con i controlli degli standard 27017 e 27018, è necessario rispettare i seguenti requisiti: ▪ essere disponibile all'atto della sottomissione ▪ l'oggetto e la versione devono essere coerenti con il requisito ▪ la data di validità deve essere maggiore della data di sottomissione ▪ l'ente certificatore deve essere presente tra i soggetti accreditati membri dell'European Accreditation ▪ in caso di ente certificatore italiano, questo deve compreso in quelli riconosciuti da Accredia ▪ parimenti gli enti certificatori europei devono essere accreditati presso gli enti analoghi ad Accredia presenti nei vari stati e membri del dell'European Accreditation (http://www.european-accreditation.org/)

Nel caso in cui si fornisca la documentazione relativa al CSA STAR Self-Assessment è necessario rispettare i seguenti requisiti:

- essere disponibile all'atto della sottomissione
- l'oggetto e la versione devono essere coerenti con il requisito
- La documentazione deve essere coerente a quanto pubblicato sul sito "Cloud Security Alliance" https://cloudsecurityalliance.org/star/registry/
- La URL indicata deve referenziare il sito Web del fornitore SaaS presso il quale è stato pubblicato il CSA STAR Self-Assessment.

2.2.4 RIP1 – Funzionalità API

Requisito	Il Fornitore SaaS dichiara che il servizio SaaS espone opportune Application Programming Interface (API) di tipo SOAP e/o REST associate alle funzionalità applicative, di gestione e configurazione del servizio.
Obiettivi	Fornire i riferimenti della documentazione tecnica delle API in formato WEB o in altro formato.
Caratteristiche e posizione nella scheda	▪ Alla sez. 3.1.3, dedicato alle informazioni riguardanti l'utilizzo del servizio, vanno indicate tutte le opzioni soddisfatte tra quelle previste: ○ url degli endpoint SOAP e/o REST ○ presenza di meccanismi di autenticazione ○ url della documentazione consultabile sulla rete, se disponibile ○ disponibilità di documentazione in altri formati ○ disponibilità di un ambiente di test della API Vanno poi specificate le funzionalità invocabili tramite API di tipo SOAP/REST e le funzionalità che non sono accessibili per mezzo di tali API ▪ Alla sez. 3.3, ai punti uno, due e tre dei Requisiti di Interoperabilità e Portabilità: ○ il servizio espone 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, i cui dettagli sono stati forniti nel par. 3.1.3 ○ in caso di aggiornamento delle funzionalità del servizio e/o delle relative API viene garantita la tracciabilità delle diverse versioni delle API disponibili (versioning) ○ le richieste SOAP/REST ricevute dal servizio e il loro esito sono tracciabili tramite sistemi di logging e accounting.
Cosa prevedere	Gli allegati che vengono forniti devono prevedere: ▪ i metodi espliciti di chiamata alle API ▪ ogni istruzione sia descritta nella sua funzionalità ▪ esempi pratici di utilizzo e relativo output atteso ▪ informazioni di supporto alla risoluzione di problemi nell'utilizzo delle API.

2.2.5 RIP5 – Procedure di reversibilità

Requisito	Il Fornitore SaaS dettaglia le procedure per garantire la reversibilità del servizio SaaS.
Obiettivi	Garantire la reversibilità del servizio SaaS, attraverso un insieme di procedure definite a tale scopo e consolidate.
Caratteristiche e posizione nella scheda	▪ Alla sez. 3.1.2, dedicato alle informazioni riguardanti l'utilizzo del servizio, vanno indicate quanto segue: ○ tempi di attivazione e disattivazione ○ le modalità ed il processo di attivazione ○ le modalità ed il processo di disattivazione ○ le tempistiche e le modalità con cui è possibile estrarre i dati gestiti e memorizzati dal servizio a conclusione della fornitura ○ l'elenco dei formati in cui è possibile estrarre i dati ○ le tempistiche, le modalità e i formati di altri asset correlati all'utilizzo del servizio, quali dati derivati, virtual machines, container descriptor files, ecc con cui è possibile estrarre i dati gestiti e memorizzati dal servizio a conclusione della fornitura ▪ Alla sez.3.1.3, dedicato alle informazioni riguardanti l'utilizzo del servizio, va inserito quanto segue: ○ una descrizione sintetica delle procedure messe a disposizione per consentire la reversibilità del servizio ○ I singoli documenti prodotti, che saranno allegati alla sottomissione ▪ Alla sez. 3.3, al punto otto dei Requisiti di Interoperabilità e Portabilità va autocertificato che i dettagli circa le procedure per garantire la reversibilità del servizio SaaS sono quelli specificati par. 3.1.3.
Cosa prevedere	Le informazioni previste: ▪ nella sezione 3.1.2 devono essere chiare, trasparenti e coerenti alle procedure di reversibilità. Vanno indicate le modalità operative e la descrizione sintetica dei processi che sottendono all'attivazione e alla disattivazione del servizio SaaS. ▪ la sezione 3.1.3 deve includere un estratto della procedura di reversibilità, meglio dettagliata nel documento allegato. In particolare, il documento allegato deve contenere una descrizione del processo dando rilievo: ○ alla cessazione del rapporto contrattuale ○ alle modalità di recupero dei dati ○ le fasi operative della procedura di reversibilità.

2.2.6 RCL1 – Conformità GDPR

Requisito	Il Fornitore SaaS specifica per quali aspetti il servizio SaaS è conforme agli obblighi e agli adempimenti previsti dalla normativa europea e italiana in materia di protezione dei dati personali.
Obiettivi	Affermare che vengono impiegati gli obblighi e gli adempimenti in materia di protezione dei dati personali.
Caratteristiche e posizione nella scheda	▪ Alla sez. 3.1.7, dedicato alle informazioni riguardanti l'utilizzo del servizio, vanno indicate le seguenti informazioni: ○ la dichiarazione che il servizio è conforme agli obblighi e agli adempimenti previsti ○ le informazioni di dettaglio circa gli aspetti del servizio conformi alla normativa europea e italiana in materia dei dati personali ed in particolare al GDPR ○ l'eventuale adesione a uno o più codici di condotta di cui agli art. 40 e 41 del GDPR ▪ Alla sez. 3.4, al punto otto dei Requisiti di Conformità Legislativa va autocertificato che le informazioni di dettaglio sugli aspetti del servizio sono conformi agli obblighi e agli adempimenti previsti dalla normativa (europea e italiana) in materia di protezione dei dati personali ed in particolare al GDPR sono quelle specificate alla sez. 3.1.7.
Cosa prevedere	Fra le informazioni di dettaglio da fornire in merito al trattamento dei dati personali, possono essere incluse: ▪ le modalità in cui i dati vengono conservati ed eventualmente archiviati ▪ le misure di sicurezza predisposte in caso di accesso non autorizzato ▪ la presenza di strumenti per monitorare i livelli di sicurezza dei dati ▪ le tempistiche e le modalità con cui vengono gestite e comunicate le eventuali violazioni dei dati ▪ le modalità attraverso cui è possibile restringere l'accesso ai dati ▪ le coperture assicurative in relazione al rischio privacy