

AS SDAPA PER L'ACQUISIZIONE DI SERVIZI CLOUD AZURE
DEL CATALOGO MICROSOFT AZURE DA IMPIEGARE PER I
PRODOTTI E SERVIZI EROGATI DA PAGOPA S.P.A.

CAPITOLATO TECNICO INTEGRATIVO

1. GLOSSARIO, ACRONIMI E TERMINOLOGIA	5
GLOSSARIO	5
ACRONIMI	5
TERMINOLOGIA	6
2. INTRODUZIONE	7
3. DEFINIZIONE DEL FABBISOGNO	8
4. OGGETTO, DURATA E CONTESTO TECNOLOGICO	9
4.1. Oggetto	9
4.2. Durata	9
4.3. Servizi Cloud Computing IaaS	9
4.3.1. IaaS: Servizi di Elaborazione (compute instance)	10
4.3.2. IaaS: Servizi di Archiviazione (storage)	10
4.3.4. IaaS: VPN Gateway	10
4.3.5. IaaS: IP Pubblici	10
4.3.6. IaaS: Traffico in Uscita (outbound)	11
4.4. Servizi Cloud Computing PaaS	11
4.4.1. Macro categorie del catalogo dei servizi	12
4.4.2. Servizi di Piattaforma a Supporto Gestione IaaS	12
4.4.2.1. VPN – GW Service (Azure VPN Gateway)	12
4.4.2.2. Load Balancing Service (Azure Load Balancer)	13
4.4.2.3. Security Monitoring Service (Azure Security Center, Azure Log Analytics)	13
4.4.2.4. Application Monitoring Service (Azure Monitoring, Application Insight)	13
4.4.2.5. Auditing Service (Azure Log Analytics, Azure Sentinel, Azure Advisor, Azure Security Center)	13
4.4.2.6. Application log service (Azure Log Service)	14
4.4.2.7. Security service (Azure Security Center)	14
4.4.2.8. Backup Service (Azure Backup)	14

4.4.2.9. DR Automation Service (Azure Site Recovery)	14
4.4.2.10. Strumenti per lo sviluppo (Azure Visual Studio, Azure DevOps, Azure SDK, Azure DevTest Lab, Azure Pipelines)	14
4.4.3. Servizi di Piattaforma abilitanti al cloud native	14
4.4.3.1. Web Application (Azure App Web Service)	15
4.4.3.2. Dispositivi Mobili (Azure App per dispositivi Mobili, API Mgmt, App Service)	15
4.4.3.3. Relational Database as a service (Azure MySQL e Azure Postgres)	15
4.4.3.4. Multi-Modal Database Service (Azure Cosmos DB)	15
4.4.3.5. In memory data archive service (Azure Cache for Redis)	15
4.4.3.6. Shared Filesystem service (Azure File Service)	15
4.4.3.7. Large object service (Azure BLOB Storage Service)	15
4.4.3.8. Datalake Storage Service (Azure Datalake Storage – Azure Datalake Analytics)	15
4.4.3.9. Analisi dei dati (Azure Power BI Embedded)	16
4.4.3.10. WAF Service (Azure Application Gateway)	16
4.4.3.11. IDM Service (Azure Active Directory)	16
4.4.3.12. Key Management Service (Azure Key Vault)	16
4.4.3.13. API Management Service (Azure Api Gateway)	16
4.4.3.14. Container Registry Service (Azure Container Registry)	16
4.4.3.15. Container service (Azure Kubernetes Service)	17
4.4.3.16. Serverless computings (Azure Service Fabric, Azure Functions)	17
4.4.3.17. Messaging queue service (Azure Message Bus)	17
4.4.3.18. Search service (Azure Search Service)	17
4.4.3.19. Cognitive Service (Azure Cognitive Service)	18
4.4.3.20. Altri servizi	18
5. EROGAZIONE DEI SERVIZI	18
5.1. Requisiti di qualità	19
5.2. Responsabile della fornitura	19
6. ESECUZIONE DELLA FORNITURA	21

6.1. Modalità di esecuzione della fornitura	21
6.1.1. Modalità di erogazione continuativa	21
6.1.2. Livelli di servizio	22
6.2. Pianificazione e Consuntivazione	22
6.3. Azioni contrattuali	22
6.4. Exit strategy e Grace period	23

1. GLOSSARIO, ACRONIMI E TERMINOLOGIA

GLOSSARIO

Amministrazione Committente	o PagoPA SpA
Impresa o Fornitore	La società affidataria della presente procedura
Contratto	Il contratto che verrà stipulato tra l'Amministrazione e il Fornitore, dove sono enunciate le regole giuridiche alle quali si dovrà conformare la fornitura
Fornitura	Il complesso dei servizi e delle attività descritte nel presente documento tecnico.
Malfunzionamento	Qualsiasi anomalia funzionale del software e, in ogni caso, ogni difformità del prodotto in esecuzione rispetto alla relativa documentazione tecnica e manualistica d'uso.
Responsabile Fornitura	della La persona individuata dall'Impresa come interlocutore e responsabile di tutte le attività contrattuali.

ACRONIMI

MAC	Manutenzione Correttiva
MEV	Manutenzione Evolutiva

TERMINOLOGIA

Attivazione	Comunicazione di nuove esigenze, quindi della partenza di un nuovo task.
--------------------	--

Attività	Quota parte di un servizio contrattuale, omogenea per tipologia, alla quale si applica una ben definita modalità di esecuzione
Autorizzazione	Assenso a procedere con le attività sul singolo task, secondo la stima e la pianificazione proposte dal fornitore.
Consegna	Rilascio dei prodotti di fornitura, sia intermedi che finali.
Difetto	Errore presente sull'applicazione, latente finché non rilevato, la cui rimozione è a carico della manutenzione correttiva.
Modalità esecuzione di	Complesso di regole e clausole che regolano la prestazione dei servizi e delle attività oggetto della fornitura
Task	Una o più attività o interventi volta a soddisfare specifiche esigenze dell'Amministrazione.

2. INTRODUZIONE

Il presente capitolato è parte integrante della documentazione della presente procedura e definisce le caratteristiche e i requisiti richiesti per l'acquisizione di servizi Cloud dal Cloud pubblico di Microsoft Azure per i prodotti e servizi erogati dalla Committente.

Le condizioni di cui al presente documento, gli atti e i documenti ivi richiamati, ancorché non materialmente allegati, costituiscono parte integrante e sostanziale del Contratto.

Le prescrizioni del presente capitolato rappresentano i requisiti minimi dell'affidamento.

3. DEFINIZIONE DEL FABBISOGNO

Il Committente già dispone di sottoscrizioni nel Cloud pubblico (Microsoft Azure) utilizzate per erogare i propri prodotti e servizi ad utenti interni, a cittadini e a Pubbliche Amministrazioni.

Nell'ambito del piano di trasformazione digitale intrapreso dal Committente, infatti, è stato previsto che alcune *le* iniziative progettuali utilizzino, inter alia, servizi IaaS, PaaS e SaaS, attraverso l'acquisizione di servizi Cloud da utilizzare per la realizzazione di sistemi moderni e *cloud native*.

In linea con le previsioni AgID si considera di riferimento il Modello Cloud della PA, nel quale è possibile individuare i servizi Cloud e CSP qualificati, consultabili mediante il Cloud Marketplace, suddivisi in IaaS, PaaS e SaaS.

Nella definizione dei servizi Cloud da acquisire, è necessario mantenere un legame con un specifico service provider, nel caso di specie Microsoft Azure, per le forti dipendenze tecnologiche che si sono venute a creare tra lo sviluppo applicativo custom e le interfacce di alcuni servizi PaaS (Azure Search, Azure API Gateway, Azure CosmosDB, ecc.), il cui adeguamento richiede ingenti investimenti economici e, soprattutto, interventi progettuali della durata di circa 12-18 mesi.

4. OGGETTO, DURATA E CONTESTO TECNOLOGICO

L'iniziativa di acquisizione ha per oggetto servizi Cloud IaaS, PaaS e SaaS del Cloud pubblico Microsoft Azure volti a soddisfare le seguenti esigenze:

- continuità dei workload cloud-native delle applicazioni già realizzate ovvero in corso di realizzazione, attraverso servizi PaaS e SaaS (Microsoft Azure);
- sviluppo di nuovi workload cloud-native.

4.1. Oggetto

L'oggetto dell'esigenza espressa dal committente, riguarda l'acquisizione di servizi del Cloud Pubblico Microsoft Azure, ed in particolare l'acquisizione di servizi Cloud Azure, **tramite iscrizione Server and Cloud Enrollment**, fino ad un massimale ("Massimale") di € 1.500.000,00 oltre IVA per un periodo di 36 mesi dall'attivazione del Contratto. La Committente nell'ambito del Massimale potrà liberamente fruire di tutti i servizi Cloud Azure di cui necessita in base alle proprie esigenze. I servizi pertanto saranno remunerati solo ed esclusivamente in base all'effettivo consumo degli stessi da parte della Committente.

4.2. Durata

La durata contrattuale prevista è pari a 36 mesi dall'attivazione dei servizi, così come disciplinato all'art. 3 dello Schema di Contratto.

4.3. Servizi Cloud Computing IaaS

Tali articoli hanno la finalità di garantire alla Committente un catalogo di servizi in cui le funzionalità cloud offerte sono di tipo infrastrutturale, con la possibilità di disporre di modalità di acquisizione autonome e in modo programmatico di risorse di computing, di storage e networking.

Si assume che i servizi IaaS proposti siano erogati da un unico CSP (Microsoft Azure) per garantire la continuità dei servizi e la possibilità di migrazione di questi workload su altro ecosistema. Inoltre, è necessario che tali servizi siano fruibili da almeno 2 distinti siti geografici di localizzazione delle risorse, su territorio europeo e con distanza adeguata alla realizzazione di soluzioni di disaster recovery. Le esigenze sono quindi espresse identificando i fabbisogni per entrambi i siti geografici di localizzazione delle risorse, che saranno nel seguito identificati genericamente come Sito Cloud Primario e Sito Cloud Secondario. Il dimensionamento massimo stimato per i servizi, riferito all'intera durata

contrattuale, è al meglio delle conoscenze attuali. Tale dimensionamento si intende pertanto non vincolante, riservandosi il committente di:

- non attivare i servizi;
- attivare i servizi in misura maggiore o minore rispetto a quanto di seguito riportato.

4.3.1. IaaS: Servizi di Elaborazione (compute instance)

Per i servizi di elaborazione richiesti si assume il BYOL di tutte le licenze di sistema operativo. Nella definizione del fabbisogno di servizi computazionali si assumono sempre inclusi – quindi non associati ad ulteriori oneri oltre il costo del singolo servizio– servizi di virtual networking e virtual firewalling di base. Sono invece esclusi fabbisogni relativi a licenze o subscription – anche in forma pay-as-you-go – di sistema operativo. Si ritiene comunque di interesse, in ottica evolutiva dei servizi da attivare in Cloud, l'avere visibilità dell'incremento di costo legato all'attivazione delle istanze con licenze o subscription – anche in forma pay-as-you-go – di sistema operativo.

4.3.2. IaaS: Servizi di Archiviazione (storage)

Tra i fabbisogni IaaS censiti rientrano i servizi di archiviazione, organizzati nelle tipologie seguenti:

- block storage, a supporto delle istanze compute attivate in modalità reserved e onDemand;
- Storage di file, per le applicazioni che devono poter accedere a file condivisi e richiedono un file system;
- Cold storage, a supporto della conservazione dei dati di back up o comunque di dati con requisiti di conservazione a lungo termine e bassa frequenza di accesso.

4.3.4. IaaS: VPN Gateway

Per assolvere alla necessità di stabilire – attraverso la rete Internet pubblica – connessioni IPsec sicure e crittografate verso reti cloud virtuali, e verso altre reti nella disponibilità del committente (on premise, ovvero altre reti in cloud) sono stati stimati i seguenti fabbisogni:

- n.2 gateway sul sito cloud primario;
- n.2 gateway sul sito cloud secondario;

ciascuno attivo per l'intera durata della fornitura.

4.3.5. IaaS: IP Pubblici

Per consentire la comunicazione in ingresso verso specifiche risorse Cloud (o la comunicazione in uscita mediante specifico IP) è stato formulato il fabbisogno di servizi di indirizzamento IP pubblico IPv4. Ciascun indirizzo pubblico potrà essere

associato dal Committente ad interfaccia di rete di istanza computazionale, ad un servizio di bilanciamento di carico di rete o applicativo con connessione Internet, ad un gateway VPN, o ad altra risorsa eleggibile per tale associazione.

4.3.6. IaaS: Traffico in Uscita (outbound)

Il fabbisogno in termini di trasferimento dati in uscita, dal sito cloud primario, è stato quantificato nella misura di un massimo di 10 TB/mese per l'intera durata del contratto. In considerazione del carattere di stima del fabbisogno, si rappresenta l'esigenza di avere evidenza delle soluzioni di scalabilità disponibili in offerta. Il traffico in ingresso ed il traffico cross-region si assumono inclusi nei corrispettivi dei servizi IaaS di cui ai precedenti requisiti e senza ulteriori oneri oltre i corrispettivi previsti per i servizi richiesti.

4.4. Servizi Cloud Computing PaaS

Il Committente intende proseguire il percorso evolutivo del proprio contesto IT con la progressiva revisione in ottica cloud based dei workload applicativi attraverso soluzioni in modalità *cloud native*. Per disporre degli strumenti utili a tale ulteriore scenario di intervento, parte della iniziativa di fornitura ha l'obiettivo di definire un catalogo di servizi nel seguito identificati genericamente come PaaS (sebbene per taluni sia applicabile anche la classificazione IaaS) e al quale si farà riferimento sulla base dell'effettivo percorso di attuazione definito. I servizi possono essere raccolti in un catalogo di macro categorie, distinguibili in due sottoinsiemi:

- Servizi a supporto, ovvero servizi per la gestione dello strato cloud IaaS e delle applicazioni;
- Servizi avanzati, abilitanti alle evoluzioni applicative in ottica *cloud native*.

Il Committente si riserva di:

- non attivare in tutto o in parte i servizi elencati nel seguito;
- attivare i servizi in misura maggiore o minore rispetto a quanto di seguito riportato;
- attivare i servizi utilizzando gli effettivi parametri dimensionali degli articoli offerti a copertura delle esigenze indicate;
- attivare i servizi disponibili nelle macro categorie, indipendentemente dalle modifiche al catalogo dei servizi Azure, dovute all'introduzione di nuovi servizi o alle modifiche tecniche e/o commerciali di quelli esistenti.

nel rispetto comunque del massimale contrattuale previsto per il totale dei servizi oggetto del presente paragrafo.

Per ciascun servizio, la modalità di remunerazione (canone, pay-as-you-go) potrà essere definita all'atto della attivazione del servizio stesso e sulla base dell'effettivo consumo.

4.4.1. Macro categorie del catalogo dei servizi

Il fabbisogno Committente riguarda le seguenti macro categorie di servizi PaaS, che dovranno essere completamente disponibili indipendentemente dalle declinazioni specifiche che seguono nei successivi paragrafi:

- Analisi – Raccolta, archiviazione, analisi di qualsiasi tipo di dati;
- Archiviazione – Soluzione di archiviazione dei dati sicura e scalabile;
- Calcolo – capacità di calcolo per specifiche esigenze;
- Container - creazione e gestione integrata dei container;
- Contenuti Multimediali – distribuzione di contenuti Video/audio di alta qualità su qualunque dispositivo;
- Database – Servizi di Database completamente gestiti;
- Desktop Virtuale Windows – Servizi di desktop virtuale;
- Dispositivi Mobili – creazione e gestione di App per dispositivi mobili.
- Gestione e Governance – Monitoraggio delle risorse, Gestione dei costi, definizione delle Politiche, Disaster Recovery;
- Gestione Identità – gestione delle identità per l'accesso ai servizi e strumenti di controllo e di sicurezza;
- Ibrido – Strumenti e servizi per la migrazione o trasferimento dei dati, tra sistemi del Data Center e sistemi del Cloud, Disaster Recovery, archiviazione dei dati remota;
- Integrazione – Servizi di ricerca avanzati, intelligenza artificiale, machine learning, servizi cognitivi, riconoscimento vocale, analisi linguistica, ecc.;
- IoT – Servizi di gestione dei dispositivi, strumenti per il controllo dei dispositivi in un contesto geo spaziale, strumenti per lo sviluppo di App per dispositivi di qualsiasi tipo;
- Rete – Servizi per la definizione di reti locali nel cloud e di interconnessione con il Data Center o con altri Cloud provider, Gateway VPN, Monitoraggio;
- Sicurezza – Servizi di gestione centralizzata della sicurezza per tutti i workload;
- Strumenti per lo sviluppo – strumenti per la produzione e la gestione del ciclo di vita del SW, DevOps, analisi e debug;
- Web – Creazione e gestione di servizi per le applicazioni web.

4.4.2. Servizi di Piattaforma a Supporto Gestione IaaS

Gli articoli elencati in questo paragrafo raccolgono i fabbisogni di servizi Cloud che potranno essere attivati a supporto di una gestione nativa di risorse IaaS e dei workload ospitati.

4.4.2.1. VPN – GW Service (Azure VPN Gateway)

Tale fabbisogno è volto ad assicurare esigenze superiori a quelle considerate nella sezione IaaS.

4.4.2.2. Load Balancing Service (Azure Load Balancer)

Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- bilanciamento del carico altamente affidabile;
- possibilità di definire diverse modalità di bilanciamento;
- utilizzo di SSL off-loading;
- supporto autoscaling automatico;
- supporto definizione metriche/eventi che determinano scale-out o scale-in automatico.

4.4.2.3. Security Monitoring Service (Azure Security Center, Azure Log Analytics)

Il servizio dovrà garantire la disponibilità di funzionalità avanzate di monitoring ed analisi di eventi di sicurezza legati a tentativi di accesso ai sistemi sia infrastrutturali che applicativi al fine di rilevare potenziali minacce di sicurezza. Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- possibilità di raccogliere dati di monitoraggio del sistema operativo guest (e.g., utilizzo CPU, RAM, disco, rete);
- monitoraggio risorse definite nel contesto dello stesso CSP;
- monitoraggio sottoscrizioni ed info relative all'integrità e al funzionamento dei servizi offerti dal CSP, anche a livello di singolo tenant;
- Possibilità di definire eventi e metriche personalizzate e dashboard personalizzate.

4.4.2.4. Application Monitoring Service (Azure Monitoring, Application Insight)

Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- possibilità di raccogliere dati di monitoraggio dell'applicazione relativi alle prestazioni ed alle funzionalità del codice (e.g., numero di utenti/sessioni, response time, frequenza richieste, richieste fallite, eccezioni), indipendentemente dalla piattaforma;
- possibilità di definire eventi e metriche personalizzate e dashboard personalizzate.

4.4.2.5. Auditing Service (Azure Log Analytics, Azure Sentinel, Azure Advisor, Azure Security Center)

Il servizio dovrà assicurare le funzionalità a supporto della governance, compliance e gestione del rischio nell'utilizzo del proprio account sul/i CSP. Il servizio dovrà permettere di monitorare in maniera continuativa le attività eseguite nell'ambito dei vari servizi e fornire uno storico di tutte le azioni che sono state intraprese. Lo storico sarà ad uso di analisi di sicurezza, troubleshooting e

change tracking e dovrà quindi assicurare adeguati contenuti informativi a tal fine.

4.4.2.6. Application log service (Azure Log Service)

Il servizio è volto a garantire la possibilità di raccogliere e centralizzare i log applicativi e di sistema. È inoltre richiesta la possibilità di integrare il collettore con SIEM di terza parte.

4.4.2.7. Security service (Azure Security Center)

Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- rilevamento delle minacce (e.g. DoS, DDoS);
- disponibilità di Intrusion & Prevention Systems;
- disponibilità di antivirus.

4.4.2.8. Backup Service (Azure Backup)

Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- possibilità di definire le policy di backup in maniera personalizzata e anche specificatamente per singolo componenti infrastrutturale;
- possibilità di definire policy di retention dei dati in maniera personalizzata e anche specificatamente per tipologia di dati trattati.

4.4.2.9. DR Automation Service (Azure Site Recovery)

Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- replica dischi, abilitante ripristino su altro sito geografico che ospita servizi cloud secondario;
- funzionalità di supporto per la migrazione dati e servizi da sito on-premise a sito cloud secondario;
- funzionalità di replica geografica orchestrata e distribuzione dei processi di replica.

4.4.2.10. Strumenti per lo sviluppo (Azure Visual Studio, Azure DevOps, Azure SDK, Azure DevTest Lab, Azure Pipelines)

Strumenti di sviluppo per qualsiasi piattaforma o linguaggio, per la distribuzione di applicazioni cloud. Il servizio offre ambienti di sviluppo integrati con funzionalità complete e di debug avanzato.

4.4.3. Servizi di Piattaforma abilitanti al *cloud native*

Il catalogo di servizi di seguito riportato, raccoglie le esigenze per strumenti abilitanti alla revisione in ottica cloud dei servizi migrati dal sito on premise e per la realizzazione di nuove soluzioni in linea con i paradigmi del cloud.

4.4.3.1. Web Application (Azure App Web Service)

Il servizio permette la creazione e la gestione di applicazioni utilizzando framework più diffusi, tra cui .NET, .NET Core, Java, Node.js, Python, PHP e Ruby. Distribuzione delle app in contenitori o come codice, in esecuzione in Linux o Windows.

4.4.3.2. Dispositivi Mobili (Azure App per dispositivi Mobili, API Mgmt, App Service)

Il servizio permette la realizzazione di App multi piattaforma per qualsiasi tipo di dispositivo.

4.4.3.3. Relational Database as a service (Azure MySQL e Azure Postgres)

Il servizio dovrà garantire la continuità delle istanze gestite per database relazionali. Sono richieste funzionalità di crittografia dati sia in transito che a riposo (TDE).

4.4.3.4. Multi-Modal Database Service (Azure Cosmos DB)

Il servizio dovrà garantire la disponibilità di istanze gestite per database multi-modal. Sono richieste funzionalità di crittografia dati sia in transito che a riposo.

4.4.3.5. In memory data archive service (Azure Cache for Redis)

Il servizio dovrà garantire la disponibilità di risorse di archiviazione rapida (in memory) ad uso delle applicazioni (memorizzazione dati su memoria distribuita, per ottenere prestazioni elevate). È prevista la possibilità di accedere alle risorse di archiviazione anche tramite client esterni alle infrastrutture cloud ospitanti. Sono richieste funzionalità di crittografia dati sia in transito che a riposo.

4.4.3.6. Shared Filesystem service (Azure File Service)

Il servizio dovrà garantire la disponibilità di share NFS condivise e la possibilità di gestire quote dello spazio isolate per applicazione/tenant.

4.4.3.7. Large object service (Azure BLOB Storage Service)

Il servizio dovrà garantire la disponibilità di risorse di archiviazione scalabili per dati non strutturali. È di interesse la visibilità dei diversi modelli di servizio/prestazioni disponibili.

4.4.3.8. Datalake Storage Service (Azure Datalake Storage – Azure Datalake Analytics)

Il servizio dovrà garantire la possibilità di usare storage Data Lake altamente scalabile e sicuro per analisi Big Data (dati non strutturati, semi strutturati e strutturati; senza limiti dimensionali).

4.4.3.9. Analisi dei dati (Azure Power BI Embedded)

Dashboard e analisi prodotte in modo semplice e immediato, personalizzate in base esigenze di sviluppo per le automazioni di monitoraggio con funzionalità di analisi intelligente dei dati.

4.4.3.10. WAF Service (Azure Application Gateway)

Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- protezione app web da attacchi esterni;
- possibilità di proteggere più applicativi con un unico WAF;
- aggiornamento automatico per protezione da nuove vulnerabilità;
- supporto SSL offloading;
- supporto end-2-end SSL;
- disponibilità log di diagnostica;
- servizi di filtering (e.g. IP, URL, malicious web traffic).

4.4.3.11. IDM Service (Azure Active Directory)

Il servizio dovrà garantire la continuità delle caratteristiche funzionali minime di seguito elencate:

- gestione identità per accesso sicuro a servizi/applicazioni/risorse su cloud;
- supporto integrazione con i servizi nativi web-app;

4.4.3.12. Key Management Service (Azure Key Vault)

Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- archiviazione credenziali e certificati delle applicazioni;
- funzionalità di generazione chiavi;
- possibilità di importare chiavi generate autonomamente.

4.4.3.13. API Management Service (Azure Api Gateway)

Il servizio dovrà garantire la continuità delle funzioni minime di seguito elencate:

- creazione, pubblicazione, manutenzione, monitoraggio e protezione di API;
- possibilità di accettare e inoltrare chiamate tra layer con differenti livelli di sicurezza (tipicamente da front end verso back end);
- verifica chiavi, token, certificati ed altre credenziali;
- raccolta log chiamate;
- prevenzione attacchi DOS;
- possibilità di attivare canali di comunicazioni protetti tra gateway API e layer contattati (tipicamente verso back end).

4.4.3.14. Container Registry Service (Azure Container Registry)

Il servizio dovrà garantire la disponibilità di un registro di immagini container, completamente gestito, per la conservazione e distribuzione in modo affidabile. È

richiesta l'integrazione con il sistema di Identity management, per la configurazione delle policy di controllo accesso al repository ed alle risorse.

4.4.3.15. Container service (Azure Kubernetes Service)

Il servizio è finalizzato a rendere disponibile all'Amministrazione la possibilità di eseguire su cloud applicazioni realizzate né rispetto di un'architettura a microservizi. Il servizio è finalizzato a rendere disponibili al Committente funzionalità a supporto del deploy di applicazioni web, senza necessità di configurare le risorse computazionali sulle quali l'applicazione sarà eseguita. Le caratteristiche minime richieste sono di seguito elencate:

- supporto dei linguaggi più comuni;
- scalabilità automatica e bilanciamento del carico integrati;
- disponibilità di piani dimensionali con tagli differenti di risorse computazionali.

4.4.3.16. Serverless computings (Azure Service Fabric, Azure Functions)

L'esigenza è quella di rendere disponibile all'Amministrazione, anche per sperimentazione e test, soluzioni di elaborazione serverless end to end che consentano una totale astrazione da attività di configurazione e gestione infrastrutturale. Si assumono come caratteristiche funzionali minime:

- Provisioning infrastruttura totalmente gestito;
- scalabilità e prestazioni by design;
- esecuzione automatica del codice attivabile da diversi tipi di eventi (es. richieste http, azioni su oggetti storage).

4.4.3.17. Messaging queue service (Azure Message Bus)

L'esigenza è quella di garantire la continuità del servizio per la gestione di code di messaggi, nell'ambito di comunicazioni asincrone tra servizi (es. a supporto di architetture applicative basate su microservizi). Caratteristiche funzionali minime richieste sono:

- affidabilità dei meccanismi di trasmissione dei messaggi;
- scalabilità delle risorse;
- supporto protezione crittografica dei messaggi scambiati.

4.4.3.18. Search service (Azure Search Service)

L'esigenza è quella di garantire la continuità del servizio gestito con il quale configurare e gestire soluzioni di ricerca "chiavi in mano" per un sito Web o un'applicazione senza intervenire per la configurazione della infrastruttura ed avere specifiche competenze tematiche. Caratteristiche funzionali minime richieste sono:

- possibilità di definire indici;
- estrapolazione risultati maggiormente rilevanti;

- supporto multi-language;
- supporto suggerimenti di completamento automatico;
- alta scalabilità;
- prestazioni risposte in near real time.

4.4.3.19. Cognitive Service (Azure Cognitive Service)

Il servizio dovrà permettere l'utilizzo di algoritmi intelligenti nelle App e nei siti Web per vedere, ascoltare, parlare, comprendere le esigenze degli utenti tramite metodi di comunicazioni naturali.

4.4.3.20. Altri servizi

La Committente, in ogni caso, a prescindere dall'elenco dei servizi di cui sopra, potrà utilizzare il Massimale per l'acquisizione di tutti i servizi cloud Azure (IaaS, PaaS e SaaS) del catalogo pubblico di Microsoft che siano presenti nel Catalogo dei servizi Cloud per la PA qualificati da AGID (<https://cloud.italia.it/marketplace/supplier/market/index.html>) nel rispetto delle circolari dell'Agenzia per l'Italia Digitale (AGID) nn. 2 e 3 del 9 aprile 2018 (GU n. 92 del 20/4/2018)

5. EROGAZIONE DEI SERVIZI

L'erogazione dei servizi oggetto di acquisizione dovrà essere effettuata, improrogabilmente, a partire dalla data di attivazione comunicata dalla Committente tramite pec inviata al Fornitore dopo la stipula del Contratto. La disponibilità dei nuovi servizi dovrà essere assicurata senza soluzione di continuità e senza alcuna operazione di migrazione. I servizi attualmente configurati all'interno di ciascuna sottoscrizione, dovranno essere mantenuti attivi e trasferiti "amministrativamente" all'interno del nuovo contesto contrattuale.

L'intervento si intende chiuso solo quando le attività di predisposizione e verifica si sono concluse con esito positivo.

5.1. Requisiti di qualità

Il Fornitore deve assicurare la qualità dei servizi erogati, attraverso la presenza al suo interno di specifiche funzioni di verifica, validazione, riesame, assicurazione qualità sui prodotti e sui processi.

Su richiesta della Committente, il Fornitore dovrà predisporre delle rappresentazioni dell'andamento della fornitura basandosi sui dati riportati nei rapporti sugli indicatori di qualità della fornitura, anche al fine di effettuare analisi a vari livelli di dettaglio delle informazioni.

5.2. Responsabile della fornitura

Entro 5 (cinque) giorni lavorativi dalla stipula del contratto, l'Impresa dovrà comunicare all'Amministrazione il nominativo del proprio rappresentante designato quale Responsabile della fornitura (o Responsabile della Società per le attività contrattuali). In particolare, tale responsabile sarà, per gli aspetti amministrativi e contrattuali, l'interlocutore unico del Committente.

Sarà cura del Responsabile della fornitura verificare il rispetto di tutti gli adempimenti contrattuali.

Tale referente non dovrà comportare alcun onere aggiuntivo per la Committente.

Il Responsabile della fornitura dovrà essere reperibile telefonicamente e partecipare alle riunioni su richiesta della Committente con un preavviso massimo di 3 giorni lavorativi.

Il Responsabile della fornitura non farà parte di alcuno dei gruppi di lavoro relativi ai servizi oggetto della fornitura.

Il Responsabile della fornitura dovrà in particolare:

- monitorare i livelli di servizio sulle attività oggetto della fornitura ed intraprendere eventuali azioni correttive a fronte del mancato rispetto delle soglie previste;
- farsi carico della soluzione dei problemi tecnici e/o di eventuale non disponibilità dei servizi Cloud che dovessero verificarsi nel corso della durata contrattuale.

6. ESECUZIONE DELLA FORNITURA

Al Fornitore è richiesto in tutte le attività della fornitura il rispetto dei processi, degli standard e delle linee guida adottate dalla Committente; il Fornitore deve farsi carico di conoscere e diffondere al proprio interno tali conoscenze, di applicarle proattivamente, e di recepire tempestivamente eventuali variazioni.

La tipologia delle attività da svolgere e la delicatezza della materia trattata richiedono che tutte le attività dell'Impresa siano improntate a un'assoluta attenzione alla riservatezza. È inoltre fatto divieto all'Impresa di utilizzare il presente affidamento quale riferimento per altri incarichi, salvo esplicita autorizzazione da parte del Committente.

Tutte le attività dovranno essere svolte in collaborazione con i referenti del Committente, secondo modalità che saranno opportunamente concordate in fase di avvio.

L'Amministrazione si riserva di modificare le modalità di esecuzione descritte e di introdurre nuove modalità, anche in corso d'opera, dandone congruo preavviso

all'Impresa. In aggiunta, tali modalità di esecuzione potranno essere congiuntamente riviste, su proposta dell'Impresa, e potranno essere concordate opportune semplificazioni o variazioni in funzione delle specificità dei singoli interventi.

Il Committente si riserva di avvalersi di terzi per il supporto allo svolgimento di attività di propria competenza, ferma restando la responsabilità globale del Committente nello svolgimento di tali attività.

6.1. Modalità di esecuzione della fornitura

La fornitura dei servizi cloud Azure erogati dal Cloud pubblico Microsoft Azure dovrà essere espletata attraverso piattaforma elettronica messa a disposizione a cura del Fornitore.

6.1.1. Modalità di erogazione continuativa

Il servizio Cloud da erogare è in modalità continuativa a decorrere dalla data di attivazione dei servizi.

L'erogazione è senza soluzione di continuità fino alla data di fine delle attività, salva ed impregiudicata la facoltà della Committente di sospendere, ridurre e/o interrompere i servizi.

Dal momento in cui una richiesta per malfunzionamento è registrata nel sistema della Committente, o nel sistema del Fornitore in assenza dello stesso, decorrono i tempi relativi ai livelli di servizio definiti nel presente capitolato tecnico.

Il Fornitore ha la responsabilità della esecuzione dell'attività di risoluzione del malfunzionamento ed è tenuto ad aggiornare le informazioni di propria competenza sul sistema fino alla soluzione del malfunzionamento stesso motivato con la opportuna e dettagliata diagnosi.

6.1.2. Livelli di servizio

Si applicano i livelli di servizio previsti per i singoli servizi cloud Microsoft presenti nel catalogo dei servizi cloud di Microsoft così come esplicitati al seguente link <https://azure.microsoft.com/it-it/support/legal/sla/summary/>

Qualora nell'erogazione dei servizi Cloud si verificassero dei problemi tecnici o una non disponibilità degli stessi, la Committente contatterà il Fornitore, per la soluzione di tali problematiche, contattando il Responsabile della fornitura a un numero telefonico o a un indirizzo di posta elettronica o un numero di fax all'uopo preposti.

6.2. Pianificazione e Consuntivazione

I servizi oggetto della fornitura potranno essere consuntivati **trimestralmente**. Per ciascun trimestre, dunque, il Fornitore potrà fatturare i servizi resi al Committente, in base all'effettiva erogazione e consumo, previo nulla osta alla fatturazione comunicato dal Committente.

6.3. Azioni contrattuali

Ogni inadempimento contrattuale darà origine ad un'azione commisurata alla criticità della violazione.

Pertanto, il mancato rispetto dei requisiti minimi richiesti determina azioni contrattuali conseguenti che possono consistere in una o più delle seguenti azioni:

- coinvolgimento di un livello più elevato di interlocutori, sia del Fornitore che della Committente, allo scopo di prendere le decisioni necessarie al ripristino delle situazioni fuori soglia o fuori controllo (attivazione di una procedura di escalation);
- ripetizione da parte del Fornitore dell'erogazione di una prestazione, rifacimento di una attività, riconsegna di un prodotto;
- riconoscimento da parte del Fornitore di crediti aggiuntivi da utilizzare per fruire di servizi cloud
- azione di intervento sui processi produttivi del Fornitore per evitare il ripetersi di sistematiche non conformità (esecuzione di una azione correttiva);
- azioni aggiuntive (richiesta danni, risoluzione anticipata del contratto, ecc.) laddove previsto contrattualmente.