classificazione documento: consip public

AS SDAPA per l’acquisizione di Servizi cloud Microsoft AZURE e servizi professionali connessi per INAIL – ID 2645

CAPITOLATO TECNICO

**INDICE**

[1. GLOSSARIO, ACRONIMI E TERMINOLOGIA 3](#_Toc136875949)

[2. INTRODUZIONE 4](#_Toc136875950)

[3. PREMESSA 4](#_Toc136875951)

[4. Contesto 5](#_Toc136875952)

[5. OGGETTO E DURATA DEI SERVIZI 13](#_Toc136875953)

[**6.** **erogazione DEI servizi** 14](#_Toc136875954)

[6.1. Consegna in gestione 14](#_Toc136875955)

[6.2. Requisiti di qualità 15](#_Toc136875956)

[6.3. Responsabile della Fornitura 15](#_Toc136875957)

[**7.** **Esecuzione della fornitura** 15](#_Toc136875958)

[7.1. Modalità di esecuzione della fornitura 16](#_Toc136875959)

[7.1.1. Modalità di erogazione continuativa 16](#_Toc136875960)

[7.1.2. Livelli di servizio 16](#_Toc136875961)

[7.1.3. La qualificazione dei servizi cloud e delle infrastrutture dei servizi cloud 17](#_Toc136875962)

[7.2. Azioni contrattuali 17](#_Toc136875963)

[7.3. Exit strategy e Grace period 18](#_Toc136875964)

[7.4. Servizi Professionali 18](#_Toc136875965)

[7.5. Verifica di conformità 21](#_Toc136875966)

# GLOSSARIO, ACRONIMI E TERMINOLOGIA

**GLOSSARIO**

|  |  |
| --- | --- |
| **Amministrazione o Committente** | L’Istituto Nazionale per l’Assicurazione contro gli Infortuni sul Lavoro (INAIL), che usufruisce dei servizi e dei prodotti descritti nel presente Capitolato tecnico. |
| **Consip** | La società che, in qualità di stazione appaltante della presente fornitura, affida la fornitura oggetto del presente Capitolato. |
| **Impresa o Fornitore** | La società affidataria della presente procedura. |
| **Contratto** | Il contratto che verrà stipulato tra INAIL e l’Impresa aggiudicataria, recante le clausole che disciplineranno i rapporti giuridici tra le parti (INAIL e Impresa) nell’esecuzione del Servizio. |
| **Fornitura** | Le attività descritte nel presente documento tecnico. |
| **Servizi** | Il complesso dei servizi e delle attività oggetto del presente Capitolato tecnico. |
| **Responsabile della Fornitura** | La persona individuata dall'Impresa come interlocutore dell’Amministrazione e responsabile di tutte le attività contrattuali. |
| **Piattaforma** | La Piattaforma software per l’erogazione dei Servizi. |
| **Giorni e Ore** | Nella documentazione per giorno e ora si intendono rispettivamente giorno lavorativo e ora lavorativa; l’orario previsto per l’erogazione dei servizi specialistici è dalle 8,00 alle 18,00 dal lunedì al venerdì. |
| **RUP e DEC** | Rispettivamente il Responsabile Unico del Procedimento e il Direttore dell’Esecuzione del Contratto che svolgono ruoli e funzioni definiti all’art.31 del D.Lgs. n. 50/2016 e s.m.i. |
|  |  |

# 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 Microsoft AZURE e servizi professionali connessi per INAIL.

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.

# PREMESSA

Nel perimetro della Convenzione stipulata tra INAIL e Consip S.p.A. in data 17/03/2022 e nell’ambito del Piano Annuale Attività per il 2023 approvato, l’Istituto ha affidato a Consip S.p.A. l’iniziativa in oggetto, relativa **all’acquisizione di Servizi cloud pubblico Microsoft AZURE e servizi professionali connessi per INAIL – ID 2645.**

Questo documento ha lo scopo di definire le caratteristiche e i requisiti relativi alla fornitura dei suddetti servizi per INAIL, in quantità, qualità e livelli di servizio adeguati.

# Contesto

L’INAIL dispone di sottoscrizioni di cloud pubblico Microsoft Azure nell’Enterprise Agreement Government Partner (EAGP) per l’erogazione di servizi PaaS e IaaS per utenti interni ed esterni. Tale ambiente è integrato tramite un percorso ibrido con le infrastrutture e applicazioni “on premise” dell’Istituto.

La sottoscrizione di riferimento è di tipologia “Server and Cloud Enrollment (SCE)” ovvero un contratto di tipologia Microsoft Enterprise Agreement, di durata pari a 36 mesi, stipulato in data 01 dicembre 2020 per la fornitura delle licenze Azure. Il predetto contratto avrà scadenza il prossimo 30 novembre 2023.

In linea con le previsioni ACN, l’INAIL ha considerato 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. Inoltre, sempre in virtù del processo di digitalizzazione, si è tenuto conto che le iniziative progettuali utilizzino esclusivamente servizi PaaS e SaaS evitando, ove possibile, altre soluzioni legate al paradigma IaaS, attraverso l’acquisizione di servizi Cloud da utilizzare per la realizzazione di sistemi moderni e per la dismissione delle componenti IT tradizionali.

In questo contesto vengono di seguito descritte le soluzioni che in Istituto si avvalgono dei servizi Azure.  
Si evincerà che nella definizione dei servizi Cloud da acquisire, è necessario mantenere un legame con un specifico service provider, nella specie Microsoft Azure, per le forti dipendenze tecnologiche venutesi a creare tra lo sviluppo applicativo custom e le interfacce di alcuni servizi PaaS (quali ad esempio: Azure Search, Azure API Gateway, Azure App Services, Azure Web Job, Azure Cache, etc.).

Inoltre, tali applicazioni native cloud, hanno interdipendenze con le applicazioni custom legacy. Queste applicazioni legacy sono state personalizzate per essere raggiunte in modalità ibrida tramite la predisposizione di servizi specifici di identità, sicurezza e gestione.

I principali servizi Azure chiamati dalle applicazioni INAIL sono:

| **Servizio** | **Scopo/descrizione** | **Tipologia Servizio** |
| --- | --- | --- |
| **Azure Active directory** | Sistema di gestione delle identità utilizzato per proteggere ed autorizzare l’accesso nell’applicativo front-end. Le identità/account presenti in questo servizio sono sincronizzati con il sistema di Identity Management On-Premises utilizzato dall’istituto. | SaaS |
| **Azure App Service** | Web Server per la gestione e pubblicazione dell’applicativo Front-End.  Il componente è protetto da Azure Active Directory e dal Web Application Firewall, sfrutta il protocollo Oauth per riconoscere ed autorizzare l’utente. | PaaS |
| **Azure App Configuration** | È un servizio per la gestione centralizzata delle impostazioni delle applicazioni e dei flag di funzionalità. I programmi moderni hanno in genere molti componenti distribuiti. Disseminare le impostazioni di configurazione tra questi componenti può generare errori difficili da risolvere durante la distribuzione di un’applicazione. Azure App Configuration consente di archiviare tutte le impostazioni dell’applicazione e di proteggerne gli accessi in un’unica posizione. | PaaS |
| **Azure Key Vault** | Azure Key Vault è un servizio cloud per archiviare i segreti e accedervi in modo sicuro. Un segreto è qualsiasi elemento per cui si vuole controllare rigorosamente l’accesso, ad esempio chiavi API, password, certificati o chiavi crittografiche. | PaaS |
| **Azure Web Job** | Servizio di batch asincroni, si interfaccia con i componenti di storage ed esegue le operazioni “Long Operation” in un processo parallelo al Front-End così da evitare impatti nella UX.  Questo servizio è una funzionalità OOTB del servizio Azure App Service. | PaaS |
| **Virtual Machine** | Servizio di provisioning di virtual machine | IaaS |
| **Azure Kubernetes Services** | Servizio di runtime per ambienti containerizzati basati su Kubernetes | PaaS |
| **Azure Storage Account** | Servizio di storage, specializzato nella gestione di:   * Tabelle non relazionali * Code * File Blob   Il componente è utilizzato per memorizzare dati puramente applicativi:   * Log Applicativo * Informazioni sulle prestazioni | PaaS |
| **Azure Application Gateway** | Il componente offre servizi di routing e bilanciamento per gestire gli aspetti di scalabilità ed alta affidabilità dell’applicativo front-end. | PaaS |
| **Azure Web Application Firewall** | Web application firewall (WAF) è una funzionalità dell’Azure Application Gateway ed offre una protezione centralizzata delle applicazioni Web da exploit e vulnerabilità comuni.  Il firewall si basa sulle regole di OWASP Core Rule Set 3.0 o 2.2.9 | PaaS |
| **Azure SQL** | Database Relazionale virtualizzato, il componente memorizza i dati di business. Il componente è protetto da firewall. | PaaS |
| **Power BI** | Servizio di reportistica SaaS, il componente viene utilizzato per visualizzare reports e dashboard all’interno dell’applicativo front-end. Gli accessi sono protetti tramite Azure Active Directory sfruttando il protocollo Oauth token. | PaaS |
| **Active directory federation services** | Sistema di federazione già in utilizzo da parte dell’Istituto. Permette di effettuare il trust tra il sistema di gestione identità on-premises ed Azure Active Directory, permettendo la gestione degli account in locale e l’accesso alle risorse cloud. | On-Premises |
| **Azure data factory v2** | È un servizio di integrazione di dati basato sul cloud che consente di creare flussi di lavoro basati sui dati nel cloud per orchestrare e automatizzare lo spostamento e la trasformazione dei dati stessi. Il sistema permette di recuperare i dati da sistemi on-premises e renderli disponibili per successive elaborazioni alle risorse azure. | PaaS |
| **Azure data lake storage** | Servizio per lo storage dei dati estratti dall’infrastruttura on-premise. | PaaS |
| **Azure data lake analytics** | Servizio di analisi e trasformazione dei dati. Tramite l’utilizzo dei script u-sql(sql/c#) è possibile effettuare trasformazioni e scrittura da e verso servizi Azure. | PaaS |
| **ADF integration runtime / gateway server** | Servizio Windows On-premise per configurare l’integrazione tra origine dati on-premise con il servizio Azure Data Factory. | On-Premises |
| **Event Hub** | È un servizio gestito (PaaS) per la gestione in streaming di eventi in grado di processare milioni di eventi al secondo. Rende disponibili degli adattatori per il processing dei dati con servizi di streaming (p.e. Spark) e per la persistenza in formato “avro” su un Data Lake con interfaccia HDFS. Il servizio garantisce la retention degli eventi in caso di indisponibilità temporanea dei consumers o in caso di picchi di carico non gestibili dai consumer. L’ingestione degli eventi è resa possibile anche mediante client che usano interfaccia Kafka | PaaS |
| **Azure CosmosDB** | È un servizio di database non relazionale no SQL per la persistenza di dati non strutturati. Il DB supporta nativamente la replica su due o più region con distanza superiore ai 1.000 Km in modalità active-active. È possibile scegliere tra vari livelli di consistenza che vanno dalla Strong consistency (i dati sono sempre allineati tra tutte le repliche) e la eventual consistency (i dati per un certo lasso di tempo posso essere disallineati tra le varie repliche). Il DB deve esporre interfaccia MongoDB, Gremlin, Cassandra, Key-Value, e SQL.  È possibile variare a caldo la potenza del DB per garantire prestazioni ottimali in caso di picchi e allo stesso tempo consumi ridotti in caso di scarso utilizzo. | PaaS |
| **Data Factory** | È un servizio per l’orchestrazione di processi per il trasferimento e la trasformazione di BigData in formato relazionale, non relazionale e su altri tipi di storage (Data Lake, Blog, File Share, etc.). I processi che il servizio supporta sono di tipo extract-transform-load (ETL), extract-load-transform (ELT) e di data integration. I dati da gestire possono essere localizzati on premise, sul cloud e i flussi saranno anche ibridi.  L’orchestrazione dei flussi può essere eseguita in modalità schedulata (batch) mediante regole periodiche e on demand (attivate da operatori umani o mediante API). I flussi per le trasformazioni dei dati si integrano in modo nativo (senza richiedere lo sviluppo di componenti custom) con servizi di elaborazione come ad esempio Hadoop, Databricks, e SQL Database. Analogamente al processing, anche i dati trasformati sono pubblicati in data stores (ad esempio SQL Data Warehouse) per fare analisi di business intelligence (BI), sempre senza richiedere lo sviluppo di codice custom.  Le funzionalità che il servizio supporta sono:  Connect and collect: acquisizione di dati da varie fonti (DB, file repository, ecc); Transform and enrich: elaborazione dei dati CI/CD and publish, rilascio agile dei cambi evolutivi e bug fix; Monitor: gestione operativa dei flussi, analisi dei tempi di esecuzione, gestione delle anomalie. | PaaS |
| **Azure VmWare Solution** | Azure VMware Solution offre un private cloud basato su un cluster VMware vSphere su un'infrastruttura bare metal dedicata di Azure.  Tale servizio consente di eseguire la migrazione dei carichi di lavoro dagli ambienti locali, la distribuzione di nuove macchine virtuali (VM) e l’estensione in cloud pubblico della farm VmWare on premise dell’Istituto.  Azure VMware Solution è un servizio certificato da VmWare ed erogato e gestito da Microsoft che ne gestisce l'infrastruttura e il software. | Paas |
| **Azure Media Services** | Piattaforma cloud based che consente di creare soluzioni per streaming video di alta qualità, migliorando accessibilità e distribuzione e analizzandone il contenuto sui browser e sui dispositivi mobili moderni più diffusi. | Paas |
| **Azure Cognitive Services** | Insieme di servizi e strumenti per Artificial Intelligence e machine learning evoluti finalizzati ad automazione processi e ricerca documentale | PaaS |
| **Servizi di piattaforma trasversali a tutti i servizi** | | |
| **LogicApp** | È un servizio managed (PaaS) per orchestrazione di flussi di lavoro completamente ospitato dal cloud ed in modalità serverless. Tale servizio dispone di connettori nativi per servizi di messaging più comuni (p.e. Mail, Social messaging, MSFT Teams, etc…), per l’integrazione con i principali DB relazionali e non (p.e. SQL Server, OracleDB, etc…), per il file transfer, data conversion, etc.  Il servizio sebbene debba sia ospitato nel cloud consente l’interazione con servizi on premise mediante un gateway che non richiede l’apertura di porte in ingresso sui dispositivi di protezione dell’Istituto. | PaaS |
| **Azure AD B2C** | È un servizio per l’autenticazione e per la gestione di utenze applicative di tipo consumer (utenze non associate a personale dell’Istituto). Il servizio consente l’autenticazione in modalità SSO con le principali utenze social, utenze aziendali, o utenze locali. Il sistema può gestire milioni di utenze con decine di milioni di autenticazioni al giorno.  Il servizio garantisce la protezione da minacce come ad esempio attacchi di tipo *DDOS, brute force o password spray*. La pagina di login è customizzabile in modo da poter mostrare il logo dell’istituto quando gli utenti si autenticano. Il sistema supporta protocolli standard di autenticazione tra cui: OpenID Connect, OAuth 2.0, and SAML.  Per gli utenti locali è possibile gestire in modo autonomo operazioni di reset della password e modifica delle informazioni del profilo. | SaaS |
| **API Management** | È un servizio per l’esposizione in modo sicuro, consistente e tracciato di funzionalità di backend mediante API Rest. Il servizio che fa da Gateway è gestito dal fornitore cloud ed è erogato in modalità PaaS. Gli sviluppatori che intendono usare le API si sottoscrivono ed ottengono una API key da usare al momento dell’invocazione. È possibile tracciare, fare *l’auditing* e fare *throttling* (in base a delle quote) delle invocazioni. Il servizio dispone di un portale amministrativo per la definizione e la gestione operativa delle API (monitor dei tempi di risposta, success/failure rate, statistiche d’uso, etc.). È disponibile anche un portale per gli sviluppatori che darà accesso alle definizioni delle API, alla documentazione e alle proprie statistiche d’uso. | PaaS |
| **Azure Function** | Soluzione serverless che consente di scrivere meno codice, gestire un'infrastruttura meno complessa e risparmiare sui costi. Non è più necessario preoccuparsi della distribuzione e della gestione dei server, in quanto l'infrastruttura cloud fornisce tutte le risorse aggiornate necessarie per mantenere le applicazioni in esecuzione. Ci si può concentrare sulle parti di codice che interessano di più e il resto viene gestito da Funzioni di Azure.  Spesso vengono sviluppati sistemi per reagire a una serie di eventi critici. Indipendentemente dal fatto che si stia creando un'API Web, rispondendo alle modifiche del database, elaborando i flussi di dati IoT o anche gestendo le code dei messaggi, ogni applicazione necessita di un modo per eseguire codice quando si verificano questi eventi.  Per rispondere a questa esigenza, Function di Azure prevede risorse di calcolo su richiesta in due modi significativi.  Prima di tutto, Function di Azure consente di implementare logica di sistema personalizzata in blocchi di codice immediatamente disponibili. Questi blocchi di codice si chiamano "funzioni". Le diverse funzioni possono essere eseguite in qualsiasi momento sia necessario rispondere a eventi critici.  In secondo luogo, quando le richieste aumentano, Funzioni di Azure soddisfa la domanda con il numero necessario di risorse e istanze di funzioni, ma solo fintanto che servono. Quando le richieste diminuiscono, le eventuali risorse e istanze dell'applicazione aggiuntive vengono rimosse automaticamente. | PaaS |
| **Monitoring Platform** | È uno strumento di monitoring integrato nativamente con la piattaforma che eroga i servizi. Il servizio di monitoring è completamente gestito ed erogato in modalità SaaS (non richiede nessuna VM per l’hosting di componenti infrastrutturali). Non è richiesta alcuna strumentazione dei servizi monitorati (siano essi VM o servizi PaaS). Include le seguenti funzionalità:   * Rilevazione e diagnostica di problemi tra applicazioni * Correlazione dei problemi di infrastruttura e quelli applicativi * Acquisizione dei log di monitoraggio in una piattaforma di Log Analytics per la risoluzione dei problemi e la diagnostica approfondita. * Possibilità di generare notifiche e di compiere azioni automatizzate. * Creazione di dashboard e workspace in ambiente cloud | PaaS |
| **Azure Defender for Cloud** | È una piattaforma CWPP (Cloud Security Posture Management) e Cloud Workload Protection Platform (CWPP) per tutte le risorse Azure, on premise e multi-cloud (Amazon AWS e Google GCP). Defender per il cloud soddisfa tre esigenze fondamentali man mano che si gestisce la sicurezza delle risorse e dei carichi di lavoro nel cloud e in locale: il punteggio di sicurezza di Defender for Cloud, le raccomandazioni di Defender for Cloud e gli avvisi di Defender for Cloud. | Paas |
| **Azure Sentinel** | È la soluzione di Security Information and Event Management (SIEM) e Security Orchestration, Automation and Response (SOAR) per l’aggregazione e l’analisi di eventi di sicurezza provenienti dai sistemi IT sia on premises che nel cloud, la rilevazione di situazioni anomale associate a questi eventi, l’individuazione di correlazioni tra le entità coinvolte negli incidenti e le informazioni di Threat Intelligence provenienti dalle fonti di interesse. | PaaS |
| **Azure Front Door** | È la rete CDN (Cloud Content Delivery Network) moderna di Microsoft che offre accesso rapido, affidabile e sicuro tra gli utenti e il contenuto Web statico e dinamico delle applicazioni in tutto il mondo. Frontdoor di Azure offre il contenuto usando la rete perimetrale globale di Microsoft con centinaia di IP globali e locali distribuiti in tutto il mondo vicino agli utenti finali aziendali e consumer. | PaaS |
| **Azure Firewall** | È un servizio di sicurezza firewall di rete intelligente e nativo del cloud, che una protezione ottimale dalle minacce per i carichi di lavoro cloud eseguiti in Azure. È un firewall con stato completo distribuito come servizio, con disponibilità elevata integrata e scalabilità cloud illimitata. Consente l'ispezione sia del traffico orizzontale destra-sinistra, sia del traffico verticale alto-basso. | PaaS |
| **Azure DDoS Protection** | Protezione DDoS di Azure, combinata con le procedure consigliate per la progettazione delle applicazioni, offre funzionalità di mitigazione DDoS avanzate per difendersi da attacchi DDoS. La protezione è semplice da abilitare in qualsiasi rete virtuale nuova o esistente e non richiede alcuna modifica di applicazioni o risorse. | PaaS |
| **Azure Bastion** | Servizio distribuito che consente di connettersi a una macchina virtuale usando il browser e il portale di Azure oppure tramite il client SSH o RDP nativo già installato nel computer locale. Offre connettività RDP/SSH sicura e ininterrotta con le macchine virtuali dal portale di Azure tramite TLS. Quando ci si connette tramite Azure Bastion, per le macchine virtuali non è necessario un indirizzo IP pubblico, un agente o un software client speciale. | PaaS |
| **Servizi trasversali** | Servizi funzionali e trasversali a tutte le applicazioni quali: expressroute, iaas generico, sicurezza, monitoring | Iaas/Paas |

Nel paragrafo successivo verranno descritte le principali applicazioni realizzate su Cloud Azure e indicati i servizi Azure da esse utilizzati.

# OGGETTO E DURATA DEI SERVIZI

L’oggetto dell’esigenza espressa da INAIL, riguarda l’acquisizione di:

1. servizi del Cloud Pubblico Microsoft Azure “**Server and Cloud Enrollment (SCE)” per Government Partner**, tipologia di Unit: **SKU (Stock Keeping Unit) – codice prodotto: 6QK-00001**,
2. servizi professionali,

come dettagliato di seguito.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Fornitura** | | | | |
| **Nome** | **Descrizione** | **SKU**  **(tipologia di Unit)** | **Quantità di Unit** | **Numero mesi - G/P** |
| Azure Monetary Commitment | AzureMonetaryCommit ShrdSvr ALNG SubsVL MVL Commit | **6QK-00001** | 4.593 | 36 |
| Servizi professionali | Architetto specialista di prodotto - Partner Microsoft Certified con le seguenti certificazioni:   * AZ 304 – Microsoft Azure Architect Design * AZ 400 – Microsoft Azure DevOps | - | - | 720 |
| Servizi professionali | Specialista Senior di prodotto - Partner Microsoft Certified con la seguente certificazione:   * AZ 104 – Microsoft Azure Administrator | - | - | 1.080 |

I suddetti prodotti e servizi (fornitura) avranno una **durata pari a 36** (trentasei) **mesi** decorrenti dalla “Data di accettazione del servizio”, di cui al successivo paragrafo 7.6.

L’avvio dell’esecuzione delle attività avverrà, nel rispetto di quanto stabilito all’art. 32, comma 13, D. Lgs. 50/2016, contestualmente alla stipula.

La Committente si riserva di redigere apposito verbale di avvio dell’esecuzione del contratto in contraddittorio con il Fornitore.

Si precisa che, in merito alla suddetta fornitura, l’Istituto intende avvalersi dell’opzione di proroga definita all’art. 106, comma 11, del D.Lgs. n. 50/2016 e s.m.i.

La descrizione delle clausole che disciplinano i Servizi Microsoft sono dettagliate nell’Appendice A e B al presente Capitolato Tecnico. Resta inteso che in caso di discordanza tra quanto indicato nei sopracitati documenti vale la regola di prevalenza prevista nel contratto – condizioni speciali.

1. **erogazione DEI servizi**

L’erogazione dei servizi IaaS, PaaS e SaaS oggetto di acquisizione dovrà essere effettuata, improrogabilmente, **entro 5 (cinque) giorni** solari a decorrere dalla data di stipula del contratto oppure entro il diverso termine stabilito tra le parti.

Contestualmente all’erogazione dei servizi IaaS, PaaS e SaaS, l’Impresa dovrà, altresì, consegnare un “Piano operativo/di collaudo”, contenente la proposta relativa alle operazioni e funzionalità che saranno oggetto di verifica di conformità dei prodotti oggetto della fornitura. Tale Piano Operativo dovrà essere approvato dalla Committente entro 5 (cinque) giorni solari dall’avvenuta consegna dello stesso.

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 manutenuti attivi e trasferiti “amministrativamente” all’interno del nuovo contesto contrattuale.

* 1. **Consegna in gestione**

Sono comprese nella fornitura tutte le attività necessarie affinché i servizi IaaS, PaaS e SaaS erogati possano essere gestiti dai team dedicati della Committente; le attività devono essere formalizzate nel suddetto *Piano Operativo/di collaudo*; in particolare dovranno essere previste almeno le seguenti attività:

* illustrazione della documentazione prodotta nell’ambito del rilascio dei servizi;
* passaggio di conoscenza funzionale e tecnica.

Il Fornitore è tenuto, preliminarmente al passaggio dei servizi in gestione, a fornire il proprio supporto a INAIL nell’esecuzione dei test di qualità e della certificazione dei servizi stessi.

* 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.

* 1. **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 di INAIL.

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 a un numero telefonico o a un indirizzo di posta elettronica o un numero di fax all’uopo preposti 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:

* predisporre ed aggiornare il piano operativo;
* 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.

1. **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 recepirne 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.

Il corrispettivo complessivo offerto dall’Impresa si intende comprensivo di tutte le attività richieste e necessarie per l’esecuzione della fornitura. Tale corrispettivo non potrà subire aumenti neanche al variare della pianificazione effettiva rispetto a quanto inizialmente previsto.

Tutte le attività dovranno essere svolte in collaborazione con i referenti dell’Amministrazione, 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.

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

* 1. **Modalità di esecuzione della fornitura**

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

Le attività correlate alla erogazione dei servizi cloud avranno luogo presso le sedi INAIL individuate dall’Istituto.

* + 1. **Modalità di erogazione continuativa**

Il servizio Cloud da erogare è in modalità continuativa, senza soluzione di continuità fino alla scadenza del contratto, salva ed impregiudicata la facoltà della Committente di sospendere, ridurre e/o interrompere il servizio.

* + 1. **Livelli di servizio**

Le modalità di erogazione del servizio (Livelli di servizio) sono regolate in dettaglio nell’Allegato 11 - Classificazione CSP (Documento AGID). In particolare, per quanto riguarda la “disponibilità”, questa dovrà essere garantita al 99,9%.

Il Fornitore si impegna a comunicare a INAIL ogni qualsivoglia variazione del predetto Allegato e produrre quello aggiornato entro il termine di 5 giorni lavorativi dalla relativa modifica, pena l’applicazione della penale prevista nel Contratto all’art. 14 Comma 10. Resta inteso che eventuali variazioni non potranno determinare riduzioni/peggioramenti dei livelli di servizio previsti per la presente iniziativa.

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.

* + 1. **La qualificazione dei servizi cloud e delle infrastrutture dei servizi cloud**

Il livello di classificazione del DATO TRATTATO dai servizi oggetto del presente appalto è ad oggi qualificato come Ordinario ai sensi dell’articolo 3 del regolamento «Cloud della PA».

Di conseguenza, in conformità a quanto previsto dal decreto direttoriale n. 29 del 2 gennaio 2023 e della precedente determina n. 307 del 18 gennaio 2022 dell’ACN (Agenzia per la Cybersicurezza Nazionale) in tema di qualificazione di servizi Cloud per le PA, nell’ambito del regime transitorio in essere, il livello di qualificazione richiesto per i servizi oggetto della presente acquisizione è Qualificazione cloud livello 1 (QC1).

**In mancanza di tale qualificazione non sarà possibile procedere alla stipula del Contratto fino all’acquisizione della stessa. La mancata stipula del contratto per fatto dell’affidatario dà luogo alla escussione della cauzione provvisoria**.

Il servizio e le sue modalità di erogazione dovranno pertanto rispettare tutti i requisiti per la qualificazione, organizzativi e specifici, previsti dalle suddette circolari e, laddove ritenuto utile o necessario, ribaditi all’interno delle prescrizioni del presente Capitolato Tecnico.

Resta inteso che troveranno applicazione, ove possibile, le disposizioni eventualmente introdotte a seguito dell’entrata in vigore del regime ordinario di qualificazione dei servizi cloud, la cui adozione da parte di ACN è prevista entro il 31 luglio 2023.

La qualificazione dovrà essere mantenuta e rinnovata per tutta la durata del Contratto; in caso contrario Inail avrà facoltà di esercitare la clausola risolutiva secondo le indicazioni fornite nel presente Capitolato e nel Contratto.

Dovrà, in ogni caso, essere garantita la continuità della prestazione, dei livelli di sicurezza e di funzionalità.

* 1. **Azioni contrattuali**

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

Pertanto, il mancato rispetto dei requisiti minimi richiesti e/o comunque delle obbligazioni previste nel presente Capitolato, sue appendici e nel Contratto 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 (chiusura di una non conformità);
* 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.
  1. **Exit strategy e Grace period**

Il Fornitore si obbliga, senza alcun onere aggiuntivo per la Committente, a fornire supporto alla Committente nell’attività di Exit strategy che avverrà entro 30 (trenta) giorni solari dalla scadenza naturale del contratto, ovvero, se prima della scadenza naturale, l’Exit strategy dovrà essere comunicata al Fornitore con 30 (trenta) giorni di preavviso (cd. Grace period), e consisterà in un supporto all’individuazione dei dati oggetto di migrazione.

Il Fornitore, inoltre si obbliga a fornire tutte le idonee garanzie a dimostrazione della eliminazione dei dati sul cloud al termine della fase di Exit strategy, nonché la disponibilità a far eseguire verifiche in tal proposito da parte della Committente o di soggetti terzi da questa designati.

Preliminarmente alla fase di Exit strategy, il Fornitore si obbliga a esportare i dati in un formato che andrà stabilito in accordo con la Committente e, comunque, idoneo a consentire la migrazione dei dati su infrastrutture individuate da INAIL.

Al momento della scadenza del contratto, il Fornitore non avrà più titolo per emettere fatture, in quanto deve intendersi attivato il Grace period, per un periodo massimo di 30 giorni, durante il quale la Committente si riserva di procedere al rinnovo del contratto, anche con altro service provider di cloud ovvero alla migrazione dei servizi (Exit strategy), che dovrà avvenire entro il Grace period.

* 1. **Servizi Professionali**

L’obiettivo principale dell’acquisizione di consulenza specialistica sul Cloud Microsoft Azure è quello di massimizzare i benefici per INAIL derivanti dall’utilizzo dei relativi servizi implementati presso l’Istituto.

In particolare, la consulenza specialistica sarà utilizzata per supportare INAIL nella pianificazione (plan), progettazione (design) e realizzazione (Implement) di funzionalità Azure secondo le raccomandazioni di Microsoft, nonché per supportare gli utenti nell’utilizzo dei servizi utilizzati nell’ambito della presente fornitura, per tutto il periodo contrattuale.

**Dimensionamento**

Durante il periodo di durata contrattuale saranno fornite, in modalità “a consumo”, su richiesta dell’INAIL, un **massimo di n. 1.800 giornate** di supporto specialistico per tutte le attività di verifica, aggiornamento, tuning e personalizzazione che si renderanno necessarie durante il periodo di esercizio delle componenti implementate.

|  |  |  |
| --- | --- | --- |
| **Descrizione** | **Durata** | **Quantità** |
| Architetto specialista di prodotto - Partner Microsoft Certified con le seguenti certificazioni:   * AZ 304 – Microsoft Azure Architect Design * AZ 400 – Microsoft Azure DevOps | 36 mesi | 720 |
| Specialista Senior di prodotto - Partner Microsoft Certified con la seguente certificazione:   * AZ 104 – Microsoft Azure Administrator | 36 mesi | 1080 |

L’utilizzo della consulenza specialistica dovrà garantire all’Istituto i seguenti benefici puntuali:

* garanzia delle conoscenze specifiche di tutte le componenti tecnologiche di Microsoft Azure;
* gestione di tali componenti in modo “olistico” e non in modo “puntuale” così da avere un ambiente integrato e sfruttare al meglio gli investimenti e le tecnologie;
* formazione continua e il trasferimento di know-how alle risorse interne dell’Istituto.

Il modello di ingaggio per le figure professionali del team di consulenza specialistica dovrà essere il seguente:

* Definizione obiettivi iniziativa progettuale;
* Definizione attività e deliverables;
* Sottoscrizione di uno SOW (Statement of Work);
* Apertura ingaggio e allocazione risorse;
* Inizio attività progettuali.

La Committente comunicherà al Fornitore l’attivazione di giorni persona per il servizio di consulenza specialistica mediante strumento telematico ad un apposito indirizzo mail all’uopo preposto.

Il servizio dovrà essere **erogato entro 5 giorni lavorativi** dalla ricezione della comunicazione di cui al precedente capoverso pena l’applicazione delle penali. Il termine utile per l’erogazione del servizio di cui in oggetto decorre dalla spedizione della e-mail.

Ogni attività ed intervento richiesto ed erogato sarà consuntivato mediante il Rapporto di intervento emesso da parte del Fornitore e sarà sottoposto all’approvazione della Committente.

Il servizio verrà svolto presso la sede di Roma della DCOD sita in via del Santuario Regina degli Apostoli n. 33 – 00145 dal lunedì al venerdì, esclusi il sabato, la domenica ed i festivi, entro l’arco orario compreso dalle 8:00 alle 18:00.

L’**Architetto** supporterà l’Istituto principalmente:

* nella definizione delle linee guida di adozione dei servizi Cloud Azure, in termini di architettura, rispondenza ai requisiti di CyberSecurity, affidabilità e resilienza;
* nel declinare i singoli progetti in ottica delle linee guida sopra menzionate, mettendo a disposizione esperienze, casi d’uso, best practices riconosciute, al fine di consentire all’Istituto l’uso ottimale dei servizi Cloud Azure.

Di seguito una descrizione delle principali attività che l’**Architetto** dovrà eseguire specificando alcune responsabilità che in determinati casi potrebbe essere chiamato ad assumersi:

Analisi dei requisiti di progetto;

* Analisi del contesto tecnologico dell’Istituto;
* Analisi dei requisiti di Cybersecurity;
* Individuazione dei servizi Azure più idonei a copertura dei requisiti e loro declinazione in termini di efficienza sui costi;
* Definizione delle architetture di riferimento integrate nel contesto tecnologico dell’Istituto in autonomia o a supporto di altri gruppi.
* Proporre all’Amministrazione soluzioni tecniche per progetti specifici fino ad assumersi la responsabilità del progetto, ove ritenuto necessario;
* Guidare le sessioni di analisi e architettura Fit/Gap e proporre/realizzare workshop su temi selezionati;
* Redazione (responsabilità) del documento di progettazione, anche con terzi delegati da INAIL, e in collaborazione con lo Specialista Senior, guidando il processo decisionale sul corretto utilizzo delle componenti Azure
* Leader di progetto di Microsoft e di INAIL, sul metodo di delivery agile, focalizzando il suo effort sul set di strumenti DevOps di Azure e includendo la comprensione della gestione delle comunicazioni e del backlog (epiche, features e attività).
* Fornire assistenza e intercettare proattivamente criticità in tutti i casi di:
  + interventi di configurazione di Azure e attività di compilazione della soluzione;
  + test della soluzione complessiva e supportare la soluzione walk-through;
  + Interventi di configurazione DevOps di Azure e di attività di creazione della soluzione usando principi di infrastructure as a code.

Lo **Specialista Senior** ha una forte competenza su tutti i servizi Cloud Azure, e supporterà l’istituto nelle fasi di realizzazione e implementazione delle soluzioni architetturali individuate, mettendo a disposizione dell’Istituto l'esperienza maturata nel contesto specifico per individuare le migliori modalità operative e di utilizzo dei servizi Azure.

Di seguito una descrizione delle principali attività che **lo Specialista Senior** dovrà eseguire specificando alcune responsabilità che in determinati casi potrebbe essere chiamato ad assumersi:

* Garantisce l'uso appropriato dei servizi Azure in termini di best pratices e sicurezza;
* Supporta l’Istituto nell’implementazione delle soluzioni;
* Contribuisce alla definizione di standard di processi e architetture;
* Fornisce formazione all’Istituto sulla gestione, il monitoraggio e la resilienza dei servizi in produzione;
* Esegue la Fit/Gap analysis e fornisce risultati al gruppo di lavoro;
* Esegue sessioni di progettazione dell'architettura, redigendo, anche in collaborazione con l’architetto e/o terzi delegati da INAIL, il documento di progettazione in cui si dettaglia corretto utilizzo ai riferimenti di Azure.
* Guida le sessioni di configurazione di Azure e tutte le attività di creazione della soluzione usando principi di infrastructure as a code.

Il Fornitore, entro 10 giorni lavorativi dalla data di stipula del contratto, dovrà presentare ad INAIL, per la dovuta approvazione, i CV delle risorse proposte per ciascuna figura professionale/ruolo, con evidenza del possesso delle competenze di cui alla precedente tabella e dell’esperienza maturata in progetti analoghi, nonché il possesso e il mantenimento delle certificazioni richieste da almeno 2 anni. Qualora i CV e/o la relativa documentazione presentata non dovessero essere ritenuti idonei da INAIL, il Fornitore, a pena di risoluzione del contratto, entro 5 giorni lavorativi dalla comunicazione di non idoneità, dovrà presentare nuovi CV e relativa documentazione rispondenti a quanto sopra richiesto.

* 1. **Verifica di conformità**

Entro il termine di **10 giorni** solari decorrente dalla data di consegna delle sottoscrizioni, Inail effettuerà una verifica di conformità il cui buon esito coincide con la “Data di accettazione del servizio”. La verifica di conformità verrà ripetuta in corso di esecuzione contrattuale sia con riferimento ai servizi cloud che ai servizi professionali, come meglio precisato nel Contratto Condizioni Speciali, Art. “Verifiche di conformità”.